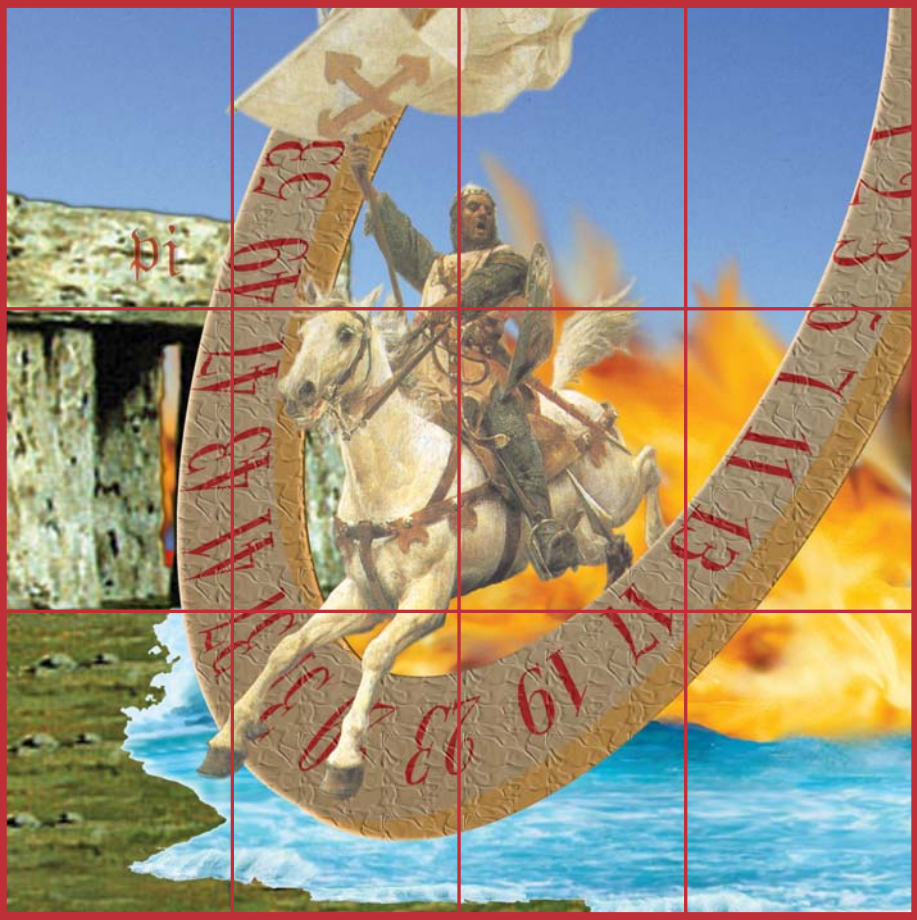
AVENTURAS MATEMÁTICAS

Dr. Leandro Cagliero
Dr. Daniel Penazzi
Dr. Juan Pablo Rossetti
Lic. Ana Sustar
Dr. Paulo Tirao



Colección: LAS CIENCIAS NATURALES Y LA MATEMÁTICA

Colección: LAS CIENCIAS NATURALES Y LA MATEMÁTICA

AVENTURAS MATEMÁTICAS

Dr. Leandro Cagliero, Dr. Daniel Penazzi, Dr. Juan P. Rossetti,
Lic. Ana Sustar y Dr. Paulo Tirao

autoridades

Presidente de la Nación
Dra. Cristina Fernández de Kirchner

Ministro de Educación
Dr. Alberto E. Sileoni

Secretaria de Educación
Prof. María Inés Abrile de Vollmer

Directora Ejecutiva del Instituto Nacional de Educación Tecnológica
Lic. María Rosa Almandoz

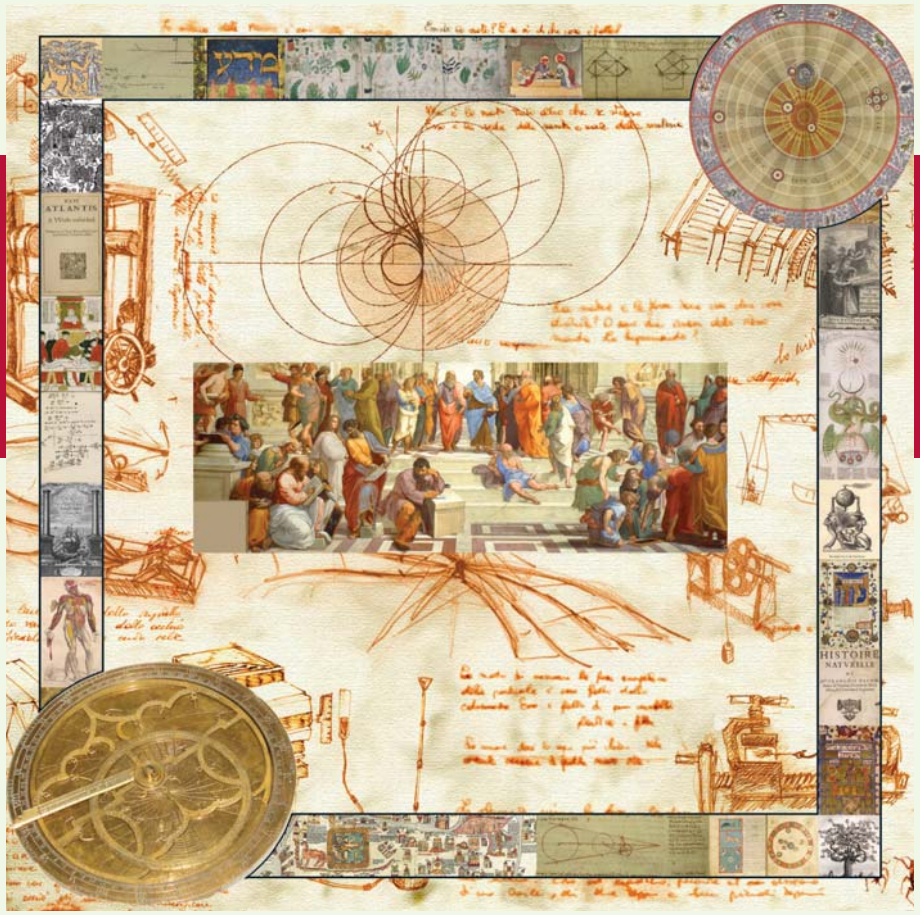
Director Nacional del Centro Nacional de Educación Tecnológica
Lic. Juan Manuel Kirschenbaum

Director Nacional de Educación Técnico Profesional y Ocupacional
Ing. Roberto Díaz

Ministerio de Educación.
Instituto Nacional de Educación Tecnológica.
Saavedra 789. C1229ACE.
Ciudad Autónoma de Buenos Aires.
República Argentina.
2010

AVENTURAS MATEMÁTICAS

Dr. Leandro Cagliero
Dr. Daniel Penazzi
Dr. Juan Pablo Rossetti
Lic. Ana Sustar
Dr. Paulo Tirao



Colección: LAS CIENCIAS NATURALES Y LA MATEMÁTICA

Colección “Las Ciencias Naturales y la Matemática”.
Director de la Colección: Juan Manuel Kirschenbaum
Coordinadora general de la Colección: Haydeé Noceti.

Industria Argentina

ISBN 978-950-00-0775-7

Director de la Colección:
Lic. Juan Manuel Kirschenbaum
Coordinadora general y académica de la Colección:
Prof. Ing. Haydeé Noceti
Diseño didáctico y corrección de estilo:
Lic. María Inés Narvaja
Ing. Alejandra Santos
Coordinación y producción gráfica:
Tomás Ahumada
Diseño gráfico:
Martin Alejandro Gonzalez
Ilustraciones:
Diego Gonzalo Ferreyro
Victoria Rossetti (Capítulo 3)
Federico Timerman
Retoques fotográficos:
Roberto Sobrado
Diseño de tapa:
Tomás Ahumada
Administración:
Cristina Caratozzolo
Néstor Hergenrether
Colaboración:
Téc. Op. en Psic. Soc. Cecilia L. Vazquez
Dra. Stella Maris Quiroga
Nuestro agradecimiento al personal del Centro Nacional de Educación Tecnológica por su colaboración.

Juan Pablo Rossetti
Aventuras matemáticas / Juan Pablo Rossetti, Leandro Cagliero... [et.al.]; dirigido por Juan Manuel Kirschenbaum.
- 1a ed. - Buenos Aires: Ministerio de Educación de la Nación. Instituto Nacional de Educación Tecnológica, 2009.
216 p.: il.; 24x19 cm. (Las ciencias naturales y la matemática / Juan Manuel Kirschenbaum.)

ISBN 978-950-00-0775-7

1. Matemática.
2. Enseñanza Secundaria.
3. Libros de Texto.
I. Cagliero, Leandro
II. Kirschenbaum, Juan Manuel, dir.

CDD 510.71 2

Fecha de catalogación: 15/04/2010

Impreso en Artes Gráficas Rioplatense S. A., Corrales 1393 (C1437GLE), Buenos Aires, Argentina.

Tirada de esta edición: 100.000 ejemplares

Los Autores

Dr. Leandro Cagliero

Doctor en Matemática de la Universidad Nacional de Córdoba y Profesor en la Facultad de Matemática, Astronomía y Física de esa universidad e investigador del CONICET. Fue becario externo del CONICET. Realizó un posdoctorado en el Instituto Tecnológico de Massachusetts (MIT). Actualmente es investigador en el área de representaciones de grupos de Lie y álgebra homológica. Ha publicado artículos científicos en revistas internacionales sobre estos temas. Dirige alumnos de doctorado, maestría y licenciatura. Realiza actividades de divulgación y apoyo a la enseñanza de la matemática en el nivel medio. Es colaborador desde 1990 de la Olimpíada Matemática Argentina, en la cual se ha desempeñado, en diversas oportunidades como jurado. Está casado y tiene tres hijos.

Dr. Daniel Penazzi

Se graduó de Doctor en Matemática (Ph.D. in Mathematics) en la Universidad de Minnesota (EE. UU). Previamente se graduó de Licenciado en Matemática en la Universidad Nacional de Córdoba. Es Profesor Adjunto en la Facultad de Matemática, Astronomía y Física de la Universidad Nacional de Córdoba. Ha dictado numerosos cursos en áreas diversas como Criptografía, Combinatoria, Álgebra, Análisis, Teoría de Grafos, Algoritmos de Flujos sobre Redes, Teoría de Complejidad Algorítmica, Teoría de Códigos y Dinámica Topológica. Ha publicado diversos artículos en las áreas de Dinámica Topológica, Combinatoria Algebraica y Criptografía. Ha dirigido 6 trabajos finales en áreas de Criptografía, Combinatoria y Teoría de Grafos. En el aspecto personal, está casado y tiene una hija, una perra, un perro, dos gatas y un gato.

Dr. Juan Pablo Rossetti

Es profesor en la Facultad de Matemática, Astronomía y Física de la Universidad Nacional de Córdoba, donde obtuvo los títulos de Licenciado y Doctor en Matemática. Es investigador del CONICET. Realizó estudios posdoctorales en EE. UU, con beca externa del CONICET y con beca de la fundación Guggenheim. En la Universidad de Princeton trabajó con el gran matemático John Horton Conway. Fue profesor visitante por un año en la Universidad Humboldt en Berlín. Sus temas de interés son la geometría de los grupos cristalográficos, la geometría espectral inversa y los retículos en espacios euclídeos. También se ha interesado por la matemática recreativa, colaborando con las Olimpíadas Matemáticas y la Competencia Paenza.

Lic. Ana Sustar

Obtuvo el título de Profesora de Matemática, Física y Cosmografía; otorgado por el Instituto Nacional de Enseñanza Superior (INES), Córdoba. Es Licenciada en Matemática de la Facultad de Matemática Astronomía y Física, (FaMAF - Universidad Nacional de Córdoba). Actualmente realiza el Doctorado en Matemática en FaMAF con beca doctoral de la Secretaría de Ciencia y Técnica, (SECyT) UNC, y es profesora de nivel medio en el Instituto "Academia Argüello" en Córdoba. Sus temas de interés son la combinatoria y el álgebra.

Dr. Paulo Tirao

Recibió el título de Doctor en Matemática de la Universidad Nacional de Córdoba y es Profesor en la Facultad de Matemática, Astronomía y Física de esa universidad e investigador del CONICET. Luego de graduarse pasó un período como posdoc en el International Centre for Theoretical Physics en Trieste, Italia, con una beca de la UNESCO y otro período en la Universidad de Düsseldorf, Alemania, con una beca externa del CONICET para regresar a Córdoba en el año 2000. Fue becario de la Fundación Alexander von Humboldt en Alemania. Sus intereses e investigación se desarrollan dentro del álgebra y la geometría diferencial en temas de la Teoría de Lie, álgebra homológica y teoría de grupos. Dirige a alumnos de doctorado, maestría y licenciatura y además de las tareas de docencia de grado y posgrado en la universidad realiza actividades de divulgación y apoyo a la enseñanza de la matemática en el nivel medio.

ÍNDICE

Introducción

Este libro pretende acercar de manera amena, aunque profunda, algunos temas importantes que se relacionan con el concepto fundamental de número, y transmitir algo de la invalorable experiencia que resulta hacer matemática.

Los cinco capítulos del libro se pueden leer en forma independiente y cada uno está presentado para que el lector pueda internarse en forma paulatina en los temas elegidos hasta alcanzar un elevado nivel de comprensión. La intención es dejarle a quien lea alguno de estos **relatos** una impresión distinta de la matemática y contribuir al desarrollo de su pensamiento lógico y crítico. Recorrer los capítulos superando los desafíos propuestos será una experiencia agradable que ayudará a apreciar la belleza y el poder de esta ciencia.

La matemática, considerada **el lenguaje del universo**, ocupa un lugar muy destacado en la cultura de la humanidad. El hombre desde sus orígenes hace matemática, ciencia ésta llena de vida y en constante crecimiento. En la matemática el valor de verdad es absoluto, el rigor de sus enunciados y la precisión de sus demostraciones son fundamentales y la imaginación y el desafío no encuentran límites. Estas distinguidas características pueden cautivar a quien se dé la oportunidad de apreciarlas.

Los capítulos tienen ejercicios y problemas que permitirán aprender y madurar los conceptos tratados, por lo que se recomienda hacerlos antes de ver las soluciones propuestas.

El **Capítulo 1** trata sobre las sorprendentes propiedades de los números primos, que son los ladrillos básicos sobre los cuales descansa la aritmética. Se presentan teoremas famosos sobre primos como el de Fermat, y problemas muy interesantes como el de la forma de factorear en primos un número cualquiera. Esto se hace en un marco histórico mostrando la manera en que ha ido evolucionando el saber humano sobre los números primos. En la última sección se incluye el uso de la computadora para factorear números compuestos, uno de los problemas más importantes en muchas áreas de la matemática, incluyendo la criptografía.

El **Capítulo 2** trata sobre conceptos y técnicas básicas de conteo, es decir formas de agrupar convenientemente conjuntos de objetos con el fin de poder calcular eficientemente la cantidad de elementos que tiene. El abordaje se realiza mediante la resolución de sucesivas situaciones problemáticas reales, seguidas de la formalización necesaria y unificadora de ideas.

Como primer problema se plantea el famoso **problema de matrimonios**, sobre las posibles maneras de sentar matrimonios alrededor de una mesa intercalando hombres y mujeres sin que se puedan sentar dos esposos juntos. Para poder resolverlo, hay que recurrir a los principios de adición y multiplicación, a las permutaciones, los arreglos, los conjuntos con repetición, y al **Principio de Inclusión-Exclusión**, que surgen como necesidad para resolver diversas situaciones más sencillas. En el Apéndice se incluye el **Principio del Palomar**, infaltable en un primer acercamiento al arte de contar.

El **Capítulo 3** trata sobre el infinito. El título puede parecer ambicioso, sin embargo, los objetivos son modestos: aprender **algo** sobre el infinito matemático. Éste es un tema que generalmente no es abordado en la escuela secundaria, donde se aprende que hay conjuntos infinitos pero no se plantea la posibilidad de comparar entre sí la cantidad de elementos que tienen distintos conjuntos infinitos. Es más común pensar que cuando algo es infinito no hay nada más que contar.

En los diálogos entre Clara y el Maestro se verá que, simplemente usando el concepto de **correspondencia biunívoca** entre dos conjuntos se puede elaborar una sólida teoría sobre las cantidades de elementos de conjuntos infinitos. Veremos que **hay infinitos tipos de infinito**s, y otras ideas que seguramente interesarán al lector tanto como a Clara, quien nos acompañará con sus preguntas y razonamientos a lo largo de esta aventura por el infinito.

El **Capítulo 4** está dedicado a la **aritmética modular**, una aritmética finita, es decir con un conjunto finito de números. En rigor hay una de estas aritméticas para cada natural mayor o igual que 2, y todas ellas tienen mucho que ver con la aritmética usual de los enteros. Esta aritmética es también llamada **aritmética cíclica** porque modeliza la aritmética de las horas del reloj, ejemplo que conocemos muy bien.

En este capítulo se encuentra la definición precisa de los elementos y operaciones de esta aritmética, hay ejemplos y también ejercicios que permiten adquirir un buen manejo de ella. Además, se muestran algunas aplicaciones interesantes como la deducción de las reglas de divisibilidad de enteros que se aprende en la escuela y la construcción de códigos sencillos para encriptar mensajes cuyo invento se le atribuye a Julio César.

Luego de esa breve introducción a la **criptografía**, es decir, a la ciencia de mandar mensajes secretos, en el **Capítulo 5** este tema se amplía. Se estudian las principales ideas de su desarrollo moderno y se ve cómo la matemática es de gran ayuda. Se verán algunos métodos históricos como el de **Vigenere** (donde se necesita algo de aritmética modular) y **Playfair o Hill** (en donde se usan matrices). También se estudiarán cifrados en bloque más modernos y se ilustrarán las características principales del estándar criptográfico actual y las razones matemáticas por las cuales es tan bueno. Se verán **cifrados de flujo** y una versión reducida del conocido **RC4**. Finalmente, se discutirá la criptografía de clave publica/privada, donde la aritmética modular será de gran importancia.

En el **Capítulo 6** están las resoluciones a todos los ejercicios y problemas planteados en los capítulos anteriores.

1. Los maravillosos números primos

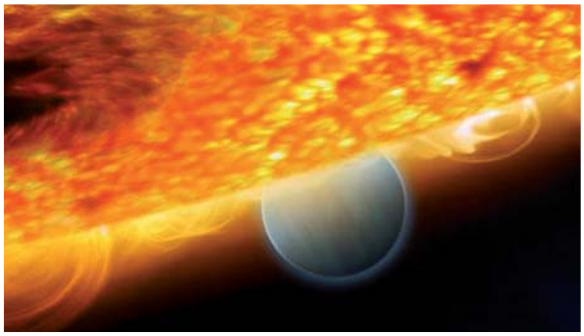
Por Leandro Cagliero

1. Los números naturales, cimientos de la matemática.
2. La irreductibilidad en las ciencias.
3. Primera etapa de la historia de los números primos.
4. Teoremas básicos sobre los números primos.
5. ¿Cómo se determinan los factores primos de un número dado?
6. ¿Cuáles son todos los números primos?

Los números primos son para la *matemática* como los elementos químicos para la *química*. Curiosamente, el ser humano se hace las mismas preguntas tanto para los elementos químicos como para los números primos.

- ¿Cuáles son todos los números primos que hay? ¿Cómo están distribuidos?
- ¿Cuáles son los números primos que aparecen en un número dado?
- ¿Cómo se hace para determinar los números primos que aparecen en un número dado?

La siguiente analogía enriquece las discusiones que puedan surgir sobre los ¿por qué? o ¿para qué? tan frecuentes en las ciencias.



Impresión realizada por un artista de la estrella HD 189733 y del planeta HD 189733b con fotos del telescopio Hubble, de la NASA

"¿... qué parece más importante?

Descubrir un método que sirva para hallar la descomposición primaria de números de más de 1.000 cifras en menos de una hora

o

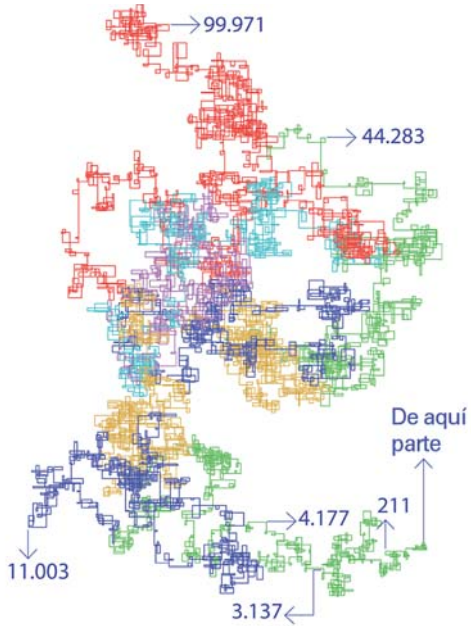
Descubrir planetas fuera del sistema solar que contengan dióxido de carbono en su composición química.

"... ambos desafíos están directamente relacionados con dos preguntas ubicadas por la revista Science entre las cien preguntas abiertas más importantes de las ciencias..."

Desde los comienzos de nuestra historia los números primos han despertado la curiosidad y asombro de muchos admiradores aficionados, y han generado en los científicos la ambición por comprenderlos en profundidad.

Aproximadamente en el año 200 a.C., Euclides demuestra que existen infinitos primos. El 10 de diciembre de 2008 la NASA anuncia que con observaciones del telescopio Hubble se ha descubierto que hay CO_2, un compuesto muy asociado a la vida, en el planeta HD189733b, que tiene el tamaño de Júpiter, que gira alrededor de una estrella que está a 63 años luz del Sol, ¡asombroso! Sin embargo, es más asombroso que todavía no sepamos de qué manera están distribuidos los números primos dentro de los números naturales. Ni siquiera se sabe si existen infinitas parejas de primos que sean impares consecutivos, es decir del tipo (3;5), (11;13), (17;19), o (1.000.000.931;1.000.000.933).

En este capítulo exploraremos el conjunto formado por los maravillosos números primos.



Camino que realiza una hormiga que va contando sus pasos y, en cada paso correspondiente a un número primo, dobla a la izquierda.

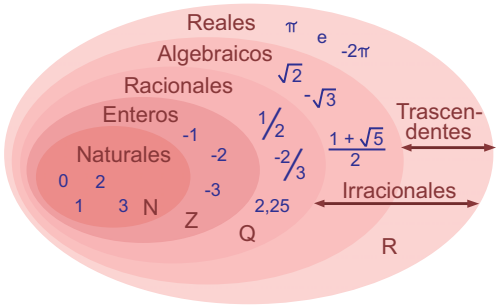
1.1. Los números naturales, cimientos de la matemática

Los **números naturales** son:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, ...

Con ellos construimos los demás números que usamos diariamente. Por ejemplo, los **números enteros** se construyen agregando el cero y los negativos a los números naturales, y los **números racionales**, a veces llamados **fraccionarios**, son los cocientes de números enteros. Además, los **números reales** se construyen con los números racionales, y los **números complejos** se construyen con los números reales. Y la aventura continúa... hay todavía más números que se construyen con los números complejos y, a su vez, estos sirven para seguir construyendo números que los científicos utilizan para describir aspectos de la naturaleza.

Podemos pensar que los números naturales son, de alguna manera, los cimientos de la matemática.



En este capítulo estamos interesados en ver cómo están fabricados estos cimientos. Queremos estudiar cómo y con qué están fabricados los números naturales.

1. ¿Cómo están fabricados los números naturales?

La respuesta a esta pregunta depende de cuál es la herramienta que utilicemos para construir. Recordemos que las dos herramientas básicas para trabajar con los números son la **adición** y la **multiplicación**. Así, surgen dos preguntas:

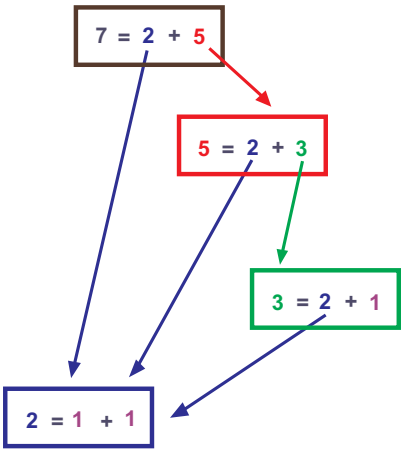
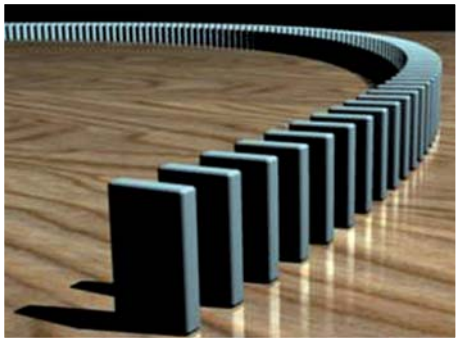


Figura 1.1: Partición del número 7 con la adición



a.- utilizando la adición, ¿cómo están hechos los números naturales?; b.- utilizando la multiplicación, ¿cómo están hechos los números naturales?

Al analizar estas preguntas aparece el proceso **de partir un número dado en partes más pequeñas** e investigar cuáles son las partes indivisibles que se obtienen.

La respuesta a la pregunta a.- no es muy complicada: por ejemplo, el 7 (**Figura 1.1**), con la adición, se puede partir como 2 + 5. A su vez el 2 se parte como 1 + 1 y el 5 es 2 + 3. Como el 3 es 2 + 1, concluimos que el 7 "está hecho" de

$$1 + 1 + 1 + 1 + 1 + 1 + 1.$$

Y se acaba aquí el proceso de partición, pues el 1 no se parte como suma de números naturales más pequeños.

Lo que sucede con el número 7 ocurre con cualquier número natural: todos se construyen sumando unos. El número 1 es el único número que no se puede partir en partes menores. Este análisis nos lleva a concluir que el número 1 es la única pieza básica que tienen los naturales cuando la herramienta considerada es la adición.

El hecho de que todo número natural se construya sumando números 1, y que el número 1 no se pueda partir en partes más pequeñas, es la base de lo que en matemática se conoce como Principio de Inducción.

Al analizar estas preguntas aparece el proceso de partir un número dado en partes más pequeñas e investigar cuáles son las partes. A los matemáticos les gusta representar este principio con fichas de dominó organizadas de tal forma que al caer la primera (que simboliza el número 1), todas las demás caigan. Esto representa el hecho de que todos los números naturales son construidos con el primero de ellos.

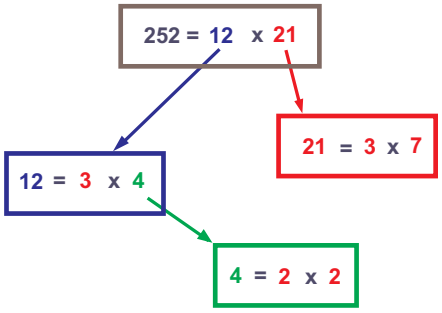


Figura 1.2: Partición del número 252 con la multiplicación.

La respuesta a la pregunta b.- es mucho más rica que la respuesta de la pregunta a.- Cuando consideramos la multiplicación como herramienta hay muchas piezas irreducibles. Por ejemplo el 252 (**Figura 1.2**) se parte como 12 × 21 y, a su vez, el 12 es 3 × 4, el 21 es 3 × 7 y el 4 es 2 × 2. Aquí el proceso de partición termina pues los números 2, 3 y 7 no pueden ser partidos en partes más pequeñas usando la multiplicación, son irreducibles. Por lo tanto el 2, 3 y 7 son las "piezas básicas" del número 252:

$$252 = 2 \times 2 \times 3 \times 7 \times 3.$$

Este proceso de partición de los números con la multiplicación se llama **factoreo** y nos lleva a distinguir entre dos clases de números naturales: los que se pueden partir en partes más pequeñas, es decir que son factoreables, y los que no, es decir los que son irreducibles. Los primeros son llamados **números compuestos**. Los segundos, a excepción del número 1, son llamados **números primos**. El número 1 no sirve para construir ningún número usando la multiplicación. El número 1 en la multiplicación tiene el mismo rol que el número 0 para la adición. Por este motivo, el número 1 no es considerado primo, tampoco es compuesto, y es llamado **unidad**.

En resumen:

Números Compuestos: son los números naturales que ***sí*** se pueden expresar como producto de dos números naturales menores a ellos.

Números Primos: son los números naturales que ***no*** se pueden expresar como producto de dos números naturales menores a ellos, excepto el 1.

Los números primos constituyen las piezas básicas de los cimientos de la matemática: con ellos y con la multiplicación construimos todos los números naturales. Los primeros (considerando desde 1 a 3.571) son:

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113	127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863	877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151	1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291	1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733	1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889	1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053	2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213	2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357	2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531	2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
2621	2633	2647	2657	2659	2663	2671	2677	2683	2687	2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819	2833	2837	2843	2851	2857	2861	2879	2887	2897	2903

2909 2917 2927 2939 2953 2957 2963 2969 2971 2999 3001 3011 3019 3023 3037 3041 3049 3061 3067 3079

3083 3089 3109 3119 3121 3137 3163 3167 3169 3181 3187 3191 3203 3209 3217 3221 3229 3251 3253 3257

3259 3271 3299 3301 3307 3313 3319 3323 3329 3331 3343 3347 3359 3361 3371 3373 3389 3391 3407 3413

3433 3449 3457 3461 3463 3467 3469 3491 3499 3511 3517 3527 3529 3533 3539 3541 3547 3557 3559 3571

En la página http://primes.utm.edu/lists/small/millions/ aparecen los primeros 50 millones de números primos.

Cerramos esta primera sección aclarando que en matemática también se consideran primos a los negativos de los números naturales primos, es decir que el -2, -3, -5, etcétera también son primos.

Para resolver

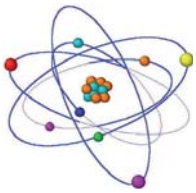
¿Cómo son los siguientes números? ¿Es alguno de ellos primo?

El número de tres cifras de la patente de tu auto.
El número de la dirección de tu casa.
El número de tu teléfono o celular.
El número de tu documento.

1.2. La irreductibilidad en las ciencias

Desde siempre el hombre ha estudiado diferentes clases específicas de objetos, ya sean materiales, espirituales, numéricos, concretos o abstractos. Independientemente de cuál sea la clase que haya estudiado, siempre estuvo muy interesado por encontrar respuestas a las siguientes preguntas:

- ¿qué herramientas podemos utilizar para dividir los objetos en partes más pequeñas?;
- dado un objeto de la clase que estamos estudiando, ¿es posible dividirlo en dos porciones más pequeñas? ¿es posible volver a dividir cada porción resultante en otras dos y luego seguir dividiendo y dividiendo en partes cada vez más pequeñas las porciones obtenidas?;
- ¿se llegará en algún momento a obtener piezas irreducibles, es decir porciones tan "pequeñas" que no puedan ser divididas en partes menores?;
- conociendo todas las piezas irreducibles de la clase de objetos estudiada, ¿es posible construir con ellas todos lo otros objetos de la clase? ¿es única la manera de reconstruir los objetos con las piezas irreducibles?;
- ¿cuáles son todas las piezas irreducibles?, ¿cómo están distribuidas?



Estas preguntas han intrigado a científicos y filósofos desde hace miles de años, en parte por la curiosidad de comprender cuáles son los elementos básicos con los que está formado nuestro universo.

Es probable que el ejemplo más familiar de esta situación sea el de la química. En esta ciencia, cuando el objeto de estudio es la materia y

la división en partes menores debe llevarse a cabo con herramientas que conserven las propiedades químicas de la materia, los elementos irreducibles que aparecen son los elementos químicos que conocemos de la tabla periódica (**Figura 1.3**).

Figura 1.3. Tabla periódica de los elementos.

El concepto de que la materia no puede ser dividida en porciones arbitrariamente pequeñas, es decir la existencia de elementos químicos irreducibles, es muy antiguo. Por ejemplo, la palabra **átomo** proviene de un término griego que significa **imposible de cortar** y se cree que fue introducida por Demócrito alrededor del año 450 a.C.

Este concepto ha sido estudiado, cuestionado y revisado en numerosas oportunidades, desde los filósofos de la antigüedad hasta los científicos de la actualidad que, dependiendo de las herramientas permitidas para dividir y de las propiedades de la materia que se deban preservar, se dedican a buscar en profundas investigaciones respuestas a las preguntas que planteábamos anteriormente.

1.2.1. La irreductibilidad en la matemática

Cuando los objetos de estudio son los números naturales y la herramienta utilizada es la multiplicación no es posible llevar a cabo un proceso de división en partes más pequeñas que no se termine nunca, porque después de cierta cantidad de pasos se llega, inevitablemente, a los números primos; estos son elementos irreducibles. Los números primos, pueden pensarse como análogos a los elementos químicos cuando el objeto de estudio son los números naturales y la herramienta de construcción es la multiplicación.

En otras áreas de las ciencias no existen elementos irreducibles, incluso en áreas de la matemática. Es ilustrativo analizar el caso de los números racionales porque, en este aspecto, son muy diferentes a los números naturales. Con ellos sí es posible llevar a cabo un proceso de partición en partes más pequeñas que no se termine nunca. Por ejemplo, veamos lo que sucede con el número 12 (**Figura 1.4**):

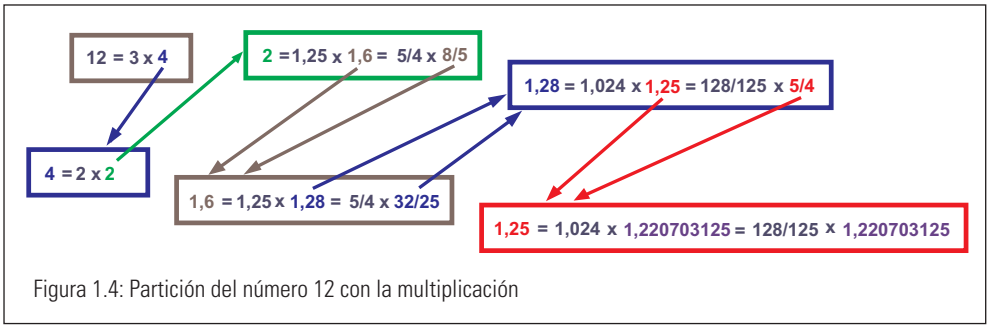


Figura 1.4: Partición del número 12 con la multiplicación

El proceso se puede repetir tantas veces como queramos. Esto lo podríamos hacer con cualquier número racional y, por lo tanto el conjunto de números racionales no tiene números irreducibles con la multiplicación.

Lo que acabamos de ver es un lindo ejemplo de "infinita divisibilidad". Sin embargo, no es muy relevante para la matemática, pues como ya dijimos, los números racionales se construyen con los enteros, los enteros con los naturales y en estos últimos sí hay piezas irreducibles: **los números primos**.

A modo de resumen, y para organizar la lectura de este capítulo, adaptamos al contexto de los números naturales las preguntas que destacábamos como fundamentales para el estudio de los elementos irreducibles. Algunas de ellas ya se respondieron, otras no.

Preguntas fundamentales de los números naturales	
Pregunta 1	¿Qué herramientas podemos utilizar para dividir los números naturales en números más pequeños?
Respuesta.	Podemos utilizar la adición o la multiplicación. Son las dos herramientas principales. Nosotros estaremos interesados en trabajar con la multiplicación. En matemática, la acción de escribir un número como producto de dos números menores se llama **factorear**.
Pregunta 2	Dado un número natural arbitrario, ¿es posible expresarlo como producto de dos números menores a él?
Respuesta.	Hay algunos números factoreables y otros no. Los primeros se llaman **compuestos** y pueden expresarse como producto de dos menores. Los segundos, a excepción del 1, se llaman **primos**.
Pregunta 3	Si empezamos a factorear un número natural, ¿podremos seguir factoreando los factores que obtengamos indefinidamente? ¿o siempre se llegará en algún momento a factores irreducibles, es decir que no puedan ser factoreados?
Respuesta.	Siempre se llegará en algún momento a factores irreducibles y el motivo será analizado en la **Sección 4**.
Pregunta 4	¿Es posible expresar a todos los números naturales como producto de números primos?
Respuesta.	Sí. La razón será estudiada en la **Sección 4**.
Pregunta 5	¿Hay algún número natural que pueda ser expresado como producto de números primos de dos maneras distintas?
Respuesta.	No, y también discutiremos esta pregunta en la **Sección 4**. Las dos últimas preguntas son tan importantes que sus respuestas constituyen el **Teorema fundamental de la aritmética**: "Todo número natural se factorea de una ***única forma*** como producto de números primos."
Pregunta 6	¿Cuántos números primos hay?
Respuesta.	Veremos en la **Sección 4** que son infinitos.
Pregunta 7	¿Cómo se hace para averiguar si un número dado es primo o compuesto? Y, en caso de ser compuesto, ¿cómo encuentro sus factores primos?
Respuesta.	Es fácil si el número dado es pequeño, pero muy difícil si el número es grande. Discutiremos esta pregunta en la **Sección 5**.

Pregunta 8	¿Cuáles son todos los números primos?
Respuesta.	**¡Qué interesante es esta pregunta!** Recién dijimos que son infinitos y por lo tanto no hay una tabla como la de los elementos químicos que contenga a todos los primos. ¿Qué quiere decir la pregunta? ¿Cuáles son todos los números primos? ¿y cuál sería una buena respuesta? En la **Sección 6** daremos algunas respuestas a las siguientes variantes de esta pregunta.
Variante (a)	Entre los números naturales, ¿qué porcentaje corresponde a los números primos?
Variante (b)	¿Hay una fórmula que dé todos o algunos números primos?
Variante (c)	¿Cuáles son todos los números primos ***conocidos***?

Para resolver

1.1 Decidir cuáles de los siguientes números son primos y descomponer como producto de números primos los que sean compuestos:

73, 173, 273, 373, 473, 573, 673, 773, 873, 973, 1.073.

1.2 Descomponer los siguientes números como producto de números primos:

4.875, 18.207, 236.769 y 710.073.

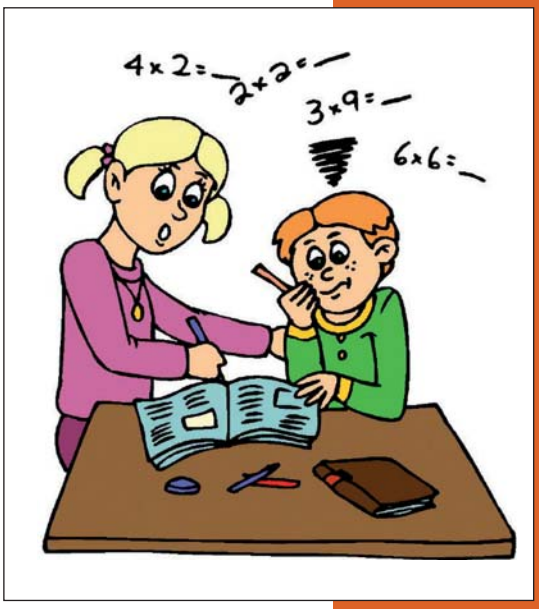
1.3 Éste es más difícil: descomponer el 322.423 como producto de números primos.

1.4 Explicar el porqué es más difícil hallar la descomposición en primos del número 322.423 que la del número 710.073.

1.5 Encontrar el primo que seguiría en la tabla de primos de la **Sección 1**.

1.6 Expresar el número racional 1,220703125 = 625/512 como producto de dos números racionales positivos menores a él, y continuar partiendo en dos una vez más.

1.7 Ya vimos que en el conjunto de números racionales no hay números irreducibles con la multiplicación. Ahora preguntamos, ¿hay elementos irreducibles en el conjunto de números racionales positivos cuando usamos como herramienta la adición?



1.8 No es difícil, pero hace falta pensar un poco. Supongamos que nuestro objeto de estudio son los números naturales pares: 2, 4, 6, 8, 10, 12, 14, etc. Debemos jugar a que los *únicos números que existen son los números pares*. ¿Cuáles son los números irreducibles? El análisis empieza así: el 2 es irreducible, el 4 no pues es 2×2, hasta aquí nada raro, pero se viene la sorpresa ¡el 6 es irreducible, pues el 3 no existe, sólo existen los pares!

1.3. Primera etapa de la historia de los números primos

1.3.1. Más de 2.000 años atrás

Papiro de Rhind, 1650 a.C.

Portada de una traducción al latín de los Elementos, año 1309 - 1316.

Los números primos, los irreducibles de la multiplicación, despertaron la atención del hombre por primera vez hace más de 3.500 años. Una famosa manifestación de esto se encuentra en el *papiro de Rhind*, que fue escrito por el escriba egipcio Ahmes aproximadamente en el año 1650 a.C. En él se discuten varios problemas de matemática y se puede observar el conocimiento que los egipcios ya tenían del hecho de que algunos números son factoreables como producto de dos menores y otros no.

Alrededor del año 500 a.C. los pitagóricos estudiaron diferentes tipos de números. Probablemente, buscaban clasificarlos según las propiedades que tuvieran sus divisores, motivados por las consecuencias geométricas de estas propiedades. Un ejemplo paradigmático de ello, son los *números perfectos*. Estos son aquellos que son iguales a la suma de sus divisores positivos menores. Por ejemplo el 6 es igual a 1 + 2 + 3; y el 28 es igual a 1 + 2 + 4 + 7 + 14.

En el año 300 a.C comienza el estudio sistemático de los números primos cuando el matemático griego **Euclides** escribe la maravillosa obra **Elementos**. **Los Elementos** de **Euclides** es un tratado de matemática que consta de 13 libros en el que se recopilan los conocimientos de matemática que tenían los griegos hasta entonces. Esta enciclopedia fue desde siempre una obra muy valorada por diversos motivos. El principal es que en ella se establece el carácter axiomático-deductivo de la matemática, especialmente manifestado en el famoso tratamiento que se hace de la geometría plana.

En los libros VII - IX se trata la aritmética de los números naturales y, en particular, se establecen las propiedades básicas de los números primos con énfasis en el rigor de las demostraciones. Así surgió la rama de la matemática que hoy se conoce como **teoría de números.**

En la obra de Euclides se nota el interés que había en encontrarle respuestas a las preguntas que planteábamos en la **Sección 2**. En los Elementos son contestadas con demostraciones rigurosas las **preguntas 4, 5 y 6**.

Haciendo honor al trabajo de Euclides, es el momento adecuado para recordar que las verdades en matemática se llaman teoremas y requieren ser demostradas rigurosamente. Veremos las demostraciones de Euclides en la próxima sección.

Desde entonces, los matemáticos han hecho muchos esfuerzos por dar respuestas a las **preguntas 7 y 8** que planteamos al final de la sección anterior, y todavía hoy sigue la lucha.

El primer paso hacia estas respuestas fue dado en el año 200 a.C. por ***Eratóstenes***. Él descubrió un método para reconocer si un número dado es primo, es decir para dar una respuesta a la **pregunta 7**. Este método es conocido como la ***Criba de Eratóstenes*** y consiste en una serie de pasos a seguir que conducen a decidir si un número dado es primo. Hoy llamamos a este tipo de métodos *algoritmos*. Siempre sucede que hay métodos mejores que otros y, más adelante, veremos que el de Eratóstenes requiere demasiados pasos.

Eratóstenes

Además de matemático, Eratóstenes era astrónomo, deportista e incluso poeta. Uno de sus logros más famosos es haber medido con gran precisión el radio de la Tierra.

Para hacerlo utilizó el hecho de que en ciertos lugares de la Tierra (los que están sobre los trópicos) los rayos de sol caen verticalmente a la hora del mediodía del día del solsticio. La **figura 1.5** ilustra este hecho mostrando que la luz solar pasa verticalmente dentro de un pozo de agua. En estos lugares, a esa hora, un poste vertical no tiene sombra. Justo a esa misma hora Eratóstenes midió la sombra que proyectaba un poste en su ciudad natal, Alejandría, que **no estaba sobre el trópico de Cáncer** y por eso el poste sí producía sombra. Midiendo la distancia entre Alejandría y el trópico de Cáncer, y utilizando los conocimientos de geometría que él tenía (seguramente por haber estudiado los Elementos de Euclides) obtuvo el radio de la Tierra con un error de aproximadamente el 17%.

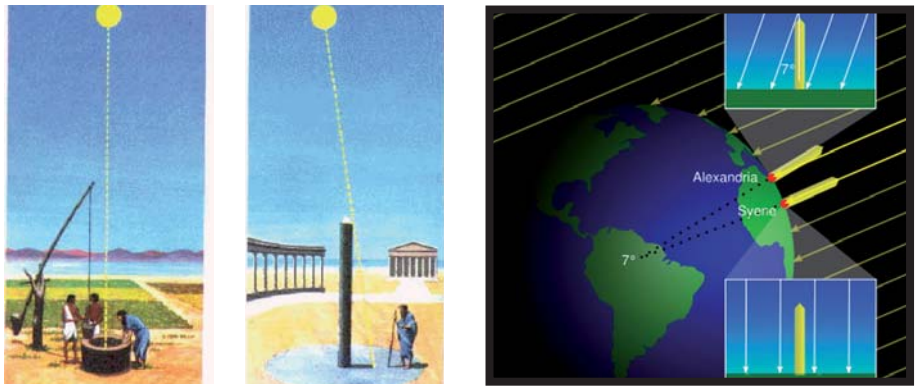


Figura 1.5 Eratóstenes mide el radio de la Tierra durante el solsticio de verano en Egipto

1.3.2 En la era cristiana

Después de los griegos no hubo progresos significativos en el estudio de los números primos hasta que en el siglo XVII el famoso abogado (sí, abogado) francés ***Pierre de Fermat*** hizo importantes avances.

Pierre de Fermat 1601 - 1665

Aunque originalmente estudió derecho, Fermat se dedicó a investigar diversos temas de matemática. Fue contemporáneo de René Descartes, creador del área de la matemática que hoy conocemos como Geometría Analítica. Y aunque contribuyó en esa área, Fermat fue más famoso por sus resultados relacionados con los números primos. Uno de los principales fue el descubrimiento del siguiente teorema, conocido hoy como el Pequeño Teorema de Fermat.

Pequeño Teorema de Fermat: Si p es un número primo y n es un número que no es múltiplo p, entonces n^{p-1} da resto 1 al dividirlo por p.

No demostraremos este teorema, pero sí vamos a desarrollar un ejemplo. El número 5 es primo. En la siguiente tabla analizamos las potencias cuartas de 1, 2, 3, 4, 6, 7, 8, 9 y 11 (salteamos los múltiplos de 5 pues el teorema los excluye). Podemos ver en la tabla que el resto de dividir n^4 dividido 5 es siempre 1. Este hecho se manifiesta en que los resultados de n^4 terminan todos en 1 ó 6.

n	n^4	Cociente al dividir por 5	Resto al dividir por 5
1	1	0	1
2	16	3	1
3	81	16	1
4	256	51	1
6	1.296	259	1
7	2.401	480	1
8	4.096	281	1
9	6.561	1.312	1
11	14.641	2.928	1

Esto no ocurre en general si el número p no es primo. Por ejemplo si $p = 4$ entonces los restos de dividir n^3 dividido 4 son:

n	n^3	Cociente al dividir por 4	Resto al dividir por 4
1	1	0	1
2	8	2	0
3	27	6	3
4	125	31	1
5	216	54	0
6	343	85	3
7	4.096	281	1

El Pequeño Teorema de Fermat tiene diversas consecuencias. Una de ellas es la aparición de una regularidad, o propiedad en común, que gozan todos los números primos. Otra, es un nuevo aporte para contestar parcialmente la **pregunta 7**: ¿cómo hacemos para darnos cuenta si un número dado es o no primo? El Pequeño Teorema de Fermat da un argumento para darnos cuenta de que algunos números no son primos. Por ejemplo, podríamos argumentar que el 4 no es primo pues 3^3 no da resto 1 al dividirlo por 4.

Advertencia

El Pequeño Teorema de Fermat sólo sirve para confirmar que un número no es primo, dado que algunos números, sin ser primos, cumplen la propiedad del Pequeño Teorema de Fermat. Un ejemplo de ello es el número compuesto $561 = 3 \times 11 \times 17$, que cumple que n^{560} da resto 1 al dividirlo por 561 si n es un número que no es múltiplo ni de 3, 11 ó 17.

Fermat también se preocupó por encontrar fórmulas que dieran números primos como resultado. Ésta es la **Variante (b)** de la **Pregunta 8**. Descubrió que los siguientes números eran primos:

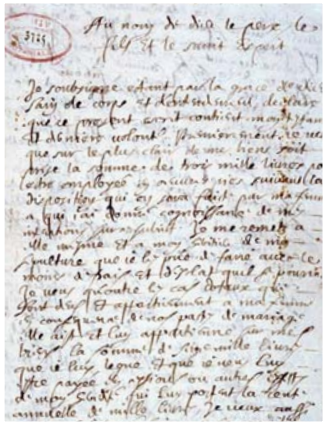
$$2^{2^1}+1=2^2+1=5$$

$$2^{2^2}+1=2^4+1=17$$

$$2^{2^3}+1=2^8+1=257$$

$$2^{2^4}+1=2^{16}+1=65.537$$

y se convenció de que, cualquiera sea el número n, siempre sucedía que 2^{2^n} era primo. Él sabía que $2^{2^5}+1=2^{32}+1$ da como resultado 4.294.967.297 y sospechaba que era primo. Aproximadamente 100 años después, en 1732, ***Leonard Euler*** descubre que 4.294.967.297 es compuesto pues es igual a 641 × 6.700.417. Esto frustró el intento de obtener una fórmula que siempre diera primo. Fermat había errado en esta oportunidad; incluso hasta el día de hoy no se conoce ningún número $n > 4$ tal que $2^{2^n}+1$ sea primo. En lo que no erró, y muy por el contrario lo catapultó a la fama, fue al descubrir lo que hoy se conoce como ***Último Teorema de Fermat.***



Copia del testamento de Fermat escrito de su puño y letra (1660)

Leonard Euler 1707 - 1783

Último Teorema de Fermat: Si n es un número natural mayor que 2 entonces no existen números naturales a, b y c que cumplan

$$a^n + b^n = c^n$$

Aunque no sea evidente a primera vista, este teorema está muy relacionado con los números primos y con otras áreas de la matemática. Si $n=2$ **sí** existen a, b y c que cumplan $a^n+b^n=c^n$. Por ejemplo: $3^2+4^2=5^2$, $5^2+12^2=13^2$, entre muchas más opciones. Las ternas a, b y c que cumplen $a^2+b^2=c^2$ se llaman *ternas pitagóricas* (**Figura 1.6**) porque son números naturales que sirven como medidas para armar triángulos rectángulos.

El último Teorema de Fermat ha sido, y es, muy renombrado. Su trascendencia alcanzó diversos ámbitos, hasta en series televisivas.

A pesar haber sido llamado desde siempre "teorema", su demostración fue hallada 350 años más tarde por el matemático inglés ***Andrew Wiles***, actual jefe del departamento de matemática de la Universidad de **Princenton**. Numerosos investigadores, e incluso aficionados, habían trabajado intensamente buscando una demostración del **Último Teorema de *Fermat***. En gran parte, la motivación provenía por la desafiante anécdota que dice que Fermat escribió en un libro que utilizaba para estudiar lo siguiente: "conozco una demostración verdaderamente maravillosa de este teorema pero el margen de este libro es demasiado pequeño para contenerla". En latín original *"Cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet".*

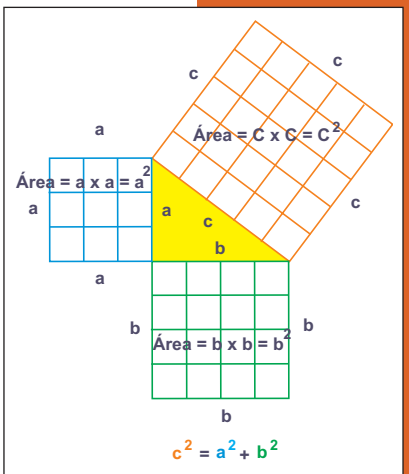


Figura 1.6 Ternas pitagóricas

Andrew Wiles

Se sabe que Fermat había probado su teorema para n = 4. Más tarde Euler lo demuestra para $n = 3$ y en 1825 Dirichlet y Legendre, cada uno por su lado, para $n = 5$. Con el correr de los años, se ofrecieron premios en dinero para la demostración del caso n arbitrario, lo que provocó una avalancha de intentos. Se cree que entre 1908 y 1911 hubo más de 1.000 demostraciones incorrectas.

El libro del que estudiaba Fermat, cuyo margen se volvió tan famoso, es *La Arithmetica* de *Diofanto de Alejandría*, un matemático del siglo III DC. El libro constaba de una larga lista de problemas de álgebra.

En la **figura 1.7** visualizamos la tapa de la traducción al latín de este libro. En la **figura 1.8** reproducimos una página de este libro en su edición de 1621. En ella se ve el renombrado margen. La **figura 1.9** nos muestra la misma página en la que, en una edición posterior, se incorpora la pregunta que había hecho Fermat.

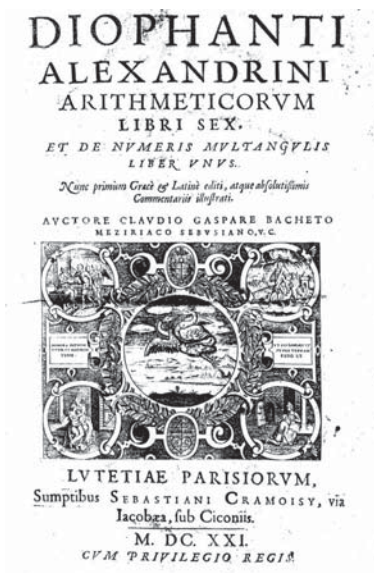

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V. C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS

Figura 1.7.


Arithmeticorum Lib. II. 85

QVÆSTIO VIII.

QVÆSTIO IX.

Figura 1.8.


Arithmeticorum Liber II. 61

IN QVÆSTIONEM VII.

QVÆSTIO VIII.

OBSERVATIO DOMINI PETRI DE FERMAT.

QVÆSTIO IX.

Figura 1.9.

Ésta es la primera etapa de la rica historia de los números primos. Relataremos la etapa más moderna de su historia en las **Secciones 5 y 6.**

□ 1.4. Teoremas básicos sobre los números primos

En esta sección demostraremos las propiedades básicas de los números primos. De ellas obtenemos las respuestas de las **preguntas 4, 5 y 6** de la **Sección 2**. Como ya dijimos, estas respuestas aparecieron en el año 300 a.C en los Elementos de Euclides. El hilo lógico y las demostraciones que presentaremos son muy similares a las de ese libro[1].

1.4.1. Primera propiedad

Para responder a la **pregunta 4.**

Teorema sobre la factorización de los números naturales
Todo número natural se factorea como producto de números primos.

Demostración

Se demostrará por el absurdo. Supongamos que existe un número que no se puede factorear como producto de números primos y llamemos n_0 al menor de todos esos números. Este número n_0 tiene que ser compuesto, pues si fuera primo ya estaría factoreado como "producto" de un sólo número primo. Al ser n_0 un número compuesto resulta que $n_0 = n_1 \times n_2$, con n_1 y n_2 menores que n_0. Pero como n_0 era el menor número no factoreable como producto de primos y n_1 y n_2 son menores que n_0, obtenemos que n_1 y n_2 sí son factoreables como producto de primos, es decir que n_1 es producto de primos y n_2 es producto de primos. Como $n_0 = n_1 \times n_2$, obtenemos que n_0 también es producto de primos lo cual es una contradicción.

Del dicho al hecho hay mucho trecho.
El teorema que acabamos de enunciar afirma que todo número natural se factorea como producto de números primos, pero no es tan sencillo factorear un número dado.

Recordemos un método para factorear, que probablemente hayamos aprendido alguna vez: Dado el número que queremos factorear:

se lo divide por 2 todas las veces que sea posible,
luego se divide el resultado por 3 todas las veces posible,
luego por 5, luego por 7, etc.

Por ejemplo, para factorear el número 12.936 hacemos:

12.936	2
6.468	2
3.234	2
1.617	3
539	7
77	7
11	11
1	

[1] Una excelente fuente para profundizar sobre estos temas son los libros [1] y [6].

Así obtenemos que $12.936 = 2^3 \times 3 \times 7^2 \times 11$. Este método presume que se descubre fácilmente el menor primo que divide el número que va quedando. Sin embargo, esto no siempre es sencillo.

Analicemos el número 12.345.678:

12.345.678	2
6.172.839	3
2.057.613	3
685.871	????

Aquí se pone más complicado. Después de pensar un rato descubrimos que la factorización continúa así:

12.345.678	2
6.172.839	3
2.057.613	3
685.871	47
14.593	????

y nuevamente nos trabamos. Hace falta trabajar un buen rato para verificar que 14.593 es primo y por lo tanto hemos terminado:

12.345.678	2
6.172.839	3
2.057.613	3
685.871	47
14.593	14.593
1	

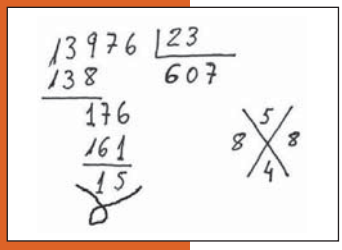
La factorización en primos de 12.345.678 es $2 \times 3^2 \times 47 \times 14.593$.

Para resolver

1.9 Encontrar la factorización en primos de 226.738.512.

1.10 Encontrar la factorización en primos de 3.772.486.575.

1.4.2. Segunda propiedad

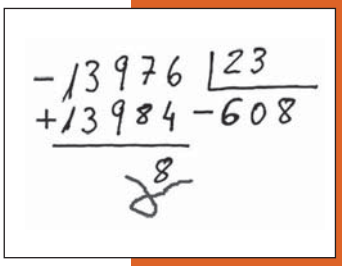


Antes de seguir adelante con las preguntas de la **Sección 2** recordemos el *algoritmo de división*, porque es una herramienta fundamental para trabajar con números naturales o enteros.

Algoritmo de división. Sean a y b dos números naturales. Entonces existen únicos naturales q (llamado cociente) y r (llamado *resto*) con $0 \leq r < b$ tales que $a = b \times q + r$.

Una manifestación de este algoritmo en la vida real es ganar un premio entre varios y repartirlo. Como ejemplo, en la división del dibujo de arriba, podemos ver un premio de $ 13.976 repartido entre 23 personas. A cada una le toca $ 607 y sobran $ 15.

A pesar de que en este capítulo estamos interesados principalmente en los números naturales, vale la pena destacar que la mayoría de los resultados que establezcamos son válidos también para números enteros que incluyen a los negativos de los números naturales.



Esto ocurre con el algoritmo de división, que cambia ligeramente del siguiente modo: si el número a es negativo, entonces el cociente da negativo, pero el resto sigue siendo positivo. Este caso también se manifiesta en la vida real, como pagar una deuda entre varias personas. Por ejemplo, si tenemos una deuda de $ 13.976 que debe ser pagada entre 23 personas y cada una pusiera $ 607 entonces faltarían $ 15. Lo que debemos hacer es que cada uno ponga $ 608 para que sobren $ 8. Por lo tanto el cociente de dividir –13.976 dividido 23 es –608 y el resto es positivo 8.

El algoritmo de división tiene diversas consecuencias. Una de ellas es la siguiente propiedad de los números primos.

Teorema: Sea p un número primo.

1.- Si n no es múltiplo de p, entonces existen números naturales a y b tales que $a \times n - b \times p = 1$. Es decir que hay un múltiplo de n y un múltiplo de p que restados dan 1.

2.- Si m y n son naturales tales que $m \times n$ es múltiplo de p, entonces al menos uno de los dos números m o n es múltiplo de p.

Antes de demostrar este teorema veamos unos ejemplos para comprender mejor lo que afirma.

La segunda afirmación nos dice que no se pueden fabricar múltiplos de un primo p multiplicando dos números tales que ninguno sea múltiplo de p. Esto es diferente con los números compuestos. Por ejemplo, podemos fabricar un múltiplo de 4 multiplicando el 6 por 2, y ni el 6 ni el 2 son múltiplos de 4.

Sobre la primera afirmación veamos cómo expresar el 1 como diferencia de un múltiplo de $n = 18$ y un múltiplo de $p = 7$.

Múltiplos de 18:	Múltiplos de 7:
0, 18, 36, 54, 72, 90, 108, …	0, 7, 14, 21, 28, 35, 42, 49, …

Vemos que podemos expresar el 1 como la resta de 36 menos 35.

En cambio, si p hubiera sido 15 (en lugar de ser primo) la resta de un múltiplo de 18 menos un múltiplo de 15 siempre da un múltiplo de 3, y por lo tanto es imposible obtener el 1 restando múltiplos de 18 y múltiplos de 15.

Aclaración

La parte 1.- del teorema anterior vale con mayor generalidad que la enunciada

Teorema (parte 1.- generalizada): Si n y m no tienen factores primos en común, entonces hay un múltiplo de m y un múltiplo de n que restados dan 1.

Por ejemplo, si $m = 22$ y $n = 15$, entonces:

los múltiplos de 22 son:
0, 22, 44, 66, 88, 110, 132, 154, 176, 198, 220, 242, 264, 286, 308, 330, 352, ...

los múltiplos de 15 son:
0, 15, 30, 45, 60, 75, 90, 105, 120, 135, 150, 165, 180, 195, 210, 225, 240, 255, 270, 285, 300, ...

Vemos que podemos expresar el 1 como la resta de 286 menos 285.

No demostraremos esta generalización, sólo el teorema enunciado anteriormente.

Demostración del Teorema.

1.-Si aplicamos el algoritmo de división a n y p: resulta que $n = q \times p + r$, con $0 < r < p$ (r no puede ser cero pues n no es múltiplo de p). Es decir que $r = n - q \times p$ es un número natural menor que p que es diferencia de un múltiplo de n y un múltiplo de p.

Llamemos r_0 al menor número natural que se pueda expresar como resta de un múltiplo de n menos un múltiplo de p. Tenemos que $r_0 = a \times n - b \times p$, y por el argumento del primer párrafo sabemos que $r_0 < p$. Queremos demostrar que $r_0 = 1$.

Si r_0 fuera mayor que 1, aplicamos el algoritmo de división a p y r_0 y resulta que:

$$p = t \times r_0 + r$$

con $0 < r < r_0$ (r no puede ser cero pues p es primo y $1 < r_0 < p$). Por lo tanto:

$$\begin{aligned} r_0 &= a \times n - b \times p && (1)\\ t \times r_0 &= t \times a \times n - t \times b \times p && (2)\\ t \times r_0 + r &= t \times a \times n - t \times b \times p + r && (3)\\ p &= t \times a \times n - t \times b \times p + r && (4) \end{aligned}$$

Sumando las igualdades (1) y (4) obtenemos que:

$$r_0 + p = a \times n - b \times p + t \times a \times n - t \times b \times p + r$$

y, por lo tanto,

$$r_0 - r = a \times (t+1) \times n - (\, b \times t + b + 1\,) \times p$$

Esto es una contradicción pues hemos escrito el número $r_0 - r$ como diferencia de un múltiplo de n y un múltiplo de p a pesar de que r_0 era el menor con esta propiedad.

2.-Supongamos que $m \times n$ es múltiplo de p. Si m es múltiplo de p ya tenemos lo que queremos probar. Si m no es múltiplo de p usamos la parte 1.- del teorema y obtenemos que hay números a y b tales que:

$$a \times m - b \times p = 1.$$

Multiplicamos ambos miembros por n y obtenemos:

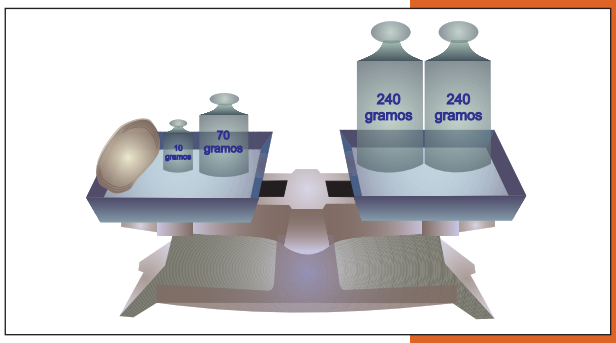
$$a \times m \times n - b \times p \times n = n$$

lo que expresa a n como resta de dos múltiplos de p (recordar que por hipótesis $m \times n$ es múltiplo de p). Por lo tanto n es múltiplo de p.

Para resolver

1.11 Expresar el 1 como resta de un múltiplo de 42 menos un múltiplo de 11.

1.12 En una balanza de platillos hay una pesa de 10 g en un platillo. ¿Cómo se puede hacer para equilibrar la balanza con pesas de 240 g y 70 g?



1.13 ¿Es posible expresar el 1 como resta de un múltiplo de 11 menos un múltiplo de 42? ¿Y cómo resta de un múltiplo de 7 menos un múltiplo de 18?

1.14 Demostrar que se puede invertir el orden de la resta en el teorema anterior, es decir que si n no es múltiplo de p (p primo) entonces existen números naturales a y b tales que $b \times p - a \times n = 1$, es decir que hay un múltiplo de p y un múltiplo de n que restados dan 1.

1.4.3. Tercera propiedad

Demostremos la respuesta a la **pregunta 5**.

Teorema de la unicidad de la factorización en primos. Todo número natural tiene una **única** factorización en primos.

Demostración.

Supongamos que hay números que se pueden factorear de dos formas distintas como producto de números primos, y llamemos n_0 el menor de todos esos números.

Tenemos así que:

$$n_0 = p_1 \times p_2 \times \ldots \times p_r = q_1 \times q_2 \times \ldots \times q_s$$

Como $n_0 = q_1 \times q_2 \times \ldots \times q_s$ es múltiplo de p_1, la parte (2) del teorema que se probó antes dice que p_1 debe ser divisor de alguno de los q_j y como todos los q_j son primos la única forma de que p_1 sea divisor de q_j es que $p_1 = q_j$. Entonces, se puede simplificar p_1 con q_j en la igualdad de arriba y obtener que $\frac{n_0}{p_1}$ es un número menor que n_0 y con dos formas distintas de ser factoreado como producto de números primos, lo que contradice el hecho que n_0 era el menor posible con esta propiedad.

Para acentuar la atención sobre la relevancia del teorema que acabamos de demostrar, veamos como ejemplo, el factoreo del número 101.599.344.

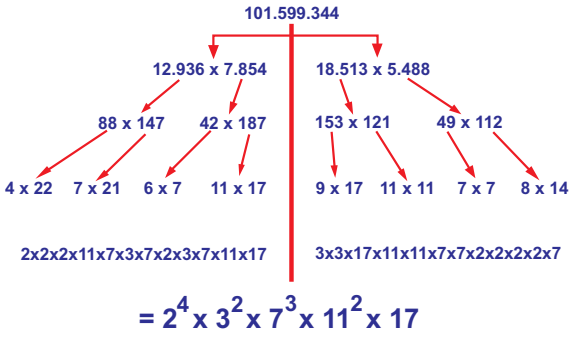


Figura 1.10 Dos caminos para el factoreo del número 101.599.344

Comencemos por dos caminos diferentes: (**Figura 1.10**)

$$101.599.344 = 12.936 \times 7.854$$
$$101.599.344 = 18.513 \times 5.488$$

Luego seguimos por cada camino factoreando. En la cuarta fila del proceso de factorización, se empiezan a ver algunos números primos pero todavía quedan algunos compuestos. En esta cuarta fila, los números de la izquierda no lucen muy parecidos a los de la derecha, dando la impresión de que existe la posibilidad de terminar con dos factorizaciones en primos diferentes entre sí. Sin embargo, si hacemos un paso más factoreando los números compuestos de la cuarta fila resulta que, tanto por el camino de la izquierda como por el de la derecha, obtenemos los mismos números primos, tal cual afirma el teorema.

1.4.4. Cuarta propiedad

Cerramos esta sección con el teorema que responde a la **pregunta 6.**

Teorema de la cantidad de primos. Existen infinitos números primos. Es decir, dada una lista con cierta cantidad finita de números primos es posible encontrar un número primo que no esté en la lista. En particular, hay números primos tan grandes como uno quiera.

La demostración de este teorema es constructiva. Significa que da un método para encontrar un primo que no esté en una lista de primos que tengamos. Funciona de la siguiente manera. Busquemos un primo que no esté en esta lista:

$$2, 3, 5, 7, 11, 13.$$

Construyamos el número que resulta de multiplicar a todos los de la lista y sumar 1, es decir:

$$n = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30.031$$

Ahora factoreamos el número n y obtenemos $n = 59 \times 509$. Observamos dos números primos que no teníamos. En resumen este es el método para encontrar un primo que no esté en una lista que tengamos:

1.- multiplicar los primos de la lista entre sí,
2.- sumarle al resultado 1,
3.- factorear el nuevo resultado,

Para hacer la demostración del teorema enunciado es necesario probar que este método **siempre** produce números primos que no estaban en la lista.

Demostración. Supongamos que la lista de primos es $p_1, p_2, \ldots, p_n$. Construyamos:

$$n = p_1 \times p_2 \times ... \times p_n + 1$$

y factoricemos n como producto de números primos. Elijamos alguno de los primos obtenidos al cual llamaremos p. Afirmamos que p no es ninguno de los p_j que teníamos. Si p fuera alguno de ellos tendríamos que tanto n como $p_1 \times p_2 \times ... \times p_n$ serían divisibles por p, y por lo tanto su resta sería divisible por p, lo cual es imposible, pues la resta da 1 y 1 no es divisible por ningún número primo.

Imaginemos que comenzamos sólo con los primos 2 y 3, y vayamos aplicando el método para ver qué nuevos primos van apareciendo.

Tenemos: 2, 3.
1. Multiplicamos: 6.
2. Sumamos 1: 7.
3. Factoreamos: 7.

Tenemos: 2, 3, 7.
1. Multiplicamos: 42.
2. Sumamos 1: 43.
3. Factoreamos: 43.

Tenemos: 2, 3, 7, 43.
1. Multiplicamos: 1.806.
2. Sumamos 1: 1.807.
3. Factoreamos: 13 × 139.

Tenemos: 2, 3, 7, 13, 43, 139.
1. Multiplicamos: 3.263.442.
2. Sumamos 1: 3.263.443.
3. Factoreamos: 3.263.443. (¡Hace falta mucho trabajo para verificar que 3.263.443 es primo!)

Tenemos: 2, 3, 7, 13, 43, 139, 3.263.443.

Vemos que los primos que van apareciendo son enormes. El próximo paso requiere factorear el número 10.650.056.950.807, ¿quién se anima? También observamos que pareciera que no aparecen todos los primos, ¿obtendremos todos los primos si seguimos?

Para resolver

1.15 Repetir los primeros pasos del procedimiento anterior de fabricación de primos, pero comenzando con los primos 2, 3 y 5.

1.16 Demostrar que nunca obtendremos el número primo 5 si continuamos el proceso de fabricación de primos que hicimos más arriba empezando con el 2 y el 3. (Ayuda, mirar en qué terminan los números obtenidos luego de sumar 1: 7, 43, 1.807, 3.263.443, etc.)

□ 1.5 ¿Cómo se determinan los factores primos de un número dado?

En esta sección discutiremos la **pregunta 7** de la **Sección 2**. ¿Cómo encontrar los factores primos de un número dado? Ya comentamos que es muy difícil si el número que queremos factorear es grande.

Para entrar en calor hagamos un pequeño paseo por la química. Los siguientes datos han sido extraídos de los sitios http://es.wikipedia.org/wiki/Tierra, http://es.wikipedia.org/wiki/Sol. Sabemos, por ejemplo, cómo está compuesta nuestra Tierra y nuestra atmósfera.

Composición de la atmósfera terrestre

Nitrógeno	78,08%
Oxígeno	20,95%
Argón	0,93%

Composición de la Tierra

Hierro	34,6%
Oxígeno	29,54%
Silicio	15,2%
Magnesio	12,7%
Níquel	2,4%
Azufre	1,9%

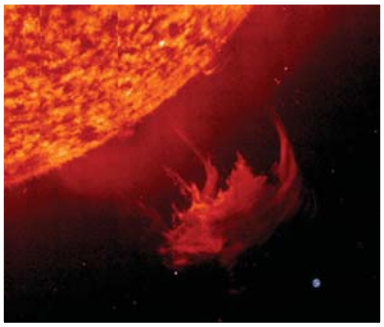


Figura 1.11 Foto del Sol de la NASA en la cual se ha incorporado a la Tierra en tamaño relativo

Figura 1.12 Foto de nuestra atmósfera con la Luna de fondo.

Con mayor asombro podemos ver que hemos podido determinar la composición química de la fotosfera del Sol. A la derecha vemos una hermosa foto del Sol de la NASA en la cual se ha incorporado a la Tierra en tamaño relativo (**Figura 1.11**) y arriba a la izquierda tenemos una foto de nuestra atmósfera con la Luna de fondo (**Figura 1.12**).

Composición de la fotosfera del Sol			
Hidrógeno	73,46%	Neón	0,12%
Helio	24,85%	Nitrógeno	0,09%
Oxígeno	0,77%	Silicio	0,07%
Carbono	0,29%	Magnesio	0,05%
Hierro	0,16%	Azufre	0,04%

Para completar el asombro de lo que es capaz el ser humano, se conoce que la estrella 14 Herculis, que no se puede ver a simple vista, está ubicada a 59 años luz de la Tierra y tiene planetas girando en su órbita. Además sabemos que comparada con el Sol, tiene un tamaño aproximadamente igual al 80% pero tiene el triple de hierro. ¡Asombroso! (ver http://es.wikipedia.org/wiki/14_Herculis y su versión en inglés) ¿Cómo hacen los científicos para descubrir cuánto hierro tiene esta invisible estrella?

Y aunque parezca mentira, es más difícil determinar los factores primos de algunos números de más de 500 cifras que encontrar la composición química de la fotosfera del Sol.

¿A quién se le ocurre querer factorear un número de más 500 cifras?

Por un lado, es parte de la maravillosa curiosidad que tiene el hombre. La misma curiosidad que lo lleva a buscar la composición química de cada estrella, o tratar de determinar la geometría de nuestro universo, o a descubrir la estructura de algún perdido ecosistema del fondo del mar, o tratar de encontrar la manera más eficiente de factoraer cada número natural. Por otro lado, un poco más práctico y menos romántico, actualmente las contraseñas de internet o números de tarjetas de crédito son trasmitidos electrónicamente con técnicas de encriptación que utilizan números tan grandes, justamente por tener la virtud de ser difíciles de factorear.

Determinar los factores primos de un número dado es difícil pues hay infinitos números primos, y a veces aparecen algunos tan grandes que ni las computadoras pueden encontrarlos.

El proceso de encontrar la factorización de un número requiere de dos tipos de pasos fundamentales. →

Pasos fundamentales para factorear un número *n*

Tipo 1. Saber determinar si un número dado es primo o compuesto. Esto sirve para saber cuándo hay que hacer pasos de Tipo 2.

Tipo 2. Saber cómo descomponer un número compuesto a como producto de dos números menores a_1 y a_2.

Con estos dos pasos podemos armar el siguiente método:

Método para factorear. Para factorear un número n hay que:

1. determinar si n es primo o compuesto (Paso tipo 1),
2. si es compuesto, escribir n como producto de dos números menores n_1 y n_2, (Paso tipo 2),
3. determinar si n_1 y n_2, son primos o compuestos (Paso tipo 1),
4. si n_1 es compuesto, escribir n_1 como producto de dos números menores n_3 y n_4, y si n_2 es compuesto escribir n_2 como producto de dos números menores n_5 y n_6, (Paso tipo 2).

Seguir haciendo lo mismo con n_3, n_4, n_5 y n_6, y así sucesivamente hasta ir encontrando los factores primos. Es decir, alternar pasos de tipo 1 y 2 hasta que sólo nos queden números primos.

Ya sabemos que es muy complicado realizar estos dos tipos de pasos. Si queremos recordar lo difícil que es podemos intentar factorear el número 62.615.533. Más abajo, revelaremos su descomposición. Por ahora tenemos una ayuda que no ayuda mucho: uno de sus factores primos es aproximadamente 8.000 y ocupa la posición número 1.000 en la lista de primos.

En contraste a lo difícil que es factorear es muy fácil multiplicar, aún si se trata de números grandes. Si quisiéramos multiplicar:

$$\begin{array}{r} 233.793.395.921.694.337 \\ \times \quad 661.194.147.491 \\ \hline \end{array}$$

no tendríamos ninguna dificultad, en menos de media hora habríamos terminado. Sin embargo, sería absolutamente imposible hallar la factorización de

154.582.825.105.470.523.344.997.458.467, que es el resultado de esa multiplicación, sin la ayuda de una computadora.

Factorear y multiplicar son procesos uno el inverso del otro, pero sucede como con el café con leche.

> Es muy fácil mezclar café y leche para preparar un café con leche, pero ante un café con leche es casi imposible separar el café de la leche.

1.5.1 ¿Cómo determinar si un número es primo y cómo encontrar dos factores de un número compuesto?

Hay una manera muy primitiva de hacer ambas cosas al mismo tiempo.

> **Método primitivo de llevar a cabo los pasos tipo 1 y tipo 2 al mismo tiempo.** Dado el número n, para saber si es primo o compuesto, y en caso de ser compuesto encontrar dos factores de él se divide n por todos los números menores que él. Si en algún momento es divisible por alguno, entonces n es compuesto y se conocen los dos factores. Si no es divisible por ninguno, entonces n es primo.

Este método es muy bueno para números pequeños, pero requiere muchísimas cuentas (y por lo tanto mucho tiempo) si el número es muy grande.

Pensemos dividir 62.615.533 por todos los números desde el 2 hasta el 62.615.533. En realidad, bastaría dividirlo por todos los números desde el 2 hasta la mitad de 62.615.533, porque de ahí en adelante la división no dará un entero. Aún así, considerar desde el 2 hasta el 31.307.766 sigue siendo una cantidad enorme. Esto se puede mejorar.

En la **Sección 3** comentamos que en el año 200 a.C. Eratóstenes hizo una observación que ayudaba a reducir la cantidad de cuentas necesarias. Él se dio cuenta de que si

$$n = n_1 \times n_2$$

entonces, n_1 o n_2 debe ser menor que la raíz cuadrada de n, porque si ambos fueran mayores que la raíz cuadrada de n, entonces el producto $n_1 \times n_2$ sería mayor que n. Esta observación nos permite la siguiente mejoría al método primitivo.

> **Método primitivo mejorado por Eratóstenes.** Dado el número n, para saber si es primo o compuesto, y en caso de ser compuesto encontrar dos factores de él se divide n por todos los números menores que su raíz cuadrada. Si en algún momento es divisible por alguno, entonces n es compuesto y se conocen dos factores. Si no es divisible por ninguno, entonces n es primo.

Entonces, para encontrar dos factores de 62.615.533 hay que probar con todos los números desde el 2 hasta el 7.913. Muchísimos menos, pero todavía demasiados. Por eso,

es casi imposible encontrar los factores de este número sin la ayuda de una computadora o de una persona muy paciente.

Eratóstenes se dio cuenta de otra cosa más. No hace falta probar dividiendo con **todos** los números desde el 2 hasta el 7.913, porque si no funcionó el 2, tampoco lo harán el 4, el 6, el 8 ni ningún número par. De igual manera, si no sirvió el 7, tampoco servirá ningún múltiplo de 7. Eratóstenes se dio cuenta de que sólo hace falta probar con **todos** los números **primos** desde el 2 hasta el 7.913. Esto simplifica la cantidad de operaciones, pero incorpora una complicación: se necesita tener (para este caso) la lista de primos menores a 8.000. Entonces inventó un método para armar una lista de primos desde el 2 hasta un número *M* dado. Este método es conocido como la **Criba de Eratóstenes**.

La **Criba de Eratóstenes** consiste en lo siguiente: se escriben los números desde el 2 hasta el *M* en una tabla cuadrada. Por ejemplo, para *M* igual a 100: →

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

El primer número negro en la primera fila es el 2, que es primo. Se lo pinta de rojo y se pintan de azul todos sus múltiplos. ↓

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Ahora el primer número negro en la primera fila es el 3, que es primo. Se lo pinta de rojo y se pintan de azul todos sus múltiplos. ↓

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Ahora el primer número negro en la primera fila es el 5, que es primo. Se lo pinta de rojo y se pintan de azul todos sus múltiplos.

←

Ahora el primer número negro que tenemos en la primera fila es el 7, que es primo. Se lo pinta de rojo y se pintan de azul todos sus múltiplos.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Obtuvimos los primos hasta el 100. Pero para factorear el 62.615.533 lo debemos dividir por los primos hasta el 7.913. Redondeando, necesitaríamos la lista de primos hasta el 10.000. Vemos en la **figura 1.13** la Criba de Eratóstenes hasta el número 10.201, cuya raíz cuadrada es 101.

No queda ningún número negro en la primera fila. En las otras filas sí hay números negros, pero no son divisibles por ningún número menor que su raíz cuadrada, porque no son múltiplos de los de la primera fila. Por lo tanto todos los negros que quedan son primos y se pintan de rojo.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

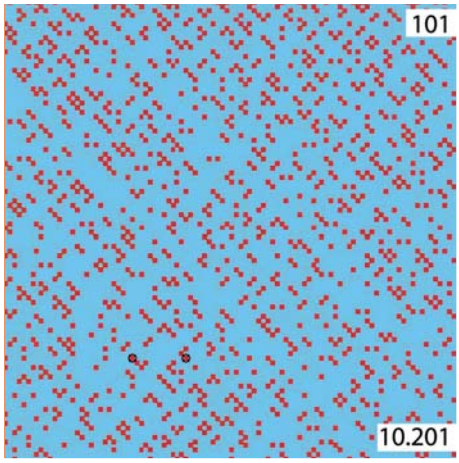


Figura 1.13 Criba de Eratóstenes hasta el número 10.201, cuya raíz cuadrada es 101.

En este caso quedan 1.252 números primos para intentar dividir el 62.615.533, que es mucho menos que las 7.913 divisiones que dijimos antes, pero sigue siendo mucho. A esta altura, es bueno saber que

$$62.615.533 = 7.907 \times 7.919$$

Los primos 7.907 y 7.919 están destacados en la figura con círculos negros.

La Criba de Eratóstenes fue una buena idea, pero es claro que para factorear números de más de ocho dígitos hacen falta tantos pasos que sólo una computadora puede lograrlo.

¡El tema es más grave todavía! Porque utilizando como herramienta la Criba de Eratóstenes las computadoras de hoy no pueden factorear números de más de 70 cifras. ¡Hace falta algo mejor que la Criba de Eratóstenes para llegar a 500 cifras!

Debido a la gran importancia que tiene saber factorear los números enteros y a la gran cantidad de cuentas que requiere la Criba de Eratóstenes, los científicos siguen trabajando hasta el día de hoy en la búsqueda de métodos para factorear que requieran la menor cantidad de operaciones posibles.

¿Qué sería lo ideal? Sería encontrar un método para factorear tal que la cantidad de operaciones requerida sea lo más cercana posible a la **cantidad de cifras del número**. Hoy se conocen buenos métodos de factoreo, pero para nada se está cerca de encontrar uno que requiera una cantidad de operaciones parecida a la cantidad de cifras del número.

Comparemos

Para factorear el 62.615.533 con la Criba de Eratóstenes se requieren más de 1.000 divisiones, y lo que los científicos buscan es un método que requiera cerca de 8 operaciones.

Para factorear el 123456789123456789123456789123456789123456789123456789123456789123456789123456789123456789123456789123456789123456789

(que tiene 99 cifras) se requieren más de 1.000.000.000 operaciones con la Criba de Eratóstenes, y lo que los científicos buscan es un método que requiera cerca de 99 operaciones.

Criba de Eratóstenes hasta el número 1.000.

La Criba de Eratóstenes es un clásico de la aritmética y a pesar de que es lenta, hasta los artistas son seducidos por ella.

1.5.2. Un poco de historia más reciente

A pesar de que la Criba de Eratóstenes trata las dos preguntas ¿cómo determinar si un número dado es primo o compuesto? y ¿cómo expresar un número compuesto a como producto de dos números menores a_1 y a_2?, los matemáticos, desde el Renacimiento, tratan cada una por separado, y los progresos que se han hecho hasta hoy son diferentes para cada una de ellas.

Johann Carl Friedrich Gauss
1777 - 1855

En los siglos XVII y XVIII los matemáticos que trabajaban en estas preguntas estaban centralmente preocupados por encontrar fórmulas que dieran números primos (ver más detalles en la **Sección 1.6**).

En el año 1801, el príncipe de la matemática Carl Friedrich Gauss con sólo 21 años, escribió el libro *Disquisitiones Arithmeticae*, y declaró:

"El problema de distinguir números primos de compuestos, y el problema de hallarle a estos últimos sus factores primos, es conocido por ser uno de los más importantes y útiles en aritmética... Es más, la dignidad de la ciencia misma parece exigir que todos los caminos posibles sean analizados a fin de obtener la solución de un problema tan elegante y tan renombrado."

Durante el siglo XIX hubo progresos muy importantes en relación con la distribución

de los números primos. Los discutiremos en la **Sección 6.**

Con estos avances y con la aparición de las primeras calculadoras y computadoras, el hombre comenzó a desarrollar métodos mejores que la Criba de Eratóstenes. Se necesitaron más de 2.000 años para superarla.

En 1975 el Prof. Vaughan Pratt, Profesor Emérito de la Universidad de Stanford, establece un primer paso hacia el desarrollo de un método rápido para determinar si un número es primo. Su método estaba basado en el pequeño teorema de Fermat.

A partir de entonces, se lograron muy buenos métodos para determinar si un número es primo (no para factorear números compuestos). Los más destacados son:

- Los algoritmos de Miller–Rabin y de Solovay–Strassen. Ambos aparecen entre la década del 70 y del 80 y han sido perfeccionados muchas veces. Ambos métodos son muy rápidos: requieren una cantidad de cuentas de orden de la cantidad de cifras al cubo. Esto es 1.000.000 cuentas en un número de 100 cifras. ¡Bastante bien! Pero tienen un defecto: no son exactos, es decir contestan si un número es primo o compuesto **con un ínfimo margen de error teórico**. Estos son los algoritmos que actualmente se utilizan en la práctica y contestan acertadamente a gran velocidad.

- En 1983, Adleman, Pomerance, y Rumely consiguen un método con 100% de certeza, que utiliza la siguiente cantidad de cuentas: en un número n que tenga K cifras, la cantidad de cuentas es $K^{\ln(\ln(K))}$. Esto es 1.200 cuentas en un número de 100 cifras.

- En 2002 los científicos indios Manindra Agrawal, Neeraj Kayal, y Nitin Saxena consiguen el extraordinario logro de desarrollar un algoritmo con el 100% de certeza y que requiere la siguiente cantidad de cuentas: en un número n que tenga K cifras, la cantidad de cuentas es K^6. Esto no es mejor que el método Adleman, Pomerance, y Rumely en números de 100 cifras, pero sí lo es para números de más de 10^{180} cifras. Este algoritmo no es muy eficiente en la práctica, pero tiene destacada virtud teórica de tener 100% de certeza y de requerir una cantidad de cuentas que es polinomial en la cantidad de cifras.

La contracara es que, lamentablemente, no hay muchos avances en dar un algoritmo que utilice pocas cuentas para factorear un número compuesto. Actualmente, uno de los mejores métodos es conocido como la **Criba en cuerpos de números generales**. Este método requiere para factorear un número n de K cifras, aproximadamente la siguiente cantidad de cuentas:

$$3^{2\times\sqrt[3]{K}\times\sqrt[3]{(\ln K)^2}}$$

Comparado con la Criba de Eratóstenes tenemos:

Cifras	10	100	1.000	10.000
Cuentas en la Criba de Eratóstenes (aprox.)	5.000	10^{50}	10^{500}	$10^{5.000}$
Cuentas en la Criba en cuerpos de números generales (aprox.)	3.800	10^{13}	10^{35}	10^{91}

1.5.3. La computadora en acción

Hay programas de computación que factorean todos los números de menos de 30 cifras en un abrir y cerrar de ojos. Sin embargo, para números más grandes hasta las mejores computadoras tienen problemas.

Analicemos, por ejemplo, los siguientes números:

$a1$ = 12.345.678.910;
$a2$ = 1.234.567.891.011.121.314.151.617.181.920;
$a3$ = 123.456.789.101.112.131.415.161.718.192.021.
222.324.252.627.282.930;
$a4$ = 12.345.678.910.111.213.141.516.171.819.202.122.
232.425.262.728.293.031.323.334.353.637.383.
940;
$a5$ = 1.234.567.891.011.121.314.151.617.181.920.212.
223.242.526.272.829.303.132.333.435.363.738.
394.041.424.344.454.647.484.950

Son números (naturales) que resultan de escribir, uno detrás de otro sin separación de comas, los números naturales.

El número $a1$ es 12.345.678.910 tiene 11 cifras y se lee en castellano doce mil trescientos cuarenta y cinco millones seiscientos setenta y ocho mil novecientos diez.

Una computadora de las que actuamente se venden al público en general, no tarda nada en darnos la factorización de los dos primeros números:

$a1$ = 12.345.678.910
= 2 × 5 × 1.234.567.891
$a2$ = 1.234.567.891.011.121.314.151.617.181.920
= 2^5 × 3 × 5 × 323.339 × 3.347.983 ×
× 2.375.923.237.887.317

Ya que estamos con tantos números, hagamos un pequeño recreo y veamos algo de castellano como para juntar fuerzas y seguir adelante.

El a2 es **1.234.567.891.011.121.314.151.617.181.920**, tiene 31 cifras y creemos que se lee así:

Un millón doscientos treinta y cuatro mil quinientos sesenta y siete cuatrillones, ochocientos noventa y un mil once trillones, ciento veintiún mil trescientos catorce billones, ciento cincuenta y un mil seiscientos diecisiete millones, ciento ochenta y un mil novecientos veinte.

Recordamos que según el diccionario de la Real Academia Española, un billón es un millón de millones, un trillón es un millón de billones, un cuatrillón es un millón de trillones. Hasta donde pudimos averiguar, quintillón es una palabra que no existe en el diccionario de la Real Academia Española. Si existiera, correspondería a un millón de cuatrillones. Si aceptáramos usar la palabra quintillón, la primera línea de arriba podría ser reemplazada por

Un quintillón, doscientos treinta y cuatro mil quinientos sesenta y siete cuatrillones, ...

En la página **http://latecladeescape.com/w0/recetas-algoritmicas/escribir-numeros-con-letras.html** uno puede escribir un número de hasta 30 cifras y el sitio responde cómo se lee en castellano.

Reflexionemos sobre la dificultad de los pasos realizados para obtener esta factorización.

Para $a1$:
Paso tipo 2: $a1$ es 2 × 6.172.839.455 (sencillo).
Paso tipo 1: 2 es primo (sencillo).
Paso tipo 2: 6.172.839.455 es 5 × 1.234.567.891 (sencillo porque termina en 5).
Paso tipo 1: 5 es primo (sencillo).
Paso tipo 1: 1.234.567.891 es primo (bastante difícil).

Para *a*2:
Paso tipo 2: *a*2 es 2 × 617.283.945.505.560.657.075.808.590.960 (sencillo).
Paso tipo 1: 2 es primo (sencillo).
Paso tipo 2: 617.283.945.505.560.657.075.808.590.960 es 2 ×
× 308.641.972.752.780.328.537.904.295.480 (sencillo).
Paso tipo 2: 308.641.972.752.780.328.537.904.295.480 es 2 ×
× 154.320.986.376.390.164.268.952.147.740 (sencillo).
Paso tipo 2: 154.320.986.376.390.164.268.952.147.740 es 2 ×
× 77.160.493.188.195.082.134.476.073.870 (sencillo).
Paso tipo 2: 77.160.493.188.195.082.134.476.073.870 es 2 ×
× 38.580.246.594.097.541.067.238.036.935 (sencillo).
Paso tipo 2: 38.580.246.594.097.541.067.238.036.935 es 5 ×
× 7.716.049.318.819.508.213.447.607.387 (sencillo).
Paso tipo 1: 5 es primo (sencillo).
Paso tipo 2: 7.716.049.318.819.508.213.447.607.38 es 3 ×
× 2.572.016.439.606.502.737.815.869.129 (sencillo porque sus dígitos suman un múltiplo de 3, recordar que un número es divisible por 3 si y sólo si sus dígitos suman un múltiplo de 3).
Paso tipo 1: es primo (sencillo).
Paso tipo 2: 2.572.016.439.606.502.737.815.869 es 323.339 ×
× 7.954.550.609.751.693.231.611 (muy difícil, ¡sólo una computadora!).
Paso tipo 1: 323.339 es primo (difícil, no tan difícil).
Paso tipo 2: 7.954.550.609.751.693.231.611 es 3.347.983 × 2.375.923.237.887.317 ×
(muy difícil, ¡sólo una computadora!).
Paso tipo 1: 3.347.983 es primo (bastante difícil).
Paso tipo 1: 2.375.923.237.887.317 es primo (muy difícil, ¡sólo una computadora!).
Todos estos pasos fueron dados por la computadora en forma casi instantánea.

Sin embargo, la computadora tardó 30 segundos en encontrar la factorización de:

*a*3 = 123.456.789.101.112.131.415.161.718.192.021.222.324.252.627.282.930
= 2 × 3 × 5 × 13 × 49.269.439 × 370.677.592.383.442.753 ×
× 17.333.107.067.824.345.178.861

Tardó 80 segundos en encontrar la factorización de:

*a*4 = 12.345.678.910.111.213.141.516.171.819.202.122.232.425.262.728.293.031.
323.334.353.637.383.940
= 2 × 5 × 3.169 × 60.757 × 579.779 × 4.362.289.433 × 79.501.124.416.220.680.469 ×
× 15.944.694.111.943.672.435.829.023

Tardó 8 minutos en encontrar la factorización de:

*a*5 = 1.234.567.891.011.121.314.151.617.181.920.212.223.242.526.272.829.303.
132.333.435.36 3.738.394.041.424.344.454.647.484.950;
= 2×3×5×13×211×20.479×160.189.818.494.829.241×46.218.039.785.302.111.919 ×
× 19.789.860.528.346.995.527.543.912.534.464.764.790.909.391.

A la computadora le costó mucho más trabajo el a5, no por ser más grande que a4, sino porque aparecen primos muy grandes en su factorización: uno de 18 cifras, otro de 20 y el mayor de 44.

Para *a*6 = 123.456.789.101.112.131.415.161.718.192.021.222.324.252.627.282.930.313.233.343.536.373.839.404.142.434.445.464.748.495.051.525.354.555.657.585.960; (que tiene 111 cifras), después de más de media hora procesando, la computadora se colgó.

Si bien es muy difícil factorear los números a1,a2,a3,a4,a5 y a6, al menos ellos tienen la ventaja de terminar en cero lo cual implica que son divisibles por 2 y por 5 y esto ayuda a que sea sencillo empezar a factorearlos. ¿Qué pasaría entonces si pedimos a la computadora que halle la factorización de los siguientes números?

*b*1 = 123.456.789;
*b*2 = 12.345.678.910.111.213.141.516.171.819;
*b*3 = 1.234.567.891.011.121.314.151.617.181.920.212.223.242.526.272.829;
*b*4 = 123.456.789.101.112.131.415.161.718.192.021.222.324.252.627.282.930.313.233.343.536.373.839;
*b*5 = 12.345.678.910.111.213.141.516.171.819.202.122.232.425.262.728.293.031.323.334.353.637.383.940.414.243.444.546.474.849;

Sabemos que estos números están armados del mismo modo que los anteriores, sólo que terminan un par de dígitos antes.

El resultado es el siguiente:

*b*1 = 123.456.789 = 3 × 3.607 × 3.803, instantáneo;
*b*2 = 12.345.678.910.111.213.141.516.171.819 = 13 × 43 × 79 × 281 × 1193 × × 833.929.457.045.867.563, instantáneo;
*b*3 = 1.234.567.891.011.121.314.151.617.181.920.212.223.242.526.272.829
= 3 × 859 × 24.526.282.862.310.130.729 × 19.532.994.432.886.141.889.218.213; 80 segundos;
*b*4 = 123.456.789.101.112.131.415.161.718.192.021.222.324.252.627.282.930.313.233.343.536.373.839;
= 3 × 67 × 311 × 103.9 × 6.216.157.781.332.031.799.688.469 × × 305.788.363.093.026.251.381.516.836.994.235.539, más de una hora.

No pudo factorear *b*5.

□ 1.6. ¿Cuáles son todos los números primos?

Es una pregunta muy interesante porque los primos son infinitos y, por lo tanto, no hay una tabla que los contenga a todos.

Veamos algunas variantes de la misma pregunta.
Entre los números naturales, ¿qué porcentaje corresponde a los números primos?

Terence Tao, quien obtuvo la medalla Fields (equivalente a Premio Nobel de Matemática) en 2006.

¿Hay una fórmula que dé todos o algunos números primos?
¿Cuáles son todos los números primos *conocidos*?

Vimos que dos siglos a.C. se sabía que había infinitos primos, pero recién a fines del siglo XVI comenzó un trabajo sistemático por encontrar respuestas a estas preguntas.

Fórmulas que dan primos.

Ante la imposibilidad de tener una lista con todos los primos, uno de los objetivos centrales de los científicos del renacimiento era encontrar una fórmula que los produjera. Así como la fórmula $2n$ da todos los números pares, los matemáticos querían una fórmula parecida que diera todos, o al menos algunos, números primos.

Ya contamos que aproximadamente en el año 1630 Fermat descubrió que $2^{2^n}+1$ era primo para $n = 1, 2, 3$ y 4 y tenía la esperanza de que, cualquiera sea el número n, siempre sucediera que $2^{2^n}+1$ sea primo. Más tarde, en el año 1732, Leonard Euler descubrió que para $n = 5$, el número $2^{2^n}+1$ es $4.294.967.297 = 641 \times 6.700.417$.

Algunos años más tarde Euler descubrió que la fórmula $n^2 - n + 41$ daba primo para $n = 1, 2, 3, \ldots, 39$. Los primos que van apareciendo son 41, 43, 47, 53, 61, 71, ...

Lamentablemente para $n = 40$, la fórmula $n^2 - n + 41$ da $1.681 = 41 \times 41$.

Hoy se sabe que no puede haber ninguna fórmula polinomial en n que dé primo para todo n. Sin embargo, los científicos no se rinden. En 1947, el Prof. W. H. Mills demuestra que existe un número real A, que aproximadamente es 1,3063 tal que si tomamos la parte entera de A^{3n} da primo para todo n. Lamentablemente, el número A no se conoce con precisión, ni siquiera se sabe si es racional o no, lo que hace que probablemente esta fórmula no sea muy útil.

En el año 2004, los profesores Ben Green y Terence Tao descubren que dado cualquier número K existen números a y b tales que la fórmula $a \times n + b$ da primo para todo n desde 1 a K.

En 2008 Jens Andersen encuentra el a y b que sirven para $K = 25$, demostrando que

$$81.737.658.082.080 \times n + 6.089.317.254.750.551$$

es primo para todo n desde 1 a 25.

Densidad de los números primos.

Los números primos son infinitos y la siguiente tabla muestra cuántos primos hay entre 1 y N. En matemática esta cantidad se llama $\pi(N)$. También mostramos en la tabla el valor de $P(N) = N / \ln(N)$ donde $\ln(N)$ es el logaritmo natural de N. En ella podemos ver que la función $P(\mathrm{N})$ aproxima muy bien a $\pi(N)$. En la cuarta columna se muestra el

porcentaje de error con el que $P(N)$ aproxima a $\pi(N)$.

N	π (N) = cantidad de primos ente 1 y N	% de números primos sobre el total de números	P(N) = N / ln (N)	% de error entre P(N) y π (N)
10	4	40%	4,34	-7,90%
10^2	25	25%	21,71	15,13%
10^3	168	16.8%	144,76	16,05%
10^4	1.229	12.29%	1.085,74	13,20%
10^5	9.592	9.59%	8.685,89	10,43%
10^6	78.498	7.85%	72.382,41	8,45%
10^7	664.579	6.65%	620.420,69	7,12%
10^8	5.761.455	5.76%	5.428.681,03	6,13%
10^9	50.847.534	5.08%	48.254.942,50	5,37%
10^{10}	455.052.511	4.55%	434.294.482,47	4,78%
10^{11}	4.118.054.813	4.12%	3.948.131.658,80	4,30%
10^{12}	37.607.912.018	3.76%	36.191.206.872,33	3,91%
10^{13}	346.065.536.839	3.46%	334.072.678.821,51	3,59%
10^{14}	3.204.941.750.802	3.2%	3.102.103.446.199,74	3,32%
10^{15}	29.844.570.422.669	2.98%	28.952.965.497.864,30	3,08%
10^{16}	279.238.341.033.925	2.79%	271.434.051.542.477,00	2,88%
10^{17}	2.623.557.157.654.230	2.62%	2.554.673.426.282.140,00	2,70%
10^{18}	24.739.954.287.740.800	2.47%	24.127.471.248.220.200,00	2,54%
10^{19}	234.057.667.276.344.000	2.34%	228.576.043.404.192.000,00	2,40%
10^{20}	2.220.819.602.560.910.000	2.22%	2.171.472.412.339.820.000,00	2,27%
10^{21}	21.127.269.486.018.700.000	2.11%	20.680.689.641.331.600.000,00	2,16%
10^{22}	201.467.286.689.315.000.000	2.01%	197.406.582.939.984.000.000,00	2,06%
10^{23}	1.925.320.391.606.800.000.000	1.93%	1.888.236.880.295.490.000.000,00	1,96%

Para la matemática del siglo XIX fue muy importante descubrir que $P(N) = N / \ln(N)$ aproxima tan bien a $\pi(N)$, porque la verdad es que la quinta columna, la del porcentaje de error, tiende a cero. Esta verdad se conoce como **Teorema de los números primos**.

Adrien-Marie Legendre 1752 - 1833

Gauss y Legendre fueron quienes descubrieron este teorema aunque no lograron demostrar que la quinta columna tiende a cero. Es admirable que en esa época, sin computadoras que calcularan con precisión el valor de $\pi(N)$, observaran que la función que cuenta los números primos está relacionada con los logaritmos naturales. ¡Qué asombroso es que haya una relación entre los números primos y el número e = 2,718281... que es la base de los logaritmos naturales!

En el año 1896, Hadamard y de la Vallée Poussin logran demostrar el Teorema de los números primos, es decir que el porcentaje de error tiende a cero. Su demostración utiliza unos resultados que Riemann había probado sobre la famosa función:

Baron de la Vallée Poussin
1866 - 1962

Jacques Salomon Hadamard
1865 - 1963

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod \frac{1}{1 - p^{-s}}$$

que hoy se conoce como la función Zeta de Riemann. Esta función muestra que los números primos, además de estar emparentados con el número e = 2,718281... también lo están con el número π = 3,14159..., porque

$$\prod_{\substack{p \\ \text{primo}}} \frac{1}{1 - p^{-2}} = \frac{1}{1 - 2^{-2}} \times \frac{1}{1 - 3^{-2}} \times \frac{1}{1 - 5^{-2}} \times \frac{1}{1 - 7^{-2}} \times \ldots = \frac{\pi^2}{6}$$

Los primos, ¿son muchos o pocos?

Los indicios que tenemos no se ponen de acuerdo.

- Por un lado son infinitos.
- Por otro lado, entre 1 y N, hay aproximadamente $P(N) = N / \ln(N)$. Es decir que aproximadamente el porcentaje de primos entre 1 y N= $\frac{100}{\ln(N)}$ %, cantidad que se acerca a cero a medida que N crece. Por lo tanto, porcentualmente los primos son muy pocos.
- Sin embargo, Euler demostró que si uno suma los inversos de **todos los primos**, la suma da infinito.

$$\sum_{\substack{p \text{ recorre} \\ \textbf{todos} \text{ los primos}}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \cdots = \infty$$

El hecho de que esta suma dé infinito indica que son realmente muchos, teniendo en cuenta por ejemplo, que esta otra suma da 1.

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{32} + \frac{1}{64} + \cdots = 1$$

- Sin embargo, se conocen muy pocos primos. A tal punto que si uno suma los inversos de todos los primos que el ser humano conoce, la suma no alcanza a dar más que 5.

$$\sum_{\substack{p \text{ recorre} \\ \textbf{todos} \text{ los primos} \\ \textbf{conocidos}}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \cdots \leq 5$$

Mayores primos conocidos.

En 1588 Pietro Cataldi verificó correctamente que los siguientes dos números

$$2^{17} - 1 = 131.071 \text{ y } 2^{19} - 1 = 524.287$$

eran primos. Se cree que en esa época marcaron un récord en la búsqueda de números primos grandes. Para valorar debidamente el logro de Cataldi sería una buena idea invertir cierto tiempo intentando encontrar un número primo mayor que 524.287, aún utilizando calculadora o computadora (que Cataldi no tenía).


Marin Mersenne 1588 - 1648

En la misma época, el monje Marin Mersenne decide estudiar en profundidad los números de la forma $2^p - 1$ con p primo, y ver cuáles de ellos dan primos.

Por ejemplo:

$2^2 - 1 = 3$ es primo,
$2^3 - 1 = 7$ es primo,
$2^5 - 1 = 31$ es primo,
$2^7 - 1 = 127$ es primo,
$2^{11} - 1 = 2.047 = 23 \times 89$ es compuesto,
$2^{13} - 1 = 8.191$ es primo.

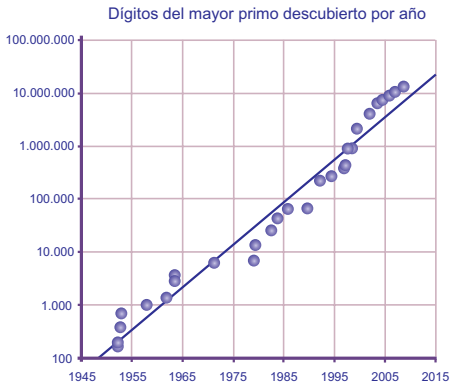
Los primos que se obtienen con la fórmula $2^p - 1$, con p primo, se conocen como primos de Mersenne. En el año 1856 Édouard Lucas descubre un método muy rápido para determinar si $2^p - 1$ es primo o compuesto. Desde entonces y hasta hoy, han sido la principal fuente de récord para primos grandes. A continuación, presentamos una tabla que contiene los números primos que, a lo largo del tiempo fueron marcando un nuevo récord en la búsqueda de primos grandes antes de la aparición de las computadoras.

Destacados récord antes de las computadoras			
Número	Dígitos	Año	Autor
$2^{17} - 1 = 131.071$	6	1588	Cataldi
$2^{19} - 1 = 524.287$	6	1588	Cataldi
$2^{31} - 1 = 2.147.483.647$	10	1772	Euler
$(2^{59} - 1) / 179951 = 3.203.431.780.337$	13	1867	Landry
$2^{127} - 1 = 170.141.183.460.469.231.731.687.303.715.884.105.727$	39	1876	Lucas
$(2^{148} - 1) / 17 = 20.988.936.657.440.586.486.151.264.256.610.222.593.863.921$	44	1951	Ferrier

En la actualidad, todos estos primos se detectan al instante con la ayuda de una computadora. Ferrier utilizó una calculadora de escritorio para demostrar que $(2^{148} - 1) / 17$ era primo. En el mismo año Miller & Wheeler demostraron, con el uso de computadoras, que el siguiente número de 79 cifras es primo.

$$180 \times (2^{127} - 1)^2 + 1 = 5.210.644.015.679.228.794.060.694.325.390.955.853.335.$$
$$898.483.908.056.458.352.183.851.018.372.555.735.221$$

Todos estos fueron resultados muy celebrados. Con la aparición de las computadoras la historia siguió un curso vertiginoso. En 1996 se puso en marcha el proyecto GIMPS, Great Internet Mersenne Prime Search, (Gran búsqueda de primos de Mersenne por Internet) en el que se invita al público que navega por Internet a compartir sus recursos informáticos para hallar el nuevo récord. A la derecha vemos la evolución que hasta la fecha tuvieron



los récords. En agosto de 2008 el proyecto GIMPS, liderado por el Prof. de Matemática Edson Smith de la Universidad de California en Los Angeles, obtuvo el primer primo de más de 10 millones de cifras. Al mes siguiente, el ingeniero electrónico Hans-Michael Elvenich de Alemania, obtuvo el segundo. Ellos son respectivamente:

$$2^{43.112.609} - 1 \text{ y } 2^{32.582.657} - 1$$

Cada uno de ellos ocuparía 2.000 páginas si los escribimos en letra de 10pt. La fundación Electronic Frontier Foundation ofrecía desde hacía más de 10 años un premio de U$D 100.000 a quienes obtuvieran el primer primo de más de 10 millones de cifras.

Lo que no se sabe todavía sobre los números primos.

Una de las grandes preguntas que todavía no tienen respuesta es ¿de qué manera están distribuidos los primos? Más precisamente: *¿hay algún tipo de patrón que respeten los primos o realmente están distribuidos aleatoriamente?*

Para entender mejor la pregunta, miremos las siguientes imágenes e intentemos descubrir alguna regularidad que cumplan los puntos rojos.

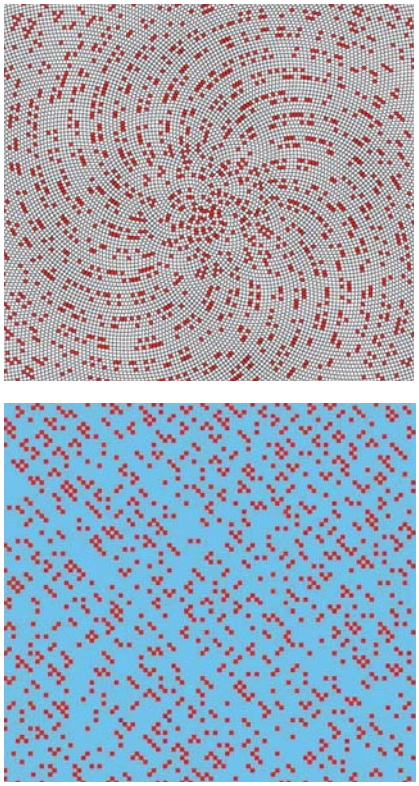


Figura 1.14 Abajo: primos menores que 10.201 distribuidos en un cuadrado de lado 101. Arriba: imagen extraída del la página web del Prof. Mark Dickinson (www.pitt.edu/~dickinsm/), del Dto. de Matemática de la Universidad de Pittsburg, se distribuyeron los primos en un esquema de flor de girasol.

Ambas muestran los primos pintados de rojo (**Figura 1.14**). En la primera están los primos menores que 10.201 distribuidos en un cuadrado de lado 101. La segunda figura es una imagen extraída del la página web del Prof. Mark Dickinson (www.pitt.edu/~dickinsm/), del Dto. de matemática de la Universidad de Pittsburg, se distribuyeron los primos en un esquema de flor de girasol.

Encontrar algún patrón que respeten los puntos rojos en alguna de las imágenes sería un descubrimiento extraordinario. Los puntos azules o blancos corresponden a los números compuestos.

Casi nada sabemos sobre regularidades de los primos. En el año 1975 el matemático alemán Don Zagier comentó al respecto lo siguiente:

> "Hay dos hechos acerca de la distribución de números primos que quiero comentar y que espero convencerlos de tal manera que quede para siempre grabadas en sus corazones. La primera es que, a pesar de su simple definición y del papel que juegan como bloques de construcción de los números naturales, los números primos crecen como yuyos entre los números naturales, y parecen no obedecer otra ley que no sea la del azar, y nadie puede predecir en dónde aparecerá el próximo. El segundo hecho es aún más sorprendente, ya que afirma justamente lo contrario: los números primos exhiben una impresionante regularidad, hay leyes que rigen su comportamiento, y esas leyes son obedecidas por ellos casi con precisión militar."

- No se sabe si hay infinitas parejas de primos consecutivos $(p, p+2)$ como (3,5), (5,7), (11,13), (17,19), (29,31). Estas parejas corresponden al esquema  en el dibujo anterior.

- No se sabe si todo número par mayor que 2 es suma de dos números primos. Si probamos un rato, veremos que parece que sí: $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, etc. En 1742, el matemático ruso Christian Goldbach le escribe a Euler haciéndole esta pregunta. Actualmente se conoce a este problema como la **Conjetura de Goldbach**. Nadie pudo demostrar que sea verdadera ni nadie ha podido encontrar un número par que no sea suma de dos primos.

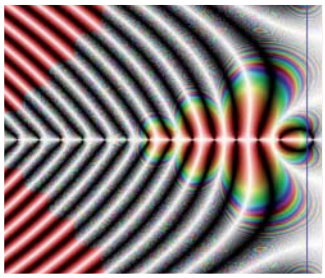


Figura 1.15. Gráfico del argumento de ζ , la línea azul corresponde a parte real 1/2.

- No se sabe si hay infinitos primos de Mersenne. Los primos de Mersenne son aquéllos que se obtienen de restarle 1 a una potencia de 2, es decir que son aquellos primos de la forma $p = 2^n - 1$. Se sabe que para que $2^n - 1$ resulte un número primo es necesario que n también sea primo. Ya vimos que estos números primos han marcado récord en la búsqueda de primos grandes.

- No se sabe si para todo n hay un número primo entre n^2 y $(n+1)^2$.

- No se sabe si es verdadera la **Conjetura de Riemann**, la cual afirma lo que a continuación explicamos resumidamente; pues es de considerable dificultad (Figura 1.15). La función Zeta de Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - p^{-s}}$$

contiene mucha información sobre la distribución de los números primos. Esta es una función que a cada número complejo le asigna un número complejo. La Conjetura de Riemann afirma que si s es un número complejo de parte real positiva, tal que:

$$\zeta(s) = 0$$

entonces, la parte real de s es 1/2. En el año 1900 D. Hilbert propuso el problema de probar esta conjetura como uno de los 23 problemas a ser resueltos durante el siglo XX. Nadie pudo resolver este problema durante ese siglo y, en el año 2000, el Clay Institute of Mathematics volvió a proponerlo como problema para el próximo milenio, esta vez ofreciendo 1 millón de dólares a quienes resuelvan el problema.

Bernhard Riemann 1826 - 1866

2. Contar sin enumerar

Por Ana Sustar

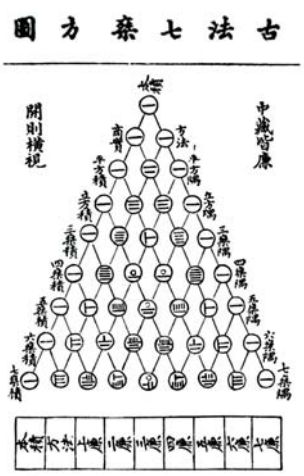


Figura 2.1 Triángulo de Yang Hui: la primera versión del triángulo de Pascal

2.1. Introducción

El "Problème des Ménages"[1]

¿Cuántas maneras hay de sentar 4 matrimonios alrededor de una mesa redonda de forma tal que hombres y mujeres estén alternados y ninguna mujer esté sentada al lado de su esposo?

En 1876 **Peter Guthrie Tait** (28 Abril 1831 - 4 Julio 1901), físico-matemático escocés, formuló este problema planteado para una cantidad n de matrimonios siendo n cualquier entero positivo. Su solución fue obtenida 58 años más tarde, en 1934, por el matemático **Jacques Touchard** (1885 – 1968).

A lo largo de este capítulo plantearemos y resolveremos diferentes problemas que, gradualmente, nos conducirán a la solución general del *Problème des Ménages* en su forma tradicional. A su vez, los conceptos e ideas que se tratan son los cimientos de la combinatoria.

Comencemos a resolver el mismo problema con un número menor de matrimonios.

Antes que nada, aclaremos que si los matrimonios están sentados de determinada manera, después todos se levantan y se corren 3 (o cualquier otro número) de lugares hacia la derecha, la nueva ubicación que tienen es equivalente a la primera. Es decir, las rotaciones alrededor de la mesa en cualquier sentido, no agregan nuevas maneras de sentarse.

Si sólo hay una pareja para sentar hay una única manera de hacerlo

[1] En castellano "Problema de los matrimonios".

en la que, claramente, no se cumplen las condiciones, porque la mujer está sentada al lado de su marido.

Si tenemos dos matrimonios e intentamos sentarlos, podremos lograr la condición de que hombres y mujeres queden separados pero siempre los matrimonios estarán juntos, o si separamos los matrimonios no se cumplirá la condición de alternar hombres y mujeres. Por lo que, con dos matrimonios, tampoco tenemos manera de hacerlo.

Cuando tenemos tres matrimonios para sentar, el problema es más interesante. Como vemos en los diagramas de la **figura 2.2**, sólo hay dos maneras posibles de sentarlos. Si H1 y M1 forman la primera pareja, H2 y M2 la segunda y H3 y M3 la tercera: →

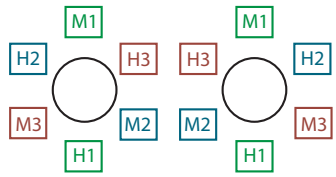


Figura 2.2: Esquema para sentar tres matrimonios

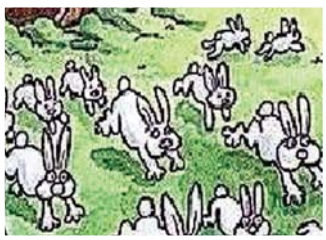
La solución que obtendremos al final del capítulo será válida para cualquier número de matrimonios n, con n mayor o igual a tres.

Otro problema de 'parejas', relacionado, es el que propuso en 1708 el matemático francés **Pierre Raymond de Montmort**, (27 de octubre 1678 - 7 octubre de 1719).

Problema de los mazos de cartas. Supongamos que tenemos dos mazos de cartas, uno azul y otro rojo. Las cartas del mazo azul se acomodan en una fila en algún orden, con el dibujo hacia arriba y luego se ubican al azar las del rojo, una arriba de cada una del azul, obteniendo así 50 parejas. El problema consiste en encontrar el número de formas de ubicar los naipes rojos, de manera tal que no haya coincidencia (en el dibujo de la carta) en ninguna de las 50 parejas.

Este problema tiene otros enunciados más atractivos, por ejemplo el siguiente problema de los sombreros (postulado y resuelto en el siglo XIX cuando todavía había sombreros) como también el problema de los conejos que enunciamos a continuación.

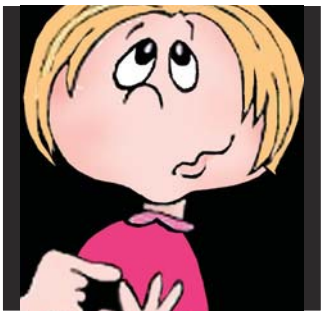
Problema de los sombreros. Si n hombres entran a un restaurante, dejan sus sombreros, y luego al irse toman los sombreros al azar, ¿de cuántas maneras pueden retirar los sombreros de forma tal que nadie tome el sombrero correcto?



Problema de los conejos. En un campo hay 30 conejos cada uno en su cueva. Por la tarde salen a pasear hasta que suena el disparo de un cazador que hace que cada conejo busque una cueva para refugiarse. ¿De cuántas maneras pueden refugiarse los conejos de forma tal que ningún conejo lo haga en su propia cueva?

Los últimos tres problemas, a pesar de las marcadas diferencias en sus enunciados, vistos desde la combinatoria son indistinguibles, es decir representan el mismo problema. Muestran cómo la combinatoria, al igual que la matemática, trabaja con modelos que son aplicables a muchos tipos de situaciones. Al comienzo de cada problema hay 'parejas' formadas con elementos de dos conjuntos: tenemos dos mazos de cartas que forman 50 parejas de cartas iguales, hay un conjunto de hombres

y un conjunto de igual número de sombreros formando cada hombre con su sombrero una pareja, y por último, hay conejos e igual número de cuevas formando cada conejo con su cueva, una pareja. Luego, por distintos motivos, hay una mezcla de las parejas: las cartas son mezcladas, los sombreros se separaron de sus dueños y los conejos se alejaron de sus cuevas. Al final, cuando se forman parejas nuevamente, se debe contar el número de posibles distribuciones en las que no se recupera ninguna de las parejas originales. Debido a este desarreglo que se produce, el problema se llama *Problema de Desarreglos.*



¿Qué significa contar?

Cuando aprendemos a contar, lo hacemos usando nuestros dedos. Cuando los dedos ya no son suficientes, nos convencemos de que si a los diez dedos le agregamos algunos más de un compañero, sigue siendo posible contar cosas con más de diez elementos. Después seguimos agregando unidades (que al principio representábamos con los dedos) hasta obtener lo que llamamos el conjunto de los Números Naturales o como los llamaban anteriormente, los números para contar. A la cantidad de elementos de un conjunto, se le llama su **Cardinalidad.**

Para contar la cantidad de gente en una sala, elegimos la primera persona a quien contar, esa será la número uno. Luego elegimos nuevamente, ahora a la persona número dos, teniendo cuidado de no cometer el error de contar otra vez a la primera persona. Ahora, es el turno de elegir la tercera persona de entre las restantes. Y el proceso sigue. Cuando a todos se les ha asignado un número y sólo uno, decimos que la cantidad de personas en la sala es igual al último número natural que asignamos. Ésta es la manera de contar *enumerando.*

En otros casos nos damos cuenta que, si agrupamos los objetos a contar convenientemente, no es necesario enumerar uno por uno los objetos que estamos contando.

Ejemplo

En un aula hay cinco filas de bancos y en cada fila hay seis bancos. Entonces, sin contar banco por banco y sin dudarlo afirmamos que en el aula hay $5 \cdot 6 = 30$ bancos. Lo que hicimos, tal vez sin darnos cuenta, fue agrupar los bancos que queríamos contar en filas, todas ellas con igual cantidad de bancos y luego multiplicar, cosa que no es más que sumar varias veces la misma cantidad. Ahora, si en otra aula tenemos filas que no tienen la misma cantidad de bancos, por ejemplo hay tres filas con seis bancos y dos con cinco bancos, nos damos cuenta que lo anterior no funciona. Lo resolvemos separando los bancos en dos grupos de filas, por un lado las que tiene seis bancos y por otro las que tienen cinco. Ahora sí podemos calcular como antes los bancos de cada grupo, concluyendo que en el primer grupo hay $3 \cdot 6 = 18$ y en el segundo hay $2 \cdot 5 = 10$, y por lo tanto hay un total de $18 + 10 = 28$ bancos en el aula.

Esta forma de **contar sin enumerar** los objetos, agrupándolos de alguna manera conveniente es lo que hace la **combinatoria**.

Los problemas planteados al comienzo, pueden ser resueltos enumerando las posibilidades, tarea que a medida que crece la cantidad de objetos involucrados se torna más tediosa, extensa y complicada.

En combinatoria, para resolver este tipo de problemas, se continúa con esta idea ***natural*** de agrupar y combinar convenientemente determinados objetos. Luego se trata de independizarse de cardinalidades particulares para poder lograr resultados generales, relaciones o fórmulas que se satisfagan para cualquier número natural n.

Ejemplo

Se quiere conocer la cantidad de partidos posibles para llevar a cabo un cuadrangular de ajedrez en el que juegan todos contra todos. Si los participantes son: Luis, Ariel, Ema y Sara, los partidos serán entre: Luis y Ariel, Luis y Ema, Luis y Sara, Ariel y Ema, Ariel y Sara y por último Ema y Sara. Es decir, seis. Pero esa respuesta no nos ayuda a conocer cuántos partidos serían si en lugar de cuatro los participantes fueran diez o treinta.

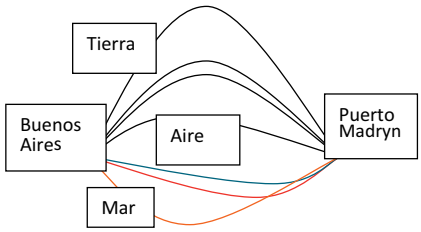
Lo que realmente necesitamos es una fórmula para calcular el número de parejas de un conjunto de n personas siendo n cualquier número natural.

En nuestro camino hacia la solución del *Problème des Ménages*, formalizaremos y demostraremos lo necesario, rescatando la interpretación combinatoria de las definiciones o expresiones involucradas. Nos aproximaremos a los conceptos, principios o ideas a través de problemas concretos que nos facilitarán la tarea.

2.2. Los principios de adición y multiplicación

Problema de transporte I. Supongamos que estamos por comprar pasajes para viajar desde la ciudad de Buenos Aires hasta la ciudad de Puerto Madryn, provincia de Chubut. En la agencia de viajes nos informan que podemos realizar el viaje por tierra, por aire o por mar. Disponen de dos maneras de hacerlo por mar, de una manera de hacerlo por aire y de 4 maneras por tierra.

¿De cuántas formas podemos viajar?



Como debemos elegir sólo una manera de viajar, el total de posibilidades es $4 + 2 + 1 = 7$.

Problema del menú I. En un restaurante ofrecen para el postre dos copas heladas diferentes y tres tartas de frutas diversas. Nos preguntamos el número total de posibles postres.

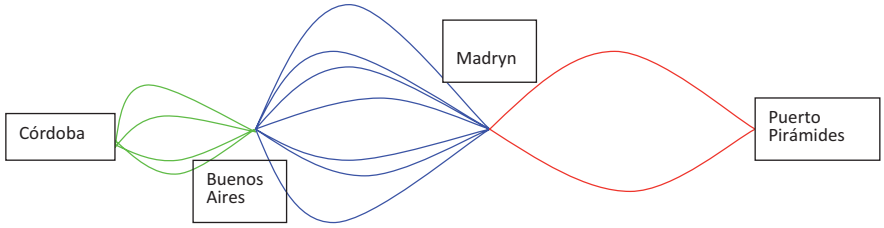
Obviamente, como debemos elegir sólo un postre entre $2 + 3 = 5$ opciones, ése será el número buscado. Formalizamos estas ideas en el principio de adición.

Principio de Adición. Si se puede realizar una acción **A** de n formas distintas, y se puede realizar una acción **B** de m formas distintas, siendo **A** y **B** excluyentes, entonces el número de formas de realizar la acción '**A** o **B**', es $n + m$.

Una forma equivalente del mismo principio usando la terminología de conjuntos es la expresada en el recuadro:

Principio de adición. Sean **A** y **B** dos conjuntos finitos y disjuntos, entonces card **(A ∪ B)** = **card A** + card **B**.

Problema de transporte II. Para viajar desde la ciudad de Córdoba (provincia de Córdoba) hasta Puerto Pirámides (provincia de Chubut), se debe pasar por Buenos Aires y luego por Puerto Madryn, tal como se muestra en la figura.



Si hay 4 formas de ir desde Córdoba a Buenos Aires, 7 para ir desde Buenos Aires a Puerto Madryn, y 2 para ir desde Puerto Madryn hasta Puerto Pirámides, ¿cuántas maneras tenemos de viajar entre Córdoba y Puerto Pirámides?

Por cada una de las 4 opciones para el primer tramo, tenemos 7 para el segundo. Por lo que tenemos 4 . 7 = 28 posibilidades para ir desde Córdoba a Puerto Madryn. Por cada una de esas 28 posibilidades tenemos 2 opciones para el último tramo, es decir en total hay 4 . 7 . 2 = 28 . 2 = 56 maneras distintas de ir desde Córdoba hasta Puerto Madryn.

Problema del menú II. Un restaurante tiene el siguiente menú:

Entrada: sopa o empanadas.
Plato Principal: lomo a la crema, arrollado de atún y nuez o cordero flambeado.
Postre: helado o pastel de manzana.

Nos preguntamos por la cantidad de comidas completas que podemos ordenar. Primero resolveremos el problema más sencillo: calcular la cantidad de posibles comidas sin postre. Para la entrada tenemos dos posibilidades. Para cada una de ellas tenemos tres opciones para el plato principal. Tendremos entonces 2 . 3 = 6 posibilidades de comidas sin postre. Volviendo a los postres, para cada una de esas seis opciones tenemos dos opciones de postres, lo que nos da un total de 6 . 2 = 12 posibles comidas completas.

Formalizamos estas ideas con el principio de multiplicación.

Principio de multiplicación. Si una acción **A** puede realizarse de n formas distintas, y una acción **B** de ***m*** formas distintas, siendo **A** y **B** independientes, entonces la acción **'A** y **B'** se puede realizar de ***n . m*** formas distintas.

Una formulación equivalente usando terminología conjuntista es la expresada en el recuadro siguiente:

Principio de multiplicación. Sea **A** x **B** = {(***a***, ***b***) : ***a*** ∈ **A**, ***b*** ∈ **B**} el Producto Cartesiano de **A** y **B**, entonces card **(A** ∪ **B)** = card **A** + card **B**.

Problema de dados. Supongamos que tiramos simultáneamente dos dados, uno blanco con puntos negros, y otro negro con puntos blancos, y queremos saber cuántos posibles resultados tenemos. El dado blanco tiene 6 formas distintas de caer, lo mismo el negro y (suponiendo que no están cargados) la caída de un dado no afecta la del otro. Por lo tanto, tenemos acciones independientes, entonces el total de posibilidades es 6 . 6 = 36.

Ahora bien, supongamos que queremos calcular cuántas formas hay de arrojar los dados de manera tal que la suma de los dos sea 7. Entonces, las acciones no son independientes y no podemos usar el principio de multiplicación. La forma de resolver este problema es la siguiente: Las acciones posibles para el primer dado son que la cara superior indique un '1', un '2', etc. Cada una de estas acciones determina automáticamente qué número debe aparecer en el otro dado: si en el blanco aparece un '1', en el negro debe haber un '6'; un '2' con un '5'; etc. Por lo tanto, hay sólo 6 posibilidades.

Similarmente, supongamos que pidiéramos que "no haya dobles". En este caso, el número en el dado blanco no determina absolutamente el número del dado negro, pero sí limita sus posibilidades: si sale '1' en el blanco, no puede salir '1' en el negro, por lo tanto el dado negro tiene sólo 5 posibilidades. Así hay sólo 6 . 5 = 30 tiradas posibles de los dados sin dobles.

También podríamos haber deducido esto haciendo el siguiente razonamiento: si hubiéramos pedido que haya sólo dobles, entonces el dado blanco determinaría el valor del negro (si sale un '1' en el blanco, debe salir '1' en el negro, etc.), por lo tanto hay sólo 6 dobles, y (recordando que el total de posibilidades para los resultados de los dos dados sin restricciones es 6 . 6 = 36), hay 36 – 6 = 30 posibles tiradas sin dobles.

Muchas veces un problema combinatorio se resuelve mucho más fácil (o incluso, es la única forma de resolverlo) pensando, como en este caso, en el 'complemento', y sustrayendo el número obtenido del total.

Los principios de adición y multiplicación, a pesar de su sencillez y claridad, son la base para resolver los problemas de conteo. Veremos que por más complicado que sea un problema, siempre lo podremos descomponer en 'subproblemas' más simples que podrán ser resueltos usando estos dos poderosos principios.

La generalización de los principios a un número finito de acciones es válida e inmediata. Veamos problemas donde usamos ambos principios.

Problema de equipos. Supongamos que un estudiante debe formar parte de dos de los equipos deportivos siguientes: 3 equipos distintos de vóley, 4 equipos distintos de fútbol y 5 equipos distintos de básquet, ¿cuántas opciones tiene?

Primero debemos usar el principio de adición para dividir el problema en casos excluyentes. En este caso, las opciones serían "elige vóley y fútbol'', "elige vóley y básquet'' y "elige básquet y fútbol''. Luego, resolvemos cada caso usando el principio de multiplicación, porque el equipo que elija para vóley, por ejemplo, no afectará el equipo que elegirá en básquet. Así, en el primer caso tenemos $3 \cdot 4 = 12$ posibilidades, en el segundo $3 \cdot 5 = 15$ posibilidades, y en el tercer caso $4 \cdot 5 = 20$ posibilidades. Aplicando el principio de adición tenemos un total de $12 + 15 + 20 = 47$ posibilidades.

Problema de números. Sea $X = \{1, 2, 3, ..., 100\}$ y sea $S = \{(a, b, c) : a, b, c \in X, a < b, a < c\}$. Encontrar la cardinalidad del conjunto S.

Dividiremos el problema en casos disjuntos considerando $a \in \{1, 2, 3....,99\}$. Como $a = k \in \{1, 2, ...,99\}$, el número de opciones para b es $(100 - k)$ y las opciones para c también son $(100 - k)$. Por lo que, aplicando el principio de multiplicación, el número de tres-uplas ordenadas (k, b, c) es $(1\,00 - k)^2$. Ahora k toma valores de $\{1, 2, 3..., 99\}$, entonces aplicando el principio de adición tenemos:

$$\begin{aligned} \text{card } S &= 99^2 + 98^2 + ... + 1^2 \\ &= 328.350 \end{aligned}$$

Para resolver

2.1. Una fábrica de automóviles produce cuatro modelos distintos de vehículos. Los modelos A y B pueden ser de cualquiera de los cuatro estilos siguientes: sedan, todo terreno, convertible y familiar. Los modelos C y D sólo vienen del tipo sedan o todo terreno. Todos pueden fabricarse en alguno de los nueve colores disponibles. ¿Cuántos automóviles diferentes produce la fábrica?

2.2. Una orquesta sinfónica siempre toca una de las 41 sinfonías de Mozart, seguida por una de las 25 canciones modernas de su repertorio, seguidas por una de las 9 sinfonías de Beethoven.

a) ¿Cuántos programas diferentes puede tocar la orquesta?
b) ¿Cuántos programas diferentes puede tocar, si las piezas pueden ser tocadas en cualquier orden?
c) ¿Cuántos programas de tres piezas son posibles, si se puede tocar más de una pieza de la misma categoría?

2.3. Permutaciones y arreglos

Problema de la Ceremonia Inaugural. ¿De cuántas maneras posibles pueden entrar las 200 delegaciones de los diferentes países en la Ceremonia Inaugural de los Juegos Olímpicos?

Podemos resolver el problema usando el principio de multiplicación. Tenemos 200 posibilidades para la primera ubicación. Para la segunda ubicación tenemos 199 posibilidades. Para la tercera, sólo 198, y así seguimos descendiendo hasta llegar a 1,

correspondiente a la situación en que ya están los 199 primeros puestos asignados y queda una posición para el único país que quedó sin ubicar. Obtenemos 200.199.198... 3.2.1 =

= 788657867364790503552363213932185062295135977687173263294742533244
359449963403342920304284011984623904177212138919638830257642790242 63
710506192662495282993111346285727076331723739698894392244562145166 42
402540332918641312274282948532775242424075739032403212574055795686 60
226031904170324062351700858796178922222789623703897374720000000000 00
000000000000000000000000000000000000000 ¡posibles ingresos!

Si consideramos el caso general de ordenar n elementos, la cantidad de maneras de hacerlo es $n(n-1)(n-2)...2.1$. Este número, que aparece muy frecuentemente, se llama factorial de n y se lo denota $n!$ Es decir, $n! = n(n-1)(n-2)...1$.

Formalizando estas ideas, decimos que:

Una ***permutación*** de los elementos de un conjunto es un reordenamiento de ellos. El número de permutaciones de un conjunto de n elementos es $n!$, donde $n! = n(n-1)(n-2)... 3.2.1$.

Problema de una carrera de caballos. En una carrera participan 12 caballos. ¿De cuántas maneras pueden resultar los tres primeros puestos?

Este problema es parecido al anterior, pero la diferencia es que necesitamos ordenar un número de elementos menor que la cardinalidad del conjunto.

Hay 12 posibilidades para el campeón. Luego sólo 11 para el subcampeón y finalmente 10 para el tercer puesto. Como se trata de elecciones sucesivas, por el principio de multiplicación tenemos un total de 12 . 11 . 10 = 1.320 posibles ternas.

Generalizando la idea, queremos saber cómo calcular un reordenamiento de r objetos de un conjunto de n siendo $n \geq r$. Definimos: →

Los ***arreglos*** son las diferentes permutaciones de r objetos de entre n, siendo $n \geq r$, se denotan $P(n, r)$, y $P(n, r) = n(n-1)(n-2)...(n-r+1)$.

Problema de tres carreras de caballos. En tres carreras hay 10, 8 y 6 caballos corriendo respectivamente. Una persona gana un premio si predice los tres primeros caballos en el orden correcto en cada carrera. ¿Cuántas predicciones posibles hay?

Primero estudiemos cada carrera separadamente. En la que participan 10 caballos hay 10. 9. 8 posibles ternas ganadoras. En la de 8, hay 8. 7. 6 ternas posibles, y en la carrera con 6 caballos habrá 6. 5. 4. Ahora bien, se debe elegir tres ternas, una de cada carrera y las elecciones son consecutivas, entonces por el principio de multiplicación tendremos un total de opciones igual a : (10. 9. 8)(8. 7. 6)(6. 5. 4) = 29.030.400.

Observaciones

- Por convención 0! = 1.
- P (0, n) = 1 (correspondiente a no permutar nada) y $P(n, n) = n!$ (correspondiente a permutar todo).
- Como $n! = n(n-1)\ldots(n-r+1)(n-r)(n-r-1)\ldots$ 3.2.1 si $r < n$ y $P(n, r) = n(n-1)(n-2)\ldots(n-r+1)$, entonces:

$$P(n, r) = \frac{n!}{(n-r)!}, \quad r \leq n.$$

Para resolver

2.3 Si las patentes de los automóviles se componen de tres letras seguidas de un número de uno, dos o tres dígitos, ¿cuántas patentes distintas puede haber?

2.4 En una reunión hay 7 varones y 3 mujeres. ¿De cuántas maneras pueden ser ubicados en fila si:

a) las tres mujeres deben estar juntas?
b) las dos posiciones del final deben ser varones y no debe haber mujeres juntas?

2.5 Encontrar el número de enteros positivos divisores de 600, incluyendo a 1 y a él mismo.

2.6 ¿Cuántas secuencias de n dígitos hay en las que no haya dos dígitos consecutivos iguales?

□ 2.4. Combinaciones y los números combinatorios

Problema de la salida al teatro. Se propone una salida voluntaria al teatro en una clase de 20 estudiantes. Se desea saber cuántos grupos posibles pueden formarse.

Una forma de resolver este problema es hacer una combinación de los principios de adición y multiplicación. Primero, dividimos el problema en casos disjuntos: el caso en que el grupo es de un estudiante, el grupo que consiste de dos estudiantes, etc. En el primer caso, tenemos 20 posibilidades. En el segundo, tenemos 20 posibilidades de elegir un alumno, y luego tendríamos 19 para elegir el segundo, pero deberíamos dividir por dos, porque que si primero escogemos a Juan y luego a María, es lo mismo que elegir a María y después a Juan. Claramente, los casos con más estudiantes se complican más porque se deben analizar 20 casos distintos. Así, a pesar de lo tedioso que resulte, se obtendría la solución.

Veamos otro método para resolver ese problema, y después generalizarlo a un conjunto de cardinalidad arbitraria.

En realidad, lo que queremos saber es cuántos subconjuntos no vacíos hay en un conjunto de 20 elementos.

Supongamos que los alumnos están numerados del 1 al 20. Dado que la salida es voluntaria, para el alumno 1 hay dos opciones: ir o no ir; también tiene las mismas dos opciones el alumno 2, el 3 y el resto. Por lo que cada uno de los 20 alumnos tiene dos posibilidades. Además, la elección de cada uno es independiente de la de los otros (o al menos las consideramos así), por lo que hay 2^{20} posibilidades en total. Notemos que al contar hemos incluido la posibilidad de que nadie vaya, que es una. Entonces, la cantidad de grupos no vacíos de alumnos que se pueden formar es $2^{20}-1 = 1.048.575$.

Este resultado se puede generalizar a un conjunto de n elementos: →

La cantidad de subconjuntos de un conjunto de ***n*** elementos es 2^n.

Veamos con un ejemplo cómo calcular el número total de subconjuntos de un determinado tamaño en lugar del número total de subconjuntos.

Ejemplo

Si agregamos al problema de la salida al teatro la condición de que el grupo sea de 12 estudiantes. Para el primer lugar tenemos 20 posibilidades, 19 para el segundo, 18 para el tercero y así hasta llegar a 9 posibilidades para el último que es elegido. Es decir, calculamos $P(20,12)$. Notemos que elegimos 12 alumnos, pero ordenados. Como el orden no nos interesa (interesa el grupo en sí), tenemos que dividir por la cantidad de formas de ordenar los 12 elementos, el número de permutaciones, es decir 12!. Entonces, la cantidad de subconjuntos de un conjunto de 20 elementos es:

$$\frac{20\,.19\,...\,11.10\,.9}{12\,!} = \frac{20!}{8!\;12!}$$
$$= 125.970$$

Generalicemos este resultado para calcular la cantidad de subconjuntos de cardinalidad k de un conjunto de cardinalidad n con $k \le n$. Razonando en forma análoga, tenemos n posibilidades para el primero que elegimos, $(n-1)$ para el segundo, $(n-2)$ para el tercero, y así sucesivamente hasta tener $(n-k+1)$ para el último elegido, el número k. Estos k elementos elegidos están ordenados (hay tantas posibles elecciones como $P(n,k)$), para no considerar este orden dividimos por $k!$ la cantidad de órdenes posibles del subconjunto elegido. Obtenemos:

$$\frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

Entonces, de acuerdo a lo visto, podemos describir explícitamente estos números:

Llamamos **números combinatorios** y denotaremos por $\binom{n}{k}$, al número de subconjuntos de tamaño ***k*** de un conjunto de tamaño ***n***.

$$\binom{n}{k} = \frac{P(n,k)}{k!}$$
$$= \frac{n!}{k!(n-k)!}$$

Observemos que $P(n, k)$ es igual a la cantidad de arreglos de $\{1,2, \ldots, n\}$ tomados de k en k. Se pueden obtener estos arreglos escogiendo primero los k elementos que vamos a ordenar (esto se hace en $\binom{n}{k}$ formas) y luego ordenándolos en $k!$ formas. Por lo tanto, $P(n\ ,\ k) = \binom{n}{k} k!$ o equivalentemente $\binom{n}{k} = \frac{P(n,k)}{k!}$.

Con esta fórmula, mediante operaciones algebraicas, se prueban la mayoría de las propiedades de los números combinatorios. Podemos obtener algunas propiedades directamente de la definición. Esto permite, además de recordarlas mejor, comprender en profundidad las fórmulas involucradas.

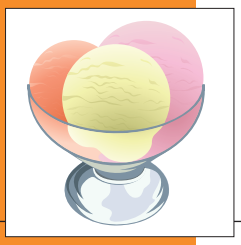
Propiedades de los números combinatorios

Los números combinatorios, como vimos, cuentan la cantidad de posibles subconjuntos de determinado tamaño de un conjunto de tamaño mayor. Pero su utilidad se extiende, combinándolos y usando los principios de adición y multiplicación, a otro tipo de situaciones en las que se calculan cardinalidades de subconjuntos con alguna condición, restricción o propiedad. Esto se verá reflejado en las siguientes propiedades:

$$\binom{n}{k} = \binom{n}{n-k} \text{ (Simetría).}$$

Veamos, con el siguiente ejemplo, cómo interpretamos combinatoriamente los números involucrados en la igualdad.

Ejemplo



Supongamos que tenemos que elegir 3 sabores de helado de entre 8. La propiedad nos dice que es lo mismo elegir los 3 sabores que queremos, a elegir los 5 sabores que no queremos, es decir $\binom{8}{3} = \binom{8}{5}$. En el gráfico están representados por E todos los sabores de helados, A representa los sabores que no elegimos y $\overline{A}$ los que sí elegimos.

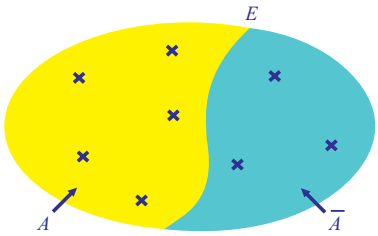


Figura 2.5. Esquema problema de los helados

En otras palabras $\binom{n}{k}$ denota el número de subconjuntos de k elementos de un conjunto de n elementos E. Sea A un tal subconjunto. Entonces, el complemento de A, $\overline{A}$ debe tener $n - k$ elementos. Así, cada subconjunto de k elementos determina un único subconjunto de $n - k$ elementos, y por lo tanto:

$$\binom{n}{k} = \binom{n}{n-k}$$

- **Teorema del Binomio**. Este conocido teorema es el que nos permite calcular fácilmente los coeficientes (llamados coeficientes binomiales) en la expansión de cual-

quier potencia de un binomio. Por ejemplo de: $(x + y)^3 = x^3 y^0 + 3x^2 y^1 + 3x^1 y^2 + x^0 y^3$. La forma general del mismo es:

$$(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \; y^{n-k}$$

El Teorema se podría probar algebraicamente, sin embargo lo demostraremos en forma combinatoria: pensemos a $(x + y)^n$ como el producto $(x + y)\,(x + y)\ldots(x + y)$. Si distribuimos la multiplicación con respecto a la adición, obtenemos una suma de elementos de la forma $x^k y^r$ con k variando entre 0 y n. En el ejemplo esta suma es: $x^3 y^0 + 3x^2 y^1 + 3x^1 y^2 + x^0 y^3$

Como en el producto $(x + y)\,(x + y)\ldots(x + y)$ tenemos n factores, al desarrollarlo, cada uno aporta un x o un y, pero no ambos. Tenemos además, que la suma de los exponentes de x e y en cada producto $x^k y^r$ debe ser n, (ya que hay n factores de la forma x o y que multiplicados dan el producto) , por lo que $r = n - k$. Lo único que queda por verificar es la cantidad de factores de la forma $x^k y^{n-k}$, es decir el coeficiente binomial correspondiente.

Si numeramos los factores $(x + y)$ en el producto $(x + y)\,(x + y)\ldots(x + y)$, (digamos factor 1, factor 2, etc.) tenemos que decidir, ¿de cuáles factores obtenemos los x? (una vez decidido esto, los y se deben obtener de los otros factores). Entonces, decidir cuántos sumandos de la forma $x^k y^{n-k}$ hay es lo mismo que decidir de cuántas formas podemos escoger k factores $(x + y)$ (de los cuales sacaremos los x). Pero tenemos n factores de los cuales debemos elegir k, por lo tanto, el número de formas de hacerlo es $\binom{n}{k}$. Ahora tenemos la suma de $n + 1$ términos de la forma $\binom{n}{k} x^k y^{n-k}$, $0 \le k \le n$ es decir, hemos probado la propiedad.

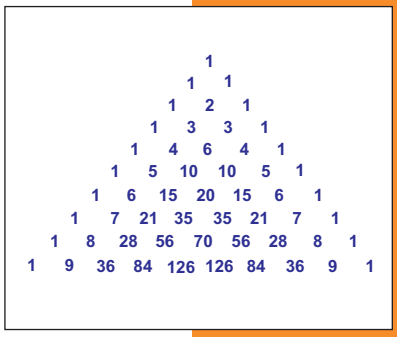
$$1 \qquad 1$$
$$a + b$$
$$1 \qquad 2 \qquad 1$$
$$a^2 + 2ab + b^2$$
$$1 \qquad 3 \qquad 3 \qquad 1$$
$$a^3 + 3a^2b + 3ab^2 + b^3$$
$$1 \qquad 4 \qquad 6 \qquad 4 \qquad 1$$
$$a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$
$$1 \qquad 5 \qquad 10 \qquad 10 \qquad 5 \qquad 1$$
$$a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

Figura 2.6: Triángulo de Pascal

Los coeficientes binomiales no sólo aparecen en las potencias de binomios. Están involucrados en muchísimas relaciones, secuencias y conjuntos de números. Para poder apreciar esto observemos ahora el esquema que se visualiza en la **figura 2.6**. En cada fila se desarrollan las potencias del binomio $(a + b)$ y se destacan los coeficientes.

El triángulo que se forma con estos coeficientes, que son los números provenientes del binomio, es el famoso: **"Triángulo de Pascal"** en honor a Blaise Pascal (1623-1662) quien realizó diversas investigaciones acerca de él en 1653. De hecho, el matemático italiano **Niccolò Fontana Tartaglia** (1500 - 1557), ya lo conocía mucho antes que Pascal. Más aún, desconocido para los europeos, los chinos ya lo estudiaban. En China el triángulo lleva el nombre de su descubridor Yang Hui (1238–1298) quien lo construyó en 1261.

Dicho triángulo se construye colocando un 1 y debajo de él otros dos números1. Cada nueva línea comienza y termina con números 1, pero los elementos en el interior de la línea se forman sumando los dos elementos en la línea superior a él que son adyacentes: →



Vemos que gracias a la propiedad de simetría de los números combinatorios antes mencionada $\binom{n}{k} = \binom{n}{n-k}$, el triángulo es simétrico con respecto a la altura del triángulo que tiene al primer uno como extremo o informalmente las filas son 'capicúas'. Por ejemplo miremos la séptima fila:

	p = 0	p = 1	p = 2	p = 3	p = 4	p = 5	p = 6	p = 7	p = 8	p = 9
n = 0	1									
n = 1	1	1								
n = 2	1	2	1							
n = 3	1	3	3	1						
n = 4	1	4	6	4	1					
n = 5	1	5	10	10	5	1				
n = 6	1	6	15	20	15	6	1			
n = 7	1	7	21	35	35	21	7	1		
n = 8	1	8	28	56	70	56	28	8	1	
n = 9	1	9	36	84	126	126	84	36	9	1

1, 6, 15, 20, 15, 6, 1. El primer 6 es el número combinatorio $\binom{6}{1}$ mientras que el último 6 es $\binom{6}{5}$.

En la figura de la izquierda hemos inscripto el Triángulo de Pascal en una tabla. El número en la línea n y la columna p, es el número combinatorio $\binom{n}{p}$.

Probaremos la propiedad que nos dice que un elemento de la fila $n + 1$ es la suma de sus dos antecesores en la fila n. Es decir:

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

Para entender y probar esta relación interpretaremos los números involucrados como cardinalidades de conjuntos con un ejemplo.

Ejemplo

Si tenemos que elegir 4 gustos de helado de entre 9 tendremos $\binom{9}{4}$ maneras de hacerlo. Por otro lado, si por ejemplo entre los 9 sabores existe el chocolate, podríamos elegirlo o no. En el primer caso, si lo incluimos, debemos elegir 3 de entre los 8 sabores restantes, es decir tenemos $\binom{8}{3}$ formas, mientras que si no lo incluimos tenemos que elegir los 4 sabores de entre 8, es decir de $\binom{8}{4}$ maneras. Ahora, como el elegir o no al chocolate son acciones excluyentes, por el principio de adición debemos sumar esas dos cantidades obteniendo como resultado: $\binom{9}{4} = \binom{8}{3} + \binom{8}{4}$. En el gráfico (**Figura 2.7**) **e** representa el sabor chocolate, A el conjunto que elegimos y E, E' los conjuntos que se forman dependiendo de si $\mathbf{e} \in A$, o no.

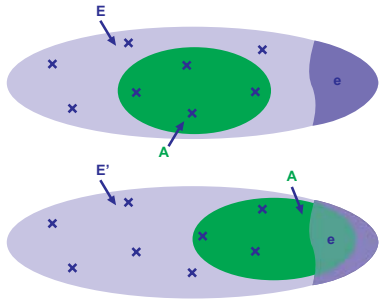


Figura 2.7: Esquema problema de gustos de helados.

Veamos ahora el caso general: tomemos A = {1, 2,… , n, n + 1}. Por definición hay $\binom{n+1}{k}$ subconjuntos de k elementos de A. Contaremos de otra manera la cantidad de estos subconjuntos. Cada subconjunto de k elementos de A, o bien contiene a 1 o no.

Si $1 \in A$ la cantidad de dichos subconjuntos es $\binom{n-1}{k-1}$. Si $1 \notin A$ la cantidad de formas de hacerlo es $\binom{n}{k-1}$. Por el principio de adición tenemos la suma deseada:

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

El Teorema del binomio permite deducir algunas identidades binomiales (es decir igualdades que involucran números combinatorios) en forma no combinatoria, por ejemplo, tomando $x = y = 1$ en la fórmula del binomio obtenemos:

$$\begin{aligned}(1+1)^n &= 2^n \\ &= \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} \\ &= \sum_{k=0}^{n} \binom{n}{k}\end{aligned}$$

Esta es, obviamente, una prueba algebraica. Veamos una prueba combinatoria de:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Puesto que cada $\binom{n}{k}$ es igual a la cantidad de subconjuntos de k elementos de un conjunto de n elementos y, como estamos sumando sobre k, resulta que la suma de la izquierda es igual a la cantidad total de subconjuntos de un conjunto de n elementos. Anteriormente, vimos que es igual a 2^n.

Veamos la prueba con argumentos combinatorios. La suma de la derecha, por los principios de adición y multiplicación, es igual a la cantidad de formas distintas de escoger un subconjunto de un conjunto de n elementos y luego distinguir uno de ellos. Por ejemplo, podríamos decir que tenemos un conjunto de n personas de las cuales hay que escoger una comisión de tamaño no especificado, y luego elegir un presidente de esa comisión. Ahora bien, esto también se puede hacer eligiendo primero al presidente entre las n personas y luego elegir al resto de la comisión de entre las $(n-1)$ personas que quedan, en 2 formas posibles.

Para quienes dominan los conceptos de derivadas

Otra fórmula que se puede obtener a partir del binomio (usando derivadas de funciones para quienes conocen este tema), es con y = 1, obteniendo

- $(x+1)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$

Ahora derivamos respecto de x:

- $n(x+1)^{n-1} = \sum_{k=0}^{n} \binom{n}{k} k x^{k-1}$

Tomando ahora x = 1, tenemos:

- $n \cdot 2^{n-1} = \sum_{k=0}^{n} \binom{n}{k} k$

- Identidad de Van der Monde

$$\sum_{k=0}^{r} \binom{n}{k}\binom{m}{r-k} = \binom{n+m}{r}$$

Se puede hacer una prueba no combinatoria comparando los coeficientes de x^r que se obtienen al desarrollar ambos miembros de la igualdad:

$$(1+x)^n (1+x)^m = (1+x)^{m+n}$$

Una prueba combinatoria más corta es la siguiente: $\binom{n+m}{r}$ es igual al número de subconjuntos de r elementos del conjunto $\{1, 2, \ldots, n+m\}$. Pero, un tal subconjunto tendrá una cantidad, digamos k, de elementos del conjunto $\{1, 2, \ldots, n\}$ y el resto $(r-k)$ estarán en $\{n+1, n+2, \ldots, n+m\}$. Así, para formar tal subconjunto debemos elegir un k y luego k elementos de $\{1, 2, \ldots, n\}$ en $\binom{n}{k}$ formas, y luego $r-k$ elementos de $\{n+1, n+2, \ldots, n+m\}$ en $\binom{m}{r-k}$ formas. Por los principios de adición y multiplicación hay $\sum_{k=0}^{r} \binom{n}{k}\binom{m}{r-k}$ formas de hacer esto.

La siguiente identidad nos dice lo que pasa si sumamos a lo largo de una diagonal del Triángulo de Pascal.

- Identidad de Chu Shih-Chieh (o del palo de Jockey):

$$\sum_{k=r}^{n} \binom{k}{r} = \binom{n+1}{r+1}$$

Ejemplo

En la **figura 2.8** están representadas las siguientes sumas:

$\binom{9}{3} = \binom{8}{3} + \binom{7}{2} + \binom{6}{1} + \binom{5}{0}$ ó $84 = 56 + 21 + 6 + 1$,

$\binom{7}{5} = \binom{6}{4} + \binom{5}{4} + \binom{4}{4}$ ó $21 = 15 + 5 + 1$ y

$\binom{10}{9} = \binom{9}{8} + \binom{9}{9}$ ó $10 = 9 + 1$.

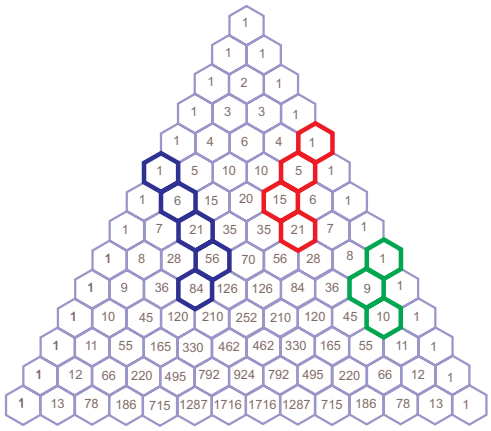


Figura 2.8.

El número $\binom{n+1}{r+1}$ es igual a la cantidad de subconjuntos de $r+1$ elementos de $\{1, 2, \ldots, n+1\}$. Para formar un subconjunto A de $r+1$ elementos debemos decidir primero cuál es el mayor número que estará en A.

Supongamos que j es tal número (observemos que como A debe tener $r+1$ elementos, j debe ser al menos $r+1$). Entonces, como $j+1, j+2, \ldots, n+1 \in A$ debemos completar A con r elementos tomados del conjunto $\{2, \ldots, j+1\}$. Podemos hacer esto de $\binom{j+1}{r}$ formas distintas. Así, tenemos que $\sum_{j=r+1}^{n+1} \binom{j+1}{r} = \binom{n+1}{r+1}$. Tomando $j = k+1$ en la suma obtenemos el resultado.

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}=0$$

Una prueba no combinatoria sencilla se obtiene evaluando $(x+1)^n=\sum_{k=0}^{n}\binom{n}{k}x^k$ en $x=-1$.

Veamos la prueba combinatoria. Basta probar que el número de subconjuntos de {1, …, *n*} con una cantidad impar de elementos es igual al número de subconjuntos con una cantidad par de elementos. Esto es obvio si *n* es impar, puesto que si *A* tiene una cantidad par de elementos entonces el complemento de *A* debe tener una cantidad impar de elementos. Si *n* es par dividimos todos los subconjuntos en dos clases:

1.ª los que contienen a *n,* y
2.ª los que no contienen a *n*.

La cantidad de subconjuntos de la 2.ª clase con una cantidad par de elementos es igual a la cantidad en la 2.ª clase con una cantidad impar puesto que ahora estos son subconjuntos de {1, …, *n* – 1}. Si *A* está en la 1.ª clase, *A* – {n} es subconjunto de {1, …, *n* – 1}, así pues: la cantidad de subconjuntos en la 1.ª clase con una cantidad impar de elementos, es igual a la cantidad de subconjuntos de {1, …, *n* – 1} con una cantidad par de elementos, que a su vez es igual a la cantidad de subconjuntos de {1 , …, *n* – 1} con una cantidad impar de elementos, e igual a la cantidad de subconjuntos de la 1.ª clase con una cantidad par de elementos. Con lo que queda probada la propiedad.

Para resolver

2.7. Más regularidades en el Triángulo de Pascal.

Hallar en el triángulo:
a.- los números naturales;
b.- los números triangulares: son aquellos que si se representan con puntos permiten formar, con ellos, triángulos equiláteros: 1, 3. 6, 10, 15, 21... (**Figura 2.9**);

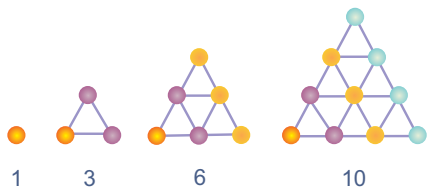


Figura 2.9.

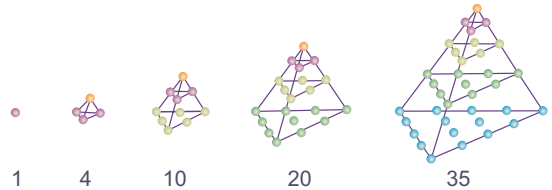


Figura 2.10.

c.- números tetraedros: aquellos que si se representan con bolitas permiten formar, con ellos, tetraedros: 1, 4, 10, 20, 35, ... (**Figura 2.10);**
d.-números pares e impares;
e.- potencias de 2. Ayuda: sumar;
f.- secuencia de Fibonachi: es la secuencia que comienza con dos unos y luego cualquier término se obtiene sumando los dos últimos: 1, 1, 2, 3, 5, 8, 13, ... ;
g.-las potencias de 11. Ayuda: mirar las filas de la **figura 2.11.**

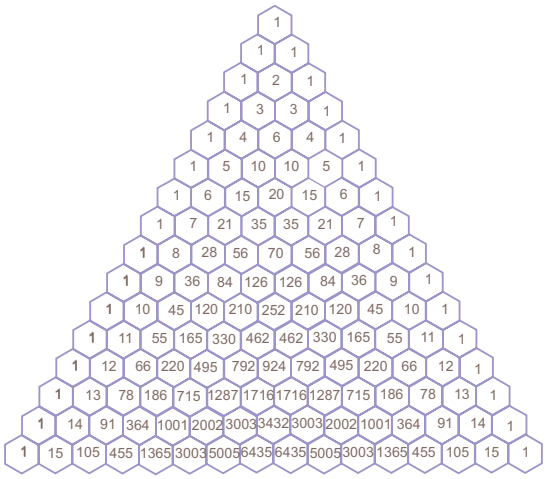


Figura 2.11.

Composiciones de un número natural

Problema de la fiesta.

Un grupo de 21 estudiantes está planeando una fiesta de recaudación de fondos para su viaje de estudios. Deben hacer varias tareas:

1. elegir el lugar donde hacer la fiesta,
2. obtener los permisos municipales,
3. contratar el DJ,
4. imprimir las entradas,
5. vender las entradas.

Se ponen de acuerdo en que todos harán la última tarea, y en dividirse las otras en 4 grupos distintos. ¿De cuántas formas pueden formarse estos grupos?

Resolver este problema es equivalente a contar cuántas maneras hay de dividir el grupo de 21 personas en 4 partes porque todos se ocuparán de vender entradas.

Una composición de un número natural n es una expresión de n como suma ordenada de números naturales. Los sumandos de una composición se llaman partes de la misma.

Ejemplo

$5 = 3 + 2$ es una composición de 5, y $5 = 2 + 3$ es otra. El número 4 tiene 8 composiciones en total: $1 + 1 + 1 + 1$; $2 + 1 + 1$; $1 + 2 + 1$; $1 + 1 + 2$; $3 + 1$; $1 + 3$; $2 + 2$ y 4.

Hay dos preguntas importantes que podemos hacernos con respecto a las composiciones. Dado n, ¿cuántas composiciones tiene n? y ¿cuántas composiciones con k partes? Por ejemplo, el número 4 tiene 3 composiciones con 3 partes y otras 3 con 2. Es muy simple responder esas preguntas. Veamos ¿cómo?

Podemos representar el número n dibujando n asteriscos en línea. Dibujando barras verticales obtenemos una composición. Por ejemplo, $* \mid * * * \mid * \mid * \mid * * \mid *$ corresponde a la composición $1 + 3 + 1 + 1 + 2 + 1$ de 9.

Si queremos que la composición tenga k partes, entonces debemos usar $(k-1)$ barras verticales. Como no se usan barras en los extremos tenemos un total de $(n-1)$ espacios interiores entre los asteriscos, por lo tanto, un total de $\binom{n-1}{k-1}$ composiciones de n en k partes. Con lo cual:

El número de composiciones de n con k partes es $\binom{n-1}{k-1}$

Podemos calcular la cantidad total de composiciones de un número calculando la cantidad de subconjuntos de

un conjunto de $n-1$ elementos, es decir la cantidad total de posibles ubicaciones de barras en los $n-1$ lugares. Ahora bien, sabemos que esta cantidad es igual a: $= 2^{n-1}$. Entonces tenemos: →

El número total de composiciones de n es 2^{n-1}.

Ahora estamos en condiciones de calcular la respuesta al problema de la organización de la fiesta. Como tenemos que calcular las composiciones de 21 en 4 partes, de acuerdo a lo visto, la respuesta es:

$$\binom{20}{3} = \frac{20.19.18}{3!}$$
$$= 1.140$$

Problema de la fiesta tercerizado. Un grupo de 21 alumnos organiza una fiesta en la que hay 5 tareas distintas para realizar. Se les permite tercerizar todas las tareas, es decir dejarlas en manos de terceros. Deben evaluar la conveniencia de esta opción. ¿De cuántas maneras pueden dividirse las tareas, si también permitimos que las mismas sean realizadas por terceros? Asumiremos un tercero por tarea.

Para resolver este problema necesitamos calcular la cantidad de formas de dividir a los 21 estudiantes en 5 grupos permitiendo que haya grupos vacíos. Para esto vamos a agregar al grupo de 21 alumnos las 5 personas que realizarían las cinco tareas en el caso que ellos no lo hagan. Tenemos ahora $21 + 5 = 26$ personas para dividir en 5 grupos, ahora no vacíos. Como en el problema anterior, la respuesta es:

$$\binom{21+5-1}{4} = \binom{25}{4}$$
$$= 12.650$$

Lo que hicimos fue agregar 5 ayudantes extras al grupo original de estudiantes a partir de allí planteamos una situación conocida: el cálculo de las composiciones en partes positivas. Esto se puede generalizar de la siguiente manera: la cantidad de *composiciones débiles* (es decir con partes no negativas) de n en k partes es igual a la cantidad de composiciones de $n + k$ en k partes, es decir:

$$\binom{n+k-1}{k-1}$$

Para resolver

2.8. Probar la siguiente identidad interpretando cada miembro de la igualdad como la cardinalidad del mismo conjunto. (Ayuda: pensar en comisiones)

$$\binom{n}{m}\binom{m}{r} = \binom{n}{r}\binom{n-r}{m-r}$$

2.9. Probar que para cada entero r, el producto de r enteros positivos consecutivos es divisible por $r!$.

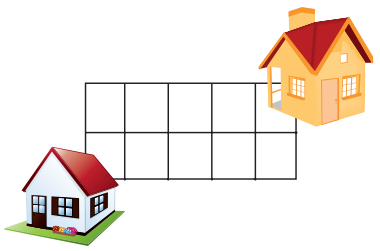


Figura 2.12.

2.10. ¿De cuántas maneras puede formarse un comité de 5 personas de un grupo de 11, en el que hay 4 profesores y 7 estudiantes si:

a) no hay restricción en la selección?
b) el comité debe incluir exactamente 2 profesores?
c) el comité debe incluir como mínimo 3 profesores?
d) hay un profesor y un alumno en particular que no pueden estar ambos en el comité?

2.11. Un alumno debe caminar desde su casa hasta la escuela por calles que se muestran en la **figura 2.12**. ¿Cuántos caminos mínimos tiene el alumno para elegir?

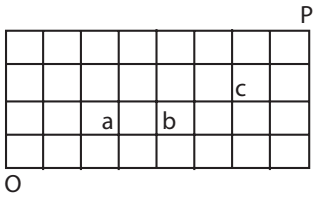
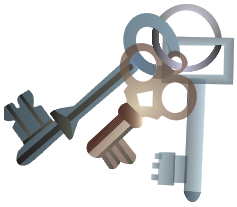


Figura 2.13.

2.12. Encontrar el número de caminos mínimos desde O hasta P, según el siguiente diagrama (**Figura 2.13**) de calles, en cada uno de los casos.

a) Los caminos deben pasar por la esquina 'a'.
b) Los caminos deben pasar por la calle 'a b ' .
c) Los caminos deben pasar por las esquinas 'a' y 'c'.
d) La calle 'a b' está cerrada.



2.13. Seis científicos están trabajando en un proyecto secreto.

Quieren guardar los documentos en un cajón bajo llaves de manera tal que se pueda abrir sólo cuando tres o más de ellos estén presentes. ¿Cuál es el mínimo número de cerraduras necesario? ¿Cuál es el mínimo número de llaves que cada científico debe llevar?

□ 2.5. Conjuntos con repetición

Problema del Senado. En el Senado se desea formar una comisión sobre enriquecimiento ilícito. La comisión debe tener 10 miembros entre los cuales debe haber al menos un representante del partido A, uno del partido B y uno del partido C. Hay 27 voluntarios: 10 pertenecen al partido A, 9 al B y 8 al C. ¿Cuántas comisiones distintas se pueden formar si no importa qué senadores específicos la forman, sino sólo el partido al cual pertenecen?

Para resolver este problema, introduciremos el concepto de multiconjunto. Un multiconjunto es un conjunto en el que se pueden repetir los elementos, es decir un conjunto con repetición. Por ejemplo, {1, 2, 2, 4, 5, 5, 5} es un multiconjunto.

Más formalmente:

Un multiconjunto (finito) M en un conjunto S es una función $v : S \to N$, tal que $\sum_{x \in S} v(x) < \infty$.

El número $v(x)$ se interpreta como el número de repeticiones de x en M. S es el "conjunto base". Se suele decir que "M es un multiconjunto sobre S" y permitiremos que $v(x) = 0$ para algún/os x de S. La cardinalidad de M es $\sum_{x \in S} v(x)$ y se denota por *card M*. Un conjunto se puede pensar como un multiconjunto en el que la función v es constantemente igual a 1 y la cardinalidad es $\sum_{x \in S} 1 =$ *card M*.

Un multiconjunto M sobre $S = \{x_1, x_2, ..., x_n\}$ con $v(x_i) = a_i$, también se puede denotar como: $M = \{x_{1,}^{a_1} x_2^{a_2}, ..., x_n^{a_n}\}$.

Diremos que M' es un submulticonjunto de M si M' es un multiconjunto sobre S con función $v' : S \to \mathbf{N}$ que satisface $v'(x) \leq v(x)$, $\forall x \in S$. Recordemos que el número de subconjuntos de un conjunto de n elementos es 2^n. Veamos ahora, ¿cuántos submulticonjuntos tiene un multiconjunto? Esto no depende sólo de la cardinalidad $n = \sum_{x \in S} v(x)$, sino de la función v misma.

El número de submulticonjuntos de un multiconjunto $M = (S, v)$ es igual a $\prod_{x \in S} (v(x)+1)$.

Pues, como debe ser $0 \leq v'(x) \leq v(x)$ para cada $x \in S$, v' puede tomar $v(x) + 1$ valores distintos. Así, usando el principio de multiplicación, tenemos que hay $\prod_{x \in S} (v(x)+1)$ posibles valores para v'.

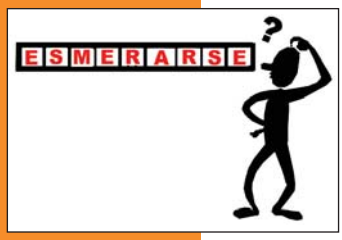
Notemos que en el caso de un conjunto $v(x) = 1$ para todo x y por lo tanto el producto es $\prod_{x \in S} (1+1) = 2^n$, lo mismo que obtuvimos anteriormente.

No vamos a desarrollar el número de submulticonjuntos de cardinalidad k de un multiconjunto, pero sí vamos a definir $\left(\!\binom{n}{k}\!\right)$ como *el número de multiconjuntos de cardinalidad k sobre un conjunto de cardinalidad n.*

Al fijar $S = \{x_1, x_2, ..., x_n\}$ entonces, un multiconjunto M sobre S queda determinado por v, con la condición de que $\sum_i v(x_i) = k$. Así, tenemos una composición de k en n enteros no negativos, que como hemos visto, es igual a $\binom{k+n-1}{k}$. Es decir: $\left(\!\binom{n}{k}\!\right) = \binom{k+n-1}{k}$.

Ahora, estamos en condiciones de resolver el problema de la comisión de enriquecimiento ilícito. Lo que importa en este problema es la composición de la comisión relativa a los partidos políticos y no a las personas. Así, lo primero que hay que hacer es asegurarse que haya uno de cada partido. En realidad, el problema consiste en elegir 7 miembros (10 – 3) entre los 24 restantes, divididos en 9 del partido A, 8 del B y 7 del C. Sin embargo, como la condición política ya está satisfecha, simplemente tenemos que escoger un multiconjunto de cardinalidad 7 sobre un conjunto S de cardinalidad 3. Así, la respuesta al número de posibilidades es:

$$\left(\!\binom{3}{7}\!\right) = \binom{3+7-1}{7}$$
$$= \binom{9}{7}$$
$$= 9.4$$
$$= 36$$



Números multinomiales

Problema de anagramas.

Calcular la cantidad de anagramas de la palabra ESMERARSE.

Un *anagrama* de una palabra dada es un reordenamiento de sus letras.

Ejemplo

La palabra PAPA, tiene los siguientes anagramas: PAPA, APAP, PAAP, PPAA, AAPP y APPA.

Veremos cómo calcular el número de anagramas que pueden tener las palabras con y sin repeticiones de sus letras.

Para responder estos problemas, vamos a introducir los Números multinomiales.

Recordemos que $n!$ es igual al número de formas de ordenar los elementos de un conjunto de n elementos. Hallaremos una fórmula para ordenar los elementos de un multiconjunto. Ahora bien, así como el número de submulticonjuntos depende no sólo de la cardinalidad sino de cómo es en sí la función v, también esta cantidad dependerá de v.

Si M = $\{x_{1,}^{a_1} x_2^{a_2},...,x_m^{a_m}\}$ y *card* $M = n$, denotaremos por $\binom{n}{a_1, a_2,..., a_m}$ a la cantidad de formas de ordenar los elementos de M.

Por ejemplo, sea $M = \{1, 1, 2, 3\}$. Entonces la cantidad de formas de ordenar los elementos de M es igual a $\binom{4}{2,1,1}$. Calculemos explícitamente este número:

Las distintas formas de ordenar los elementos de M son: 1123; 1132; 1213; 1312; 1231; 1321; 2113; 3112; 2131; 3121; 2311 y 3211; por lo tanto $\binom{4}{2,1,1} = 12$.

Hasta ahora sólo tenemos una notación. Veamos la fórmula explícita:

$$\binom{n}{a_1, a_2,..., a_m} = \binom{n}{a_1}\binom{n-a_1}{a_2}\binom{n-a_1-a_2}{a_3}\cdots\binom{n-a_1-a_2-...-a_{m-1}}{a_m}$$

Debemos ordenar un total de $a_1, a_2, ..., a_m=n$ elementos. Primero, elegimos en cuáles de los n lugares van a ir los $a_1 x_1$. Esto se puede hacer de $\binom{n}{a_1}$ formas. Como ya ocupamos a lugares, sólo nos quedan libres $n - a_1$. Escojamos en cuál ponemos los $a_2 x_2$ en $\binom{n-a_1}{a_2}$ formas. Nos quedan entonces ($n - a_1 - a_2$) lugares libres, continuando de esta manera, obtenemos el resultado expuesto y, como consecuencia, la siguiente relación:

$$\binom{n}{a_1, a_2,..., a_m} = \frac{n!}{a_1!a_2!...a_m!}$$

Veamos una prueba combinatoria de lo anterior. Supongamos que tomamos el siguiente conjunto:

$$\tilde{M} = \{ x_{(1,1)}, x_{(1,2)}, \ldots, x_{(1,a_1)}, x_{(2,1)}, x_{(2,2)}, \ldots, x_{(2,a_2)}, \ldots, x_{(m,1)}, \ldots, x_{(m,1)}, \ldots, x_{(m\,a_m)} \}$$

Como la cardinalidad de este conjunto es $a_1 + a_2 + \ldots + a_m = n$, el número total de formas de ordenar los elementos de $\tilde{M}$ es $n!$ Por otro lado, podríamos ordenar los elementos de $\tilde{M}$ ordenando primero los elementos de M en formas $\binom{n}{a_1, a_2, \ldots, a_m}$, y luego ordenando los $x_{(1,\,i)}$ de $a_1!$ formas, los $x_{(2,\,i)}$ de $a_2!$ formas, etc.

Por lo tanto, $a_1! a_2! \ldots a_m! \binom{n}{a_1, a_2, \ldots, a_m} = n!$

Como aplicación final calculamos la cantidad de Anagramas de la palabra *ESMERARSE*.

Sea M el multiconjunto formado por las letras de la palabra *'ESMERARSE'*. Es decir, $M=\{E^{3}, S^{2}, M, R^{2}, A\}$ Tenemos que calcular:

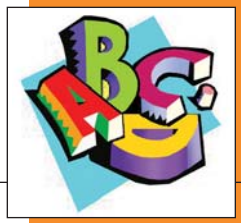
$$\binom{9}{3,2,1,2,1} = \frac{9!}{3!\ 2!\ 1!\ 2!\ 1!}$$
$$= \frac{9!}{24}$$
$$= 15120$$

Para resolver

2.14. Seis símbolos distintos se transmiten a través de un canal de comunicación. Entre los símbolos se deben insertar un total de 18 espacios en blanco, con al menos dos espacios en blanco entre cada par de símbolos. ¿De cuántas maneras se pueden transmitir los símbolos y los espacios en blanco?

2.15. ¿Cuántas palabras de 10 letras se pueden formar usando las letras: **a, b, c, d, e, f,** si:

a.- no hay restricciones;
b.- cada vocal aparece tres veces y cada consonante aparece una.



□ 2.6. El Principio de Inclusión-Exclusión

Problema de asignaturas I. Supongamos que en una escuela tenemos un grupo de 30 estudiantes. A 6 de ellos les gusta Matemática y a 15 les agrada Historia. ¿A cuántos estudiantes no les gusta ninguna de las dos materias?

Recordemos que el principio de adición, en su forma más simple, dice:

Si A y B son conjuntos finitos y disjuntos, entonces $card\,(A \cup B) = card\,A + card\,B$.

Nos preguntamos si existe una fórmula en el caso en que los conjuntos no sean disjuntos. Si A y B no son disjuntos, en la unión de los conjuntos A y B, los elementos comunes a A y B son contados dos veces. Por lo tanto será:

$$card\,(A \cup B) = card\,A + card\,B - card\,A \cap B$$

Esta relación claramente generaliza el caso en que la intersección es vacía. Cuando la intersección es vacía, el 3er término se anula y nos da el principio de adición que ya sabíamos del principio. Cuando no es vacía, vale la formula con los tres términos. Generaliza porque vale en el caso particular y en el general. Esta fórmula es la versión más simple del Principio de Inclusión-Exclusión que a continuación vamos a estudiar.

Como vimos anteriormente, para resolver ciertos problemas de conteo los conjuntos cuyos elementos queremos enumerar se separan en subconjuntos disjuntos para poder aplicar el principio de adición. Pero la tarea de dividir un conjunto en subconjuntos disjuntos puede ser muy complicada.

La última fórmula que vimos sugiere que expresemos al conjunto dado como $A \cup B$, con A y B no necesariamente disjuntos, y que luego calculemos separadamente *card A* , *card B* y *card* $(A \cap B)$ (la inclusión de *card A* y *card B* y la exclusión de *card* $(A \cap B)$ en la fórmula dará el resultado deseado para *card* $(A \cup B)$).

Volvamos ahora al problema sobre la elección de materias por un grupo de 30 alumnos entre los que hay 6 a los que les gusta Matemática, 15 a los que les gusta Historia, y se pregunta por el número de estudiantes a los que no les gusta ninguna de las dos materias. Esta pregunta no se puede responder si no se sabe la cantidad de estudiantes a los que les agradan ambas materias. Supongamos que sólo hay un estudiante así. Entonces, si llamamos A al conjunto de alumnos a los que les gusta Matemática, B al conjunto de alumnos a los que les gusta Historia, tenemos: *card A* = 6, *card B* = 15 y *card* $(A \cap B)$ = 1. Entonces:

$$\begin{aligned} card\,(A \cup B) &= 6 + 15 - 1 \\ &= 20 \end{aligned}$$

Notemos que $A \cup B$ corresponde al total de alumnos a los que les gusta por lo menos una de las dos materias, es decir, que estamos buscando su complemento, o sea los alumnos a los que no les gusta ninguna de las dos. Como el total de estudiantes es 30, y a 20 de ellos les gusta alguna de las dos materias, los alumnos a los que no les gusta ninguna serán 10.

Notemos además que hay 5 = 6 – 1 estudiantes a los que les agrada Matemática pero no Historia y 14 = 15 – 1 estudiantes a los que les agrada Historia, pero no Matemática.

Podemos generalizar lo siguiente:

Si A, B son subconjuntos de U, y si denotamos por $\bar{A}$ al complemento de A en U, entonces:
card $(\bar{A} \cap \bar{B})$ = card U – card A – card B + card (A∩B).

Como estamos restando dos veces los elementos de *card* $(A \cap B)$, debemos sumarlo una vez.

Por ejemplo: si en el problema anterior hubieran sido 10 los alumnos a los que les agrada Matemática, y a 5 de ellos también les agrada Historia, el total de alumnos a los que no les gusta ninguna de las dos habría sido 30 – 10 – 14 + 5 = 11.

Generalicemos la fórmula para 3 conjuntos. Podemos usar la fórmula anterior aplicada a los dos conjuntos $A \cup B$ y C:

$$\begin{aligned} card\,(A \cup B \cup C) &= card\,((A \cup B) \cup C) \\ &= card\,(A \cup B) + card\,C - card\,((A \cup B) \cap C) \\ &= card\,(A \cup B) + card\,C - card\,((A \cap B)\,(B \cap C)) \\ &= card\,A + card\,B - card\,(A \cap B) + card\,C - (card\,(A \cap C) + card\,(B \cap C) - card\,(A \cap C) \cap card\,(B \cap C)) \\ &= (card\,A + card\,B + card\,C) - (card\,(A \cap B) + card\,(A \cap C) + card\,(B \cap C)) + card\,(A \cap B \cap C) \end{aligned}$$

En forma combinatoria podemos razonar así: estamos descontando aquellos elementos que estén sólo en A (o sólo en B, o sólo en C) cuando restamos *card A* (o *card B* o *card C*). Ahora bien, estamos descontando dos veces a aquellos que estén en dos conjuntos solamente, digamos en A y en B: una con *card A* y otra con *card B*. Pero después los contamos una vez al sumar *card* $(A \cap B)$. Finalmente, primero descontamos 3 veces aquellos elementos de $A \cap B \cap C$, luego los contamos otras tres veces, y al final los descontamos una vez. Así, cada elemento es contado sólo una vez dándonos la relación deseada.

Generalizando tenemos:

Si A ,B y C son subconjuntos de U, entonces :
card $(\bar{A} \cap \bar{B} \cap \bar{C})$ = card U – card A – card B – card C + card $(A \cap B)$ + card $(A \cap C)|$ + card $(B \cap C)$ – card $(A \cap B \cap C)$.

Problema de asignaturas II. En el turno mañana de cuarto año de una escuela hay 100 estudiantes. A 40 de ellos les gusta Matemática, a 40 Historia y a 40 Geografía. A 20 les gusta Historia y Matemática, a 20 Historia y Geografía, y a 20 Matemática y Geografía. Además hay 10 estudiantes a los que les gustan las tres materias. ¿A cuántos estudiantes no les gusta ninguna materia?

Por la fórmula anterior habrá: 100 – 40 – 40 – 40 + 20 + 20 + 20 – 10 = 30

Problema de primos. ¿Cuántos números enteros hay menores que 154 que sean coprimos con 154?

Recordemos que dos números son coprimos cuando su máximo común divisor es 1, es decir, no existe número natural distinto de 1 que divida a ambos números.

Llamemos N al conjunto cuya cardinalidad queremos calcular. Notemos que 154 = 2 . 7 . 11 por lo que queremos contar aquellos números que no tienen a 2, ni a 7, ni a 11 como divisores.

Sean A el conjunto de números que sí son divisibles por 2, B el de los divisibles por 7 y C los divisibles por 11, entonces, queremos calcular *card* $(\bar{A} \cap \bar{B} \cap \bar{C})$.

Observemos que $A \cap B$ son aquellos números divisibles por $2 \cdot 7 = 14$, que $A \cap C$ son aquellos divisibles por $2 \cdot 11 = 22$, $B \cap C$ los divisibles por $7 \cdot 11 = 77$, y $A \cap B \cap C$ los divisibles por $2 \cdot 7 \cdot 11 = 154$. Así tenemos:

$$card\ \ A = \frac{154}{2} = 77, \quad card\ |B| = \frac{154}{7} = 22, \quad card\ |C| = \frac{154}{11} = 14$$

Con lo que $card\ (A \cap B) = \frac{154}{14}$

$= 11$

Calculando en forma análoga obtenemos:

$$\begin{aligned} card\ \mathrm{N} &= card\ (\bar{A} \cap \bar{B} \cap \bar{C}) \\ &= 154 - 77 - 22 - 14 + 11 + 7 + 2 - 1 \\ &= 60 \end{aligned}$$

Observación

La función de Euler

Alrededor de 1760, en un intento por generalizar un resultado de Teoría de Números de Fermat, el matemático suizo Leonard Euler (1707-1783) introdujo la siguiente noción: para un $n \in \mathbf{N}$, sea $\Phi(n)$ el número de enteros comprendidos entre 1 y n que son coprimos con n. La función $\Phi(n)$, conocida como la función de Euler juega un papel importantísimo en la matemática actual.

Si p, q, r son primos y si N es el conjunto de números menores a $(p\ q\ r)$ coprimos a él, entonces, razonando en forma análoga al problema de primos que vimos anteriormente, tenemos:

$$card\ N = p\ q\ r - p\ q - p\ r - q\ r + p + q + r - 1 = (p-1)(q-1)(r-1)$$

Por lo que para $n = p\ q\ r$, será: $\boxed{\Phi(n) = (p-1)(q-1)(r-1)}$

Veamos cómo generalizamos el principio de Inclusión-Exclusión:

Principio de Inclusión-Exclusión. Dados n subconjuntos de un conjunto U de cardinalidad N. Sean $A_1, A_2, \ldots, A_n$ los subconjuntos de U y para cada k, $1 \le k \le n$ sea S_k la suma de los cardinales de las intersecciones entre k de los A_i. Es decir, $S_1 = \sum$ card A_i, card $S_2 = \sum$ card $(A_i \cap A_j)$, etc. Entonces:

$$\text{card}\left(\bar{A}_1 \cap \bar{A}_2 \cap \cdots \cap \bar{A}_n\right) = N - S_1 + S_2 - S_3 + \cdots (-1)^k S_k + \cdots + (-1)^n S_n$$

Con un análisis combinatorio de la fórmula veamos cómo se cuenta cada elemento $x \in U$:

- Si $x \in (A_1 \cap \bar{A}_2 \cap \bar{} \ldots \cap A_n)$, entonces x es contado una vez por el lado izquierdo,

una vez por el lado derecho en N, y luego no se vuelve a contar porque no está en ningún A_i, los S_k no lo cuentan.

- Si x pertenece a exactamente m de los A_i, entonces en el lado izquierdo x no se cuenta, y en el lado derecho x se cuenta una vez por N, m veces por S_1 (porque x está en exactamente m de los A_i), $\binom{m}{2}$ veces por S_2 (porque x está en todas las $\binom{m}{2}$ intersecciones de los m A_i en los que está), y en general $\binom{m}{k}$ veces por S_k, si $k \leq m$. Obviamente, S_k lo cuenta 0 veces si $k > m$, porque x sólo figura en m de los A_i.

Así, el lado derecho cuenta a x un total de $1 - \binom{m}{1} + \binom{m}{2} - \binom{m}{3} + \cdots + (-1)^m \binom{m}{m} = 0$ ya que anteriormente vimos que se satisface $\sum_k (-1)^k \binom{n}{k} = 0$.

Esta generalización permitirá resolver el **Problema de los sombreros**. Si n hombres entran a un restaurante, dejan sus sombreros y luego al irse toman los sombreros al azar, ¿de cuántas maneras se pueden retirar los sombreros de forma tal que nadie tome el sombrero correcto?

Nuestro universo U es la cantidad total de formas de elegir los sombreros. Por lo que $N = n!$ Sea A_i el conjunto de aquellas distribuciones de sombreros en las que la persona i toma su propio sombrero. Entonces, como vamos a contar los casos en que nadie toma el sombrero correcto, necesitamos calcular $card\,(\bar{A}_1 \cap \bar{A}_2 \cap \ldots \cap \bar{A}_n)$. Ahora bien, si la persona i toma su propio sombrero, las otras $n - i$ personas ya no pueden tomarlo porque $card\,A_i = (n - i)!$ para todo i.

Además si $i \neq j$, entonces es el conjunto de aquellas elecciones, tales que la persona i y la persona j, ambas, obtienen su propio sombrero. Por lo tanto,

$$card\,(A_i \cap A_j) = (n-2)!.$$

Razonando en forma análoga, obtenemos en general que $card\,(A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}) = (n-k)!$.

Ahora necesitamos saber la cantidad de posibles intersecciones entre k conjuntos. Esto es equivalente a elegir los k conjuntos que van a ser intersecados, es decir que hay exactamente $\binom{m}{k}$. Por lo que tenemos:

$$|A_1 \cap A_2 \cap \ldots \cap A_n| = n! - \binom{n}{1}(n-1)! + \ldots + (-1)^k \binom{n}{k}(n-k)! + \ldots + (-1)^n \binom{n}{n} 0!$$

$$= \sum_{k=0}^{n} (-1)^k \binom{n}{k}(n-k)!$$

$$= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!}$$

$$= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

Así, la cantidad de formas posibles de retirar los n sombreros sin que nadie tome el suyo es:

$$n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}$$

Al estudiar probabilidad se ve que la probabilidad de un evento es igual al número de casos favorables, dividido el número total de casos. En esta situación, la probabilidad de que nadie reciba su propio sombrero es:

$$n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}\cdot\frac{1}{n!}=\sum_{k=0}^{n}\frac{(-1)^k}{k!}$$
$$\approx e^{(-1)}$$

Estos son los primeros términos en el desarrollo en serie de $e^{(-1)}$. La convergencia es muy rápida y, por ejemplo para $n = 6$, la suma da 0,367888 , mientras que $e^{(-1)} = 0{,}367879$. Así, podemos decir que la probabilidad de que todos tomen un sombrero equivocado es $e^{(-1)}$. Es sorprendente que esta probabilidad sea la misma tanto si se trata de 10 como de 10.000 personas con sus sombreros.

Solución del "Problème des Ménages" o "Problema de los matrimonios"

¿Cuántas maneras hay de sentar n matrimonios alrededor de una mesa de forma tal que hombres y mujeres estén alternados, y ninguna mujer esté sentada al lado de su esposo?

Para llegar a la solución primero resolveremos dos problemas más simples, por sí mismos interesantes.

Problema de vecindad I. Sea $X = \{1, 2, ...,n\}$ donde $n \in \mathbf{N}$. Calcular el número de subconjuntos de X de r elementos tal que no contengan enteros consecutivos.

Ejemplo

Sea $X = \{1, 2, ...,7\}$. Todos los subconjuntos de X de tres elementos sin enteros consecutivos son: {1,3,5},{1,3,6},{1,3,7},{1,4,6},{1,4,7},{1,5,7},{2,4,6},{2,4,7},{2,5,7}, {3,5,7}. Es decir, hay $10 = \binom{5}{3}$ conjuntos.

Volvamos al caso general. Sea A el conjunto de subconjuntos de X con r elementos, sin elementos consecutivos y B el conjunto de los subconjuntos de r elementos de Y, donde $Y = \{1, 2,\ldots,n-(r-1)\}$.

Asignaremos a cada elemento de A un único elemento de B, siendo todas las asignaciones diferentes y todo elemento de B asignado. De esta forma, vemos que A y B tienen la misma cardinalidad. (En matemática esta asignación se llama biyección entre A y B).

Sea $S = \{s_1, s_2, ..., s_r\}$un miembro de A. Podemos asumir, sin perder generalidad, que $s_1 < s_2 < s_3 ... < s_r$. Definimos $f: A \rightarrow B$

$$f(S) = \{s_1, s_2 - 1, s_3 - 2, ..., s_r - (r-1)\}$$

Observemos que como S_i y S_{i+1} no son consecutivos, todos los números en $f(S)$ son distintos. Por lo que $f(S) \in B$, por lo tanto f es realmente una función de A en B.

Para ver que las asignaciones son distintas, sean S y S' en A y supongamos lo contrario, es decir que $f(S) = f(S')$. Entonces $S_i = S_i' \forall\ 1 \leq i \leq r$, por lo que las asignaciones son distintas.

Para ver que todo B es asignado, sea $T = \{t_1, t_2, ..., t_r\} \in B$ y sea entonces $S = \{t_1, t_2 + 1, t_3 + 2 ..., t_r + (r-1)\}$ claramente no hay enteros consecutivos en S, por lo que $S \in A$.

También $f(S) = T$ por definición, con lo que f alcanza todo B y por lo tanto card A = card B, siendo la cardinalidad de B fácilmente calculable:

$$card\ B = card\ A = \binom{n - r + 1}{r}$$

Con esto, resolvimos el primero de los problemas.

Problema de vecindad II. Supongamos que los números 1 , 2 , …, m con $m \geq 3$ son ubicados alrededor de un círculo. Para $0 \leq k \leq \left[\frac{m}{2}\right]$, ($\left[\frac{m}{2}\right]$ el mayor entero menor o igual a $\left[\frac{m}{2}\right]$), calcular α (k) el número de subconjuntos de k elementos de {1,2, ..., m} de manera que no haya elementos adyacentes alrededor del círculo.

Ejemplo

Si m = 10 y k = 4, y ubicamos los 10 números alrededor de un círculo en su orden 'natural', entonces {1, 3, 6, 8} y {3, 5, 8, 10} son de esos subconjuntos, pero {1, 6, 8, 10} y {3, 5, 9, 10} no lo son.

Notemos que si $\left[\frac{m}{2}\right] < k$, no pueden existir dichos conjuntos ya que necesariamente aparecen elementos adyacentes.

Para cada i = 1, 2, …, m, sea α_i el número de tales subconjuntos de k elementos de {1, 2, ..., m} que contienen a 'i'. Por simetría, $\alpha_1 = \alpha_2 = ... = \alpha_m$.

Contamos α_1. Si B es un subconjunto de cardinalidad k conteniendo a 1, entonces por hipótesis, 2 , $m \notin B$, por lo que los restantes $k - 1$ elementos de B deben ser elegidos entre {3, 4, …, $m - 1$}, tal que no haya dos adyacentes.

Ahora, como el conjunto {3, 4, …, $m - 1$} es lineal y no en círculo, podemos usar el resultado del problema anterior, con lo que tenemos:

$$\alpha_1 = \binom{(m-3) - (k-1) + 1}{k-1}$$
$$= \binom{m - k - 1}{k - 1}$$

Y por lo tanto

$$\sum_{i=1}^{m}\alpha_i = m\binom{m-k-1}{k-1}$$

Notemos ahora que $\alpha(k) = \frac{m}{k}\alpha_1$ ya que al elegir el conjunto α_1 elegimos un primer elemento de entre $\{1, 2, \ldots, m\}$ que puede hacerse en m formas, por lo que multiplicamos por m. Por otro lado, podríamos elegir el mismo conjunto α_1 empezando con otro número distinto, y esto puede suceder en k maneras, por lo que dividimos por k. Entonces tenemos:

$$\alpha(k) = \frac{m}{k}\binom{m-k-1}{k-1}$$

Ahora estamos en condiciones de resolver el *Problème des Ménages.*

Supongamos que las sillas ubicadas alrededor de la mesa y las parejas (la mujer i es pareja del hombre i) están numeradas. Sentamos a los hombres determinando a la derecha del hombre i, la posición i.

Definimos u_n como el número de permutaciones de $\{1, 2, \ldots, n\}$ que no satisfacen ninguna de las siguientes $2n$ condiciones:

1. la mujer 1 está en la primera posición,
2. la mujer 1 está en la segunda posición,
3. la mujer 2 está en la segunda posición,
4. la mujer 2 está en la tercera posición,

⋮

$2n$ -1. la mujer n está en la enésima posición,
$2n$. la mujer n está en la primera posición.

Veremos que la cantidad de formas de sentar n parejas, alternando mujeres y hombres de manera tal que nadie esté sentado al lado de su compañero/a es $2n!\, u_n$.

Cuando sentamos a los hombres pueden ocupar los asientos numerados pares o bien los impares, y lo pueden hacer en $n!$ formas. Las mujeres se pueden sentar en u_n formas y así, por la manera en que definimos las condiciones, no estarán sentadas al lado de su esposo. Por lo que el problema será resuelto si podemos calcular u_n.

El número de formas de sentar a las mujeres sin ninguna restricción es $n!$ De ésas, necesitamos quitar todas aquellas permutaciones que satisfagan alguna de las $2n$ condiciones listadas anteriormente. Sea A_i el conjunto de todas las permutaciones que satisfacen condición i de la lista anterior. Entonces, aplicando el principio de Inclusión-Exclusión, y si S_k es la suma de los cardinales de las intersecciones entre k de los A_i, es decir, $S_1 = \sum card\, A_i$, $S_2 = \sum card\,(A_i \cap A_j)$, entonces:

$$u_n = card\,(\overline{A}_1 \cap \overline{A}_2 \cap \ldots \cap \overline{A}_n)$$

$$= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!}$$
$$= n! - S_1 + S_2 - S_3 + \ldots (-1)^k S_k + \cdots + (-1)^n S_n$$

Se puede simplificar esta expresión. Por ejemplo $A_1 \bigcap A_2$ son las permutaciones en las que la mujer 1 está en la primera y en la segunda posición. Es decir, es imposible, por lo que *card* $(A_1 \bigcap A_2) = 0$. En general, por motivos análogos, cada vez que tengamos dos condiciones consecutivas la cardinalidad de la intersección será cero. Por lo tanto, necesitamos saber el número de conjuntos de cardinalidad no nula. Podemos calcularlo usando el primer problema, es decir calculando la cantidad de formas de elegir dos condiciones no consecutivas de entre las $2n$ condiciones. De acuerdo a lo visto habrá:

$$\binom{2n-2}{2} \frac{2n}{2n-2}$$

Además, la cardinalidad de cada uno de esos conjuntos es $(n-2)!$ ya que se fijaron dos condiciones.

Hasta ahora sentamos a dos mujeres y las otras pueden hacerlo en $(n-2)!$ maneras, por lo que el número de formas que cualquier par de condiciones se satisfagan al mismo tiempo es:

$$\binom{2n-2}{2} \frac{2n}{2n-2} (n-2)!$$

Lo mismo es cierto si tratamos de elegir tres condiciones no consecutivas de a pares. Por lo visto en el problema previo, la cantidad de formas de elegir las tres permutaciones será:

$\binom{2n-3}{3} \frac{2n}{2n-3}$ y el número de formas de sentar las restantes $n-3$ mujeres será $(n-3)!$

Esto puede extenderse, obteniendo:

$$u_n = n! - \frac{2n}{2n-1}\binom{2n-1}{1}(n-1)! + \frac{2n}{2n-2}\binom{2n-2}{2}(n-2)! - \frac{2n}{2n-3}\binom{2n-3}{3}(n-3)!$$

Por lo que la solución al problema de los matrimonios se puede escribir así:

$$2n! \sum_{i=0}^{n} (-1)^i \frac{2n}{2n-i}\binom{2n-i}{i}(n-i)!\, 2n!$$

Para finalizar, debemos eliminar las rotaciones alrededor de la mesa de las distintas permutaciones por lo que debemos dividir por $2n$ obteniendo que:

El número de formas que hay de sentar n matrimonios alrededor de una mesa de manera tal que hombres y mujeres estén alternados y ninguna mujer esté sentada al lado de su esposo es:

$$(n-1)!\sum_{i=0}^{n}(-1)^i\frac{2n}{2n-i}\binom{2n-i}{i}(n-i)!$$

El número de soluciones para distintos valores de n crece rápidamente. En la tabla mostramos los valores para los primeros n, en particular está la respuesta al problema de 4 matrimonios: hay 12 maneras de sentarlos.

n	2	3	4	5	6	7
$(n-1)!\,u_n$	0	2	12	312	9.600	416.880

Nota

Nota a la solución del Problème des Ménages.

La solución del Problème des Ménages que hemos visto es la tradicional. En los últimos años Peter G. Doyle y Kenneth P. Bogart han publicado su solución en el trabajo "Non-sexist solution of the ménage problem" (ver Bibliografía) (Solución del problema de ménages asexuada). Su nombre se debe a que ellos no sientan en la mesa a los hombres o a las mujeres primero como lo hemos hecho aquí. Doyle y Bogart resuelven un problema simplificado de una manera directa con el Principio de Inclusión-Exclusión, y luego lo extienden obteniendo en una forma muy directa la solución del problema. Resulta que la tradición de sentar a uno de los dos sexos primero (cosa que parecía natural y que simplificaba) hizo que tomara tanto tiempo solucionar el problema de ménages.

Para resolver

2.16. Si 10 cartas son puestas al azar en sobres con destinatario, ¿cuántas maneras hay de poner todas las cartas en un sobre equivocado?

2.17. Un año es bisiesto si, o bien es múltiplo de 4, pero no de 100, o es múltiplo de 400. Por ejemplo: 1600 y 1924 fueron años bisiestos, pero 2200 no lo será. Calcular la cantidad de años bisiestos entre 1000 y 3000 inclusive.

2.18. ¿Cuántos números enteros hay comprendidos entre 1 y 1.000.000 que son divisibles por 2, por 3 o por ambos?

□ 2.6. Apéndice: El principio del palomar

Este principio de la combinatoria, en contraste a los que hemos utilizado para contar, no nos da información numérica, sino que trata sobre la existencia de alguna situación o esquema. Los problemas son tan sorprendentes y simples que hacen que este principio sea tratado dentro de este marco de "contar sin enumerar".

Problema de correos electrónicos. Diecisiete personas se comunican unas con otras por correo electrónico, cada una con todo el resto. En sus mensajes se discuten sólo tres temas distintos. Cada par de comunicandos trata sólo uno de esos tres temas. Probar que hay al menos tres personas que se escriben unos a otros sobre el mismo tema.

Daremos la solución del problema más adelante. Ahora veamos los enunciados de dos problemas más simples y, a la vez, íntimamente relacionados.

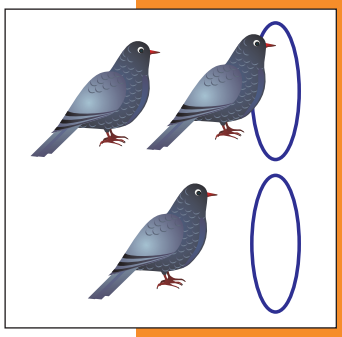
Problema de amistad. Probar que en una reunión cualquiera de seis personas, hay tres personas que, o bien son amigos entre sí, o son desconocidos entre sí.

Problema de triángulos coloreados. Seis puntos están ubicados en el espacio tal que no hay tres de ellos alineados, ni cuatro en un plano. Se dibujan los $\binom{6}{2} = 15$ segmentos, se unen de a pares, y se pintan algunos rojos y los otros azules. Probar que existe al menos un triángulo con sus tres lados del mismo color.

Los enunciados que siguen tienen la misma naturaleza matemática:

"En todo grupo de dos o más personas, hay dos que tienen el mismo número de amigos en el grupo"

"Dado un conjunto A de 5 números hay tres elementos de A cuya suma es divisible por tres."



Este tipo de problemas se refiere a la existencia de un cierto tipo de cantidad, esquema o arreglo. El Principio de las Casillas o del Palomar, es fundamental para resolverlos.

Si tres palomas deben ser ubicadas en dos compartimientos, entonces es obvio que uno de los compartimientos tendrá al menos dos palomas. Una afirmación que generaliza esta observación es:

Principio del Palomar. Sean k y n dos enteros positivos cualesquiera. Si al menos k n + 1 objetos son distribuidos en n cajas, entonces una de las cajas debe contener al menos k + 1 objetos. En particular, si al menos n + 1 objetos deben ser colocados en n cajas, entonces una de las cajas debe contener al menos dos objetos.

Para probar este principio, basta notar que si ninguna caja contiene k + 1 o más objetos entonces todas las cajas contienen a lo sumo k objetos. Esto implica que el número total de objetos distribuidos es a lo sumo $k\,n$, lo cual es un absurdo.

Este principio parece trivial, sin embargo es una herramienta poderosa para probar la existencia de ciertos elementos en Matemática. Veamos otro ejemplo:

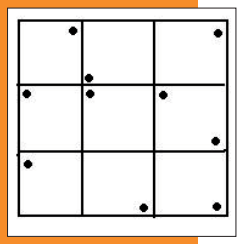
Ejemplo

En cualquier grupo de 7 personas debe haber al menos 4 del mismo sexo.

Supongamos las personas los objetos a encasillar, y las dos cajas disponibles V y M (varón y mujer). Si una persona es mujer se la ubica en M, y si es varón en V. Entonces, los 7 = 3.2 + 1 objetos se ubican en 2 (= n) cajas. Por el principio de las casillas, sabemos que hay una caja que contiene al menos 3 + 1 = k + 1 objetos, es decir, hay al menos 4 personas del mismo sexo.

Como vemos, al aplicar el principio de las casillas debemos identificar los 'objetos' tanto como las 'cajas'. Además, debemos saber los valores de k y n (número de cajas) y estar seguros de que el número de objetos sea al menos $k\,n + 1$.

Problema de falta de espacio. Mostrar que para cualquier grupo de 10 personas que están dentro de una habitación cuadrada de 3 m de lado hay dos personas que distan entre sí a lo sumo $\sqrt{2}\ m$.



Nos preguntamos, ¿cuáles son los objetos?, ¿cuáles son las cajas? Parece lógico pensar a las 10 personas como objetos. Notemos que necesitamos probar la existencia de dos de ellas que estén a una distancia máxima de $\sqrt{2}\ m$.

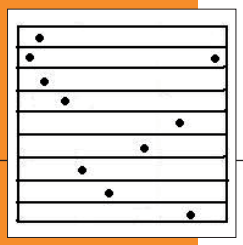
Esto indica que $k + 1 = 2$, es decir $k = 1$, y nos sugiere dividir a la habitación 3 x 3 en digamos n regiones de manera que dentro de una región la distancia entre las personas sea menor que $\sqrt{2}\ m$.

Entonces dividamos la habitación en 9 cuadrados unitarios de lado $1m$. Estas serán las cajas. Sea A cualquier conjunto de 10 personas elegidas del cuadrado grande 3 x 3 (nuestros objetos a distribuir). Como cada persona de A está contenida en al menos uno de los 9 cuadrados o cajas, y como $10 > 9$, por el Principio del Palomar hay una caja o cuadrado unidad que contiene al menos dos objetos o personas de A. Ahora la distancia máxima entre dos personas que están en el mismo cuadrado será la medida de la diagonal del mismo, es decir, $\sqrt{(1+1)}\ m = \sqrt{2}\ m$. Por lo que hemos probado la existencia de dos personas cuya distancia es a lo sumo $\sqrt{2}\ m$.

Observaciones

1) El principio de las casillas nos asegura la existencia de objetos, pero no identifica ni cuáles son estos objetos, ni la caja que los contiene.

2) Si en lugar de dividir el cuadrado en 9 cuadrados unitarios lo hubiéramos dividido en 9 rectángulos horizontales de lado $\frac{1}{9}$ y 1 y aplicamos el principio de las casillas, la información que obtenemos es que dentro de algún rectángulo hay al menos dos personas. Pero en este caso no podríamos concluir que esas personas distan menos que $\sqrt{2}\ m$. Esto demuestra la importancia de elegir las cajas en forma apropiada.



Problema de paridad. Sea $A = \{a_1, a_2, \ldots a_5\}$ un conjunto de 5 enteros positivos. Probar que para cualquier permutación $a_{i_1}, a_{i_2}, a_{i_3}, a_{i_4}, a_{i_5}$ de A, el producto $(a_{i_1} - a_1)\,(a_{i_2} - a_2)\,(a_{i_5} - a_5)$ es siempre par.

Ejemplo

Si $a_1 = 2, a_2 = 5, a_3 = 7, a_4 = 3, a_5 = 8$ en tanto que $a_{i_1} = a_4, a_{i_2} = a_3, a_{i_3} = a_5, a_{i_4} = a_1, a_{i_5} = a_4, a_{i_1} = a_2$, entonces el producto en cuestión es:

$$(3 - 2)(7 - 5)(8 - 7)(2 - 3)(5 - 8) = 6$$

Para probar que el producto es par basta con probar la existencia de un factor par. Además, una diferencia entre números enteros es par si y sólo si, ambos son pares o ambos son impares, es decir tienen la misma paridad. Por lo que creamos dos cajas, una para los números pares, y la otra para los im-

pares. Como tenemos 5 objetos para distribuir en dos cajas, por el principio de las casillas, tenemos que existen al menos tres números en la misma caja, es decir con la misma paridad. Entre estos tres números debe haber un par de ellos que sean algún número de A y su imagen por la permutación, ya que de lo contrario A tendría por lo menos 6 elementos (los tres números en la caja más sus tres imágenes por la permutación). Entonces, la diferencia entre esos dos números de igual paridad nos da el factor par que estábamos buscando. Así el producto entre las cinco diferencias es par.

La propiedad anterior es válida para cualquier número impar de enteros positivos y no es válida si el número de enteros es par.

Problema de sumas. Sea $X \subseteq \{1, 2, 3, ..., 99\}$ con $|X| = 10$ Mostrar que es posible seleccionar dos subconjuntos propios disjuntos de X, Y y Z tal que $\sum_{y \in Y} y = \sum_{z \in Z} z$.

Ejemplo

X = {2, 7, 15, 19, 23, 50, 56, 60, 66, 99} tomamos Y = {19, 50} y Z = {2, 7, 60}, entonces se cumple que:

$$\begin{aligned}\sum_{y \in Y} y &= 19 + 50 \\ &= 69 \\ &= 2 + 7 + 60 \\ &= \sum_{z \in Z} z\end{aligned}$$

La conclusión a probar sugiere que los objetos a distribuir son los subconjuntos propios no vacíos de X, y que de alguna manera debemos crear nuestras cajas para sus posibles sumas. Si el número de objetos es mayor que el número de cajas, entonces hay dos subconjuntos no vacíos propios de X que tendrán la misma suma. Esto es muy parecido a lo que queremos probar. Entonces nos queda definir el número de objetos y el número de cajas.

Como $|X| = 10$, sabemos que la cantidad total de subgrupos propios no vacíos de X (excluyendo X y el conjunto vacío) es $2^{10} - 2 = 1.022$.

Por otro lado, para cada subconjunto no vacío propio A de X, tenemos:

$$1 \leq \sum_{a \in A} a \leq 91 + 92 + ... + 99 = 855$$

o sea, que la suma de los números de cada A están entre 1 y 855. Entonces, tenemos 1.022 subconjuntos propios de X no vacíos que serán los objetos y creamos 855 cajas para las posibles sumas 1, 2, 3, ...,855 . Como 1.022 > 855 , por el principio de las casillas, existen dos subconjuntos B, C de X no vacíos y propios que tienen la misma suma, es decir:

$$\sum_{b \in B} b = \sum_{c \in C} c$$

Estos dos conjuntos no necesariamente son disjuntos. Como $B \not\subset C$ y $C \not\subset B$ definimos $Y = B - (B \cap C)$ y $Z = C - (B \cap C)$ entonces Y y Z son disjuntos y satisfacen $\sum_{y \in Y} y = \sum_{z \in Z} z$ ya que B y C la satisfacen y, a ambos, le quitamos el mismo conjunto . Por lo tanto, tenemos los dos conjuntos con las propiedades requeridas.

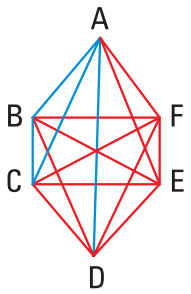


Figura 2.14

Ahora que entendemos cómo funciona el principio de las casillas, estamos en condiciones de empezar a resolver los problemas planteados al principio.

Comencemos con el problema de la coloración de triángulos: seis puntos están ubicados en el espacio tal que no hay tres de ellos alineados, ni cuatro en un plano. Se dibujan los $\binom{6}{2} = 15$ segmentos que los unen de a pares, y se pintan algunos segmentos rojos y los otros azules. Probar que existe algún triángulo con sus tres lados del mismo color.

Tenemos los seis puntos *A, B, C, D, E, F* (**Figura 2.14**) unidos por segmentos. De cada punto parten cinco segmentos. Elijamos un punto, digamos *A*. Los cinco segmentos que llegan a *A* (*AB, AC, AD, AE, AF*) son coloreados con rojo o azul. Por el principio de las casillas, considerando a los segmentos como objetos y los dos colores como cajas, uno de los colores (digamos el azul) se usa para colorear al menos tres de los cinco segmentos. Supongamos, sin pérdida de generalidad, que los segmentos azules son *AB, AC* y *AD* . Miremos el triángulo formado por los tres vértices opuestos a *A* vía esos tres segmentos, es decir, *BC, BD* y *CD* . Si cualquiera de ellos, digamos *BC*, está coloreado azul entonces tenemos el triángulo *ABC* azul. Si ninguno de ellos es azul, entonces los tres segmentos deben ser rojos obteniendo así un triángulo rojo, el *BCD* . Por lo que hemos probado que siempre existe un triángulo de un único color.

De la misma forma se resuelve el problema de amistad. Probar que en una reunión cualquiera de seis personas hay tres personas que, o bien son amigos entre sí, o son desconocidos entre sí.

Si representamos las seis personas por seis vértices *A, B, C, D, E, F,* y coloreamos azul al segmento que une a dos personas desconocidas, y rojo a los segmentos que unen personas amigas, por el problema anterior, existe un triángulo de algún color, es decir un trío, tal que son mutuamente amigos, o mutuamente desconocidos.

Finalmente, resolveremos el primer problema propuesto sobre correos electrónicos que dice: 17 personas se comunican unas con otras por correo electrónico, cada una con todo el resto. En sus mensajes sólo tres temas distintos se discuten. Cada par de comunicandos trata sólo uno de esos tres temas. Probar que hay al menos tres personas que se escriben unos a otros sobre el mismo tema.

Representemos a las 17 personas por 17 vértices *A, B, C,* ... y los unimos con segmentos. Coloreamos los segmentos con tres colores distintos, azul, rojo y amarillo de acuerdo al tema que las personas unidas por el segmento están tratando. Consideremos el vértice *A*. Entonces los 16 segmentos que parten de *A*, están coloreados por alguno de los tres colores. Como $16 = 5.3 + 1$, por el principio de las casillas, un color digamos azul, se usa para colorear al menos $5 + 1 = 6$ segmentos. Supongamos, sin pérdida de generalidad, que los azules son *AB*, *AC*, *AD*, *AE*, *AF*, *AG* . Ahora consideremos la configuración que consiste de los 6 vértices *B, C, D, E, F, G* junto con los 15 segmentos que unen los seis puntos. Si alguno de esos lados, digamos el *BC*, está coloreado azul entonces tenemos un triángulo azul, el *ABC*. Si ninguno de ellos es azul, entonces los 15 lados están colorea-

dos rojos o amarillos. Pero entonces, el caso queda reducido al problema de los 15 lados coloreados por 2 colores por lo que habrá un triángulo rojo o uno amarillo. En cualquier caso, existe un triángulo con sus tres lados del mismo color lo que significa que hay al menos tres personas que en sus comunicaciones están tratando el mismo tema.

Para resolver

2.19. En todo grupo de 13 personas debe haber al menos dos cuyos cumpleaños sean el mismo mes.
2.20. En cualquier grupo de 3.000 personas hay al menos 9 que comparten la fecha de cumpleaños.
2.21. Mostrar que en cualquier conjunto de 5 números hay 3 de ellos cuya suma es divisible por 3.
2.22. Entre 15 niños juntaron 100 manzanas. Probar que hay al menos dos de ellos que recogieron igual número de manzanas.

3. Una aventura por el infinito

Por Juan Pablo Rossetti

1. ¿Qué es el infinito?
2. Hotel Hilbert
3. La paradoja de Aquiles y la tortuga.
4. Sumas infinitas
5. La serie geométrica y la serie armónica
6. ¡Los números racionales son numerables! ... ¿y los reales?
7. ¡Los números reales no son numerables!
8. El método de la diagonal de Cantor
9. ¡Hay infinitos tipos de infinito!

□ 3.1. ¿Qué es el infinito?

- Bueno Clara, esto no es fácil de contestar porque no es fácil saberlo. Los seres humanos llevan siglos pensándolo. Muchas personas brillantes dedicaron a este tema buena parte de su vida, y aún así, todavía queda mucho por conocer.

- ¿Pero entonces, nunca vamos a entenderlo?

- No lo sé -contestó el Maestro, algo ruborizado porque no podía satisfacer la curiosidad de la niña, que siempre le hacía muchas preguntas, y generalmente se quedaba muy contenta con sus respuestas-. Pero quizás te pueda contar algunas cosas que van a gustarte.

- ¡Qué suerte! Pensé que me estaba diciendo que no valía la pena pensar en el infinito, que no podríamos comprenderlo.

- En verdad, quizá no podamos entenderlo bien. Pero ¿acaso alguien en este mundo comprende algo totalmente? A veces creemos que comprendemos algo porque ya oímos hablar sobre ese tema, o podemos decir algo sobre él o, a lo sumo, nos acostumbramos a eso. Y así, nos quedamos tranquilos, creyendo que lo entendemos, aunque en realidad no sea tan así. De cualquier modo, creo que sería muy bueno que escucharas lo que te quiero contar sobre el infinito. Te aseguro que podríamos aprender cosas muy interesantes.

Clara se quedó mirando al Maestro con curiosidad sobre esta nueva lección y con grandes expectativas. Ya había tenido muchas lecciones durante éste, su primer año en el colegio secundario, y le habían gustado.

El Maestro comenzó:
- Pensá en algunos conjuntos que ya conocemos, como por ejemplo, en **N**, el conjunto de los números naturales; en **Z**, el de los números enteros; **Q**, los números fraccionarios, también llamados racionales; o **R**, los números reales. Acordate que podemos escribir estos conjuntos así:

$$\mathbf{N} = \{1, 2, 3, 4, 5, 6...\}$$
$$\mathbf{Z} = \{..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}$$
$$\mathbf{Q} = \left\{ \frac{m}{n} : m, n \in Z, n \neq 0 \right\}$$

No es fácil describir al conjunto **R**, pero sabemos que consta de los números racionales y los irracionales. Estos últimos son los que tienen una expresión decimal que no termina nunca, ni es periódica. Pero no nos preocupemos por eso ahora.
¿Estos conjuntos tienen algo en común? ¿Qué opinás?

- No estoy segura. ¿Será que son todos conjuntos de números? -preguntó la niña, transformando su inseguro tono de voz al comienzo en una alegre sonrisa, al ir descubriendo que estaba en lo cierto.

- Sí, así es, Clara. Ahora, decime algo acerca de la cantidad de elementos de estos conjuntos.

- Perdón. ¿Qué quiere decir con eso, Maestro?

- Es sencillo. Por ejemplo, el conjunto {1, 2, 3} tiene tres elementos, el 1, el 2 y el 3, nada más. El conjunto {-1, 0, 1} también tiene tres elementos. El conjunto formado por los meses de un año tiene 12 elementos. Esto es simple. Ahora pensemos en el conjunto de los números naturales, que denotamos con **N**, o lo que es lo mismo, el conjunto {1, 2, 3, 4, 5,...}. Fijate que los puntos suspensivos indican que los números siguen, y lo hacen indefinidamente. Ahora te hago una pregunta: ¿Cuántos elementos tiene **N**? O lo mismo, ¿cuántos números naturales hay?

- Me acuerdo que una vez aprendimos que no hay un número que sea mayor que todos los demás.

- Así es, Clara. Si proponés un número natural M muy grande como el mayor de todos, por más grande que sea M, ocurre que el siguiente, o sea $M+1$, es otro número natural que, obviamente, es mayor que M. Por consiguiente, no existe un número natural mayor que todos los demás.

- ¡Fue exactamente así como me mostró que los números no se terminaban nunca!

- Bien. Y si no se terminan, entonces ¿cuántos hay?

- ¿Infinitos?

- ¡Por supuesto! Hay infinitos números naturales. También podemos expresar esto mismo diciendo que "(el conjunto) **N** es infinito".

- Esta última forma me resulta un poco más difícil, Maestro, pero no importa.

- No es difícil, Clara, te acostumbrarás. Solamente estamos diciendo que si un conjunto tiene infinitos elementos, entonces lo llamaremos *conjunto infinito*, y además, antes hemos asumido que si un conjunto tiene mayor cantidad de elementos que *M*, para todo número natural *M*, entonces tiene infinitos elementos.

- Creo que lo estoy entendiendo.

- Bien. Sigamos que ahora comienza lo más interesante:
¿Cómo son los conjuntos que mencionamos recién, **N, Z**, **Q** y **R**? Me refiero a la cantidad de elementos que tienen.

- Bueno…(Clara pensaba, muy concentrada)… **Z** es más grande que **N**. **Q** también.... y **R** más grande aún. Aunque no conozco tan bien el conjunto **R** como los otros.

- Está bien Clara. Pero quiero que me digas cuántos elementos tienen. ¿Son conjuntos finitos o infinitos?

- ¡Son conjuntos infinitos! -contestó Clara contenta.

- Correcto. Ahora me gustaría ver si podemos contar mejor cuántos elementos hay en cada uno de estos conjuntos. Me refiero a algo más profundo e importante que simplemente decir si es infinito o no. ¿Podrías ayudarme?

Ella se quedó pensando un rato antes de contestar. Estaba un poco sorprendida por esto de "*contar la cantidad de elementos*" de un conjunto infinito. Ya el infinito le parecía algo raro, y ahora esto era más raro aún. Luego dijo:

- Maestro, si estos conjuntos son infinitos, entonces no hay nada más para contar en ellos... ¡¿o sí ?!

El rostro de la niña cambió súbitamente al pronunciar estas palabras. Siempre había pensado que al tratarse de algo *infinito* no había más nada que contar, es decir, la respuesta *infinito* le parecía más que suficiente. Pero confiaba en la sabiduría del Maestro, y entonces, al ver que él indagaba más profundamente sobre esto, por primera vez en su vida pensó que quizá podrían existir "distintos infinitos". ¿Sería posible? Aunque no lo comprendía bien esto la estremeció. Por unos instantes sintió un tironeo interno entre su curiosidad y entusiasmo, que la invitaban a continuar, y sus intenciones de no complicarse que le decían que se olvidara del infinito. En medio de estos pensamientos, oyó que el Maestro continuaba:

- Clara, ésta es, justamente, una de las cuestiones interesantes que quiero que pensemos juntos. Tendremos que dilucidar, por ejemplo, si por ser dos conjuntos infinitos tienen la misma cantidad de elementos o no. ¿Me acompañás en esta *aventura por el infinito*?

Clara pensó un momento más. ¿Se podría realmente responder bien estas preguntas? ¿Sería ella capaz de hacerlo? Su entusiasmo e inquietud vencieron cualquier duda o pereza mental, y respondió:
- Sí, Maestro. ¡Me gustaría explorar el infinito! He escuchado hablar otras veces sobre el infinito y pienso que el tema le interesa a mucha gente, ¿verdad? Pero nunca he sabido ni siquiera por dónde empezar a pensar si escucho *infinito*. Siento que allí se acaba todo.

- Así suele suceder, Clara. Parece mentira, pero justamente al hablar de infinito, se nos suele terminar todo porque no sabemos cómo continuar, no imaginamos qué más se puede analizar. ¡Me alegro mucho que hayas decidido acompañarme! En este mismo momento podemos plantearnos una pregunta concreta muy interesante: ¿Es la cantidad de elementos de **Z** mayor que la de **N**? No creas que es una pregunta fácil, al contrario. Es algo que tendremos que pensar bastante para poder responder, incluso debemos ponernos de acuerdo en algunas cosas básicas desde dónde partir.

- Mmhhh... -Clara ya se había puesto a pensar. Vacilaba, hasta que dijo- No sé, me confundo un poco. Primero pienso que **N** es más pequeño que **Z**. Pero después pienso que los dos son infinitos, y entonces deben tener la misma cantidad de elementos.

- Ajá -dijo el Maestro, sin decirle si estaba en lo cierto o no-. Dijiste cosas interesantes, aunque debemos elaborarlas mejor. Precisamente a este punto quería llegar. Aunque pueda parecer contradictorio, si lo analizamos desde un punto de vista es verdad que **Z** tiene todos los elementos de **N** y otros más, es decir, **Z** *contiene propiamente* a **N**. Sin embargo, si lo miramos desde otro punto de vista, también va a ser verdadero que ambos conjuntos tienen la misma cantidad de elementos; aunque no por ser ambos infinitos, sino por una razón más sutil que veremos enseguida. Para entenderlo bien, conviene que avancemos con cierto cuidado.

En símbolos: sabemos que $\mathbf{N} \subset \mathbf{Z}$, que significa que **N** está contenido y es distinto a **Z**, y veremos que card **N**= card **Z**, que significa que los cardinales o cantidad de elementos de los dos conjuntos es la misma.

- Realmente me intriga saber bien cómo es -dijo Clara-. Y hay una cosa que no entiendo. Usted me dijo una vez que *el todo es mayor que la parte*, o algo parecido. ¿Con **Z** y **N** como sería? ¿No hay una contradicción?

- Como sabemos, **Z** son todos los enteros, en este caso es *el todo*, y **N** es *la parte*, pues existe una correspondencia entre **N** y $\mathbf{Z}^+$. Pero fijate, Clara, que no decimos que **Z** y **N** sean iguales, sino sólo que veremos que la cantidad de elementos que tienen uno y otro es la misma, que es una afirmación distinta que decir que **Z** y **N** son iguales.

- Entonces, ¿me está diciendo que veremos que hay conjuntos con la misma cantidad de elementos, pero que uno es una parte del otro?

- ¡Sí, Clara! ¡Es asombroso! Sucede que estamos acostumbrados a contar conjuntos *finitos*, y eso nunca podría suceder entre ellos, está totalmente vedada esta posibilidad. Pero tratándose de un conjunto *infinito*, en efecto, el todo puede tener la misma cantidad de elementos que una parte del mismo. Es más, esta propiedad podría ser la mismísima definición de lo que significa que un conjunto sea infinito [1].

El Maestro prosiguió:
- Si un conjunto finito **A** contiene a otro conjunto finito **B**, y además **A** es distinto de **B**, entonces sabemos que la cantidad de elementos de **A** es mayor que la de **B**. ¿Esto es sencillo, verdad? El caso finito no nos da ningún problema. Pero nosotros pensaremos ahora en el caso más interesante: ¡el infinito!

[1] Ésta es la definición de conjunto infinito propuesta por el matemático alemán J. W. Richard Dedekind, en el siglo XIX, y es equivalente (aceptando ciertos axiomas) a la definición usual de conjunto infinito que asumimos más arriba.

- Estoy sorprendida, Maestro. Creo que estoy comenzando a entender algo, pero a su vez me parece que algunas cosas me quedan en el aire.

- Está bien, Clara. En realidad todavía no hemos *demostrado* nada, sólo mencionamos lo que sucederá: ¡**N** y **Z** tienen la misma cantidad de elementos! Voy a explicártelo mejor, y vos misma serás capaz de hacer razonamientos con las herramientas que aprenderemos. Primero, nos viene bien revisar algunas cosas del caso *fácil*, cuando todo es finito. Veamos. El *cardinal* de un conjunto es la cantidad de elementos que tiene el conjunto. Por ejemplo, en tu curso son 28 compañeros en total, entonces podríamos decir que el conjunto formado por los alumnos de 1.er año B de este colegio tiene 28 elementos; o equivalentemente, que el cardinal de este conjunto es 28.

- Entiendo. Pero disculpe, Maestro, ¿no he pasado a ser un simple elemento de un conjunto, no?

- (risas)… ¡No! Bueno, sí y no. Sigues siendo Clara, sólo que además, puedes formar parte de este conjunto que te estoy proponiendo. Es un conjunto muy sencillo. ¿Y cuántos alumnos hay en 1.er año A?

- Hay 30. Ellos son dos más, pero en la mayoría de las competencias entre los dos cursos hemos ganado nosotros.

- Te felicito, pero olvidá eso. Sólo digamos que, como 30 es mayor que 28, el conjunto de alumnos de 1.º A es mayor que el de 1.º B. En otras palabras, si **A** y **B** denotan estos dos conjuntos, entonces el cardinal de **A** es mayor que el cardinal de **B**. En símbolos escribimos card(**A**) > card(**B**).

- Esto ha sido muy fácil.

- Seguro. Ahora decime, por favor, cuántos alumnos son en 2.º año, que hay una sola división.

- Son 30 también.

- ¡Qué bien! Esto nos servirá. Si llamamos **C** al conjunto de alumnos de 2.º año, entonces el cardinal es 30, es decir card(**C**) = 30. Como ya sabíamos que card(**A**) = 30, entonces podemos decir que

$$\text{card}(\mathbf{C}) = \text{card}(\mathbf{A})$$

- Esto también ha sido muy fácil.

- Sí, claro. Veamos ahora si me seguís en esto. En tu último cumpleaños, invitaste a todos los niños de 1.º A y de 1.º B, ¿verdad? Y también a tus primos, a tus vecinos, y a algunos niños y niñas más. En uno de los juegos -el que yo te propuse que hicieras- todos tuvieron que quitarse los zapatos. Ahora bien, no se sabía exactamente cuántos niños eran, ¿verdad? De modo que no sabemos cuántos zapatos había. Tampoco cuántos zapatos izquierdos y cuántos derechos había. Sin embargo, es claro que la cantidad de zapatos izquierdos era igual a la cantidad de zapatos derechos. ¿Estás de acuerdo?

- Sí. Todos habían traído sus dos zapatos y se los quitaron.

- Bien. Si denotamos con **ZI** y con **ZD** los conjuntos de zapatos izquierdos y derechos respectivamente, entonces, lo que hemos dicho es que:

$$\text{card}(\mathbf{ZI}) = \text{card}(\mathbf{ZD}).$$

- Esto también ha sido sencillo, Maestro.

- Pronto entenderás a dónde quiero llegar. Aunque no parezca, lo de los zapatos es algo muy importante. Disculpame que te lo remarque, pero posiblemente todavía no vislumbres su valor: ¡podemos afirmar que estos dos conjuntos tienen el mismo cardinal aún sin saber cuántos elementos tienen estos conjuntos!

- Sí Maestro, estoy de acuerdo, sólo que me parece que de algún modo ya sabía esto.

- Bueno, tanto mejor. Entonces estás bien preparada para lo que sigue. Concentrate por favor, que no es tan sencillo. Pensemos en los números naturales y en los números naturales pares. Ahora veamos la correspondencia que asigna a cada número natural n el doble del mismo, es decir, al número n le asigna el número $2n$. Esto se puede expresar como $n \mapsto 2n$ donde n varía entre los elementos de **N**. Es decir, a la izquierda, van apareciendo todos los números naturales, y a la derecha sólo los de la forma $2n$, o sea, los números naturales pares (que denotaremos, como conjunto, con **NP** por naturales pares). El número par que le corresponde al 1 es el 2 x 1 = 2; el que le corresponde al 2, no es el 2, sino el 2 x 2 = 4; al 5 le corresponde el 2 x 5 = 10, etc. Pensemos que ésta es una correspondencia entre los conjuntos **N** y **NP**. A este tipo de correspondencia, la llamaremos *correspondencia biunívoca* entre **N** y **NP** porque a cada elemento de **N** le corresponde uno, y solo uno, de **NP**, y viceversa. Si tomamos un número par cualquiera, por ejemplo el 42, entonces sabemos que hay un único número natural que le corresponde, que es el 21, porque 42 = 2 x 21. Conviene que denotemos esto por:

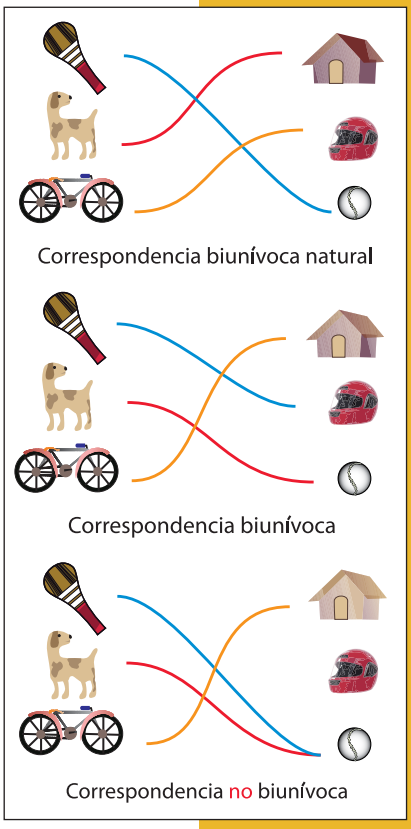
$$\mathbf{N} \leftrightarrow \mathbf{NP}$$
$$n \mapsto 2n$$

y que recordemos su nombre. ¿Cómo era, Clara?

- Usted dijo "correspondencia biunívoca". Ahora creo recordar que una vez vimos esto, con un dibujo así: →

Teníamos que unir con líneas las cosas que se correspondían. Unimos el perro con su cucha, la bicicleta con el casco y la paleta con la pelota. ¿Esto es una correspondencia biunívoca? -preguntó Clara, con cierto orgullo.

- Sí, eso es. Ahora debés tener en cuenta que si nos piden unir con líneas los objetos que se corresponden tendemos a recurrir al sentido común, a la lógica. Sin embargo, uno bien podría unir el perro con la pelota, la bicicleta con la cucha, y la paleta con el casco, y eso sería *otra* correspondencia biunívoca, distinta de la anterior. ¿Lo entendés? En cambio, si dibujáramos tres líneas, una que sale de la paleta y llega a la pelota, otra



desde el perro a la pelota y otra desde la bicicleta a la cucha, entonces, no sería una correspondencia biunívoca.

Problema 3.1. Ayudar a Clara a responder las siguientes preguntas (las respuestas y soluciones se encuentran en el Capítulo 6).

Enumerar todas las correspondencias biunívocas que hay entre el conjunto {1, 2, 3} y el {*A* , *B*, *C* }.

¿Cuántas correspondencias biunívocas hay entre los conjuntos {1, 2, 3, 4} y {*A*, *B*, *C, D*}?

El Maestro prosiguió:
- Cuando hay una correspondencia biunívoca entre dos conjuntos, podemos identificar los elementos de un conjunto con los del otro, justamente a través de dicha correspondencia. En ese caso, ¿qué sucede con la cantidad de elementos de ambos conjuntos?

- Creo que son iguales -respondió Clara.

- Por supuesto. Exactamente esto es lo que sucedía en el ejemplo de los zapatos izquierdos y derechos. Había una correspondencia biunívoca entre esos conjuntos que llamábamos **ZI** y **ZD**, por lo tanto, sus cardinales eran iguales.
Veamos más ejemplos, Clara. Te voy a decir una correspondencia de la vida real, a ver si podés responder si es biunívoca o no: cada persona tiene un nombre, un primer nombre de pila. Podemos pensar esto como una asignación:

$$\text{persona} \longmapsto \text{nombre de pila de la persona}$$

- ¿Tengo que contestar si es una correspondencia biunívoca?

- Así es. ¿Qué te parece?

- ¿Puede haber personas con el mismo primer nombre?

- Seguro. Éste es un ejemplo de la vida real.

- Entonces, esta asignación no es biunívoca porque hay personas distintas que tienen el mismo nombre.

- ¡Muy bien! Lo estás entendiendo. Hagamos un ejemplo más. Pensemos que a cada país le asignamos su ciudad con mayor cantidad de habitantes, es decir:

$$\text{país} \longmapsto \text{ciudad más populosa del país}$$

¿Esta asignación es una correspondencia biunívoca?

- Creo que sí, pero no estoy tan segura.

- Bien, Clara. Analicemos esto porque al no decir claramente cuáles son los conjuntos de salida y de llegada de la asignación pueden crearse confusiones. Si pensamos que va desde el conjunto de los países al conjunto de todas las ciudades del mundo, entonces no es biunívoca porque quedarían ciudades sin nombrar. Ahora, si consideramos que la asignación va del conjunto de países al conjunto de las ciudades más populosas de cada país, entonces sí es una correspondencia biunívoca. Por consiguiente, para decidir si una

asignación o correspondencia es biunívoca o no, es fundamental decir cuál es el conjunto de llegada de la asignación.

- Está bien. Ya no es tan sencillo, pero lo he seguido.

- ¿Serías capaz de decir qué ciudad se le asigna a Brasil?

- Sí, creo que es San Pablo -dijo Clara bastante segura, porque conocía algo sobre Brasil.

- ¿Y a Colombia?

- No estoy segura, pero arriesgaría Bogotá porque es la capital.

- Correcto. Ahora, asumamos que en el año 2010 hay 198 países. Si quisieras memorizar esta asignación para los 198 países, yo te diría el país y tú deberías responder con su ciudad más populosa. ¿Cuántas ciudades deberías saber?

- Creo que 198.

- ¡Por supuesto! Esto es así porque la correspondencia es biunívoca. Claro que para responder bien no alcanza con saber los nombres de las ciudades, pero al menos hay que saberlos.

-Y el Maestro prosiguió-
Ahora que tenés claro este ejemplo y los anteriores, estás lista para lo siguiente: ¿No te parece que cuando hay una correspondencia biunívoca entre dos conjuntos, es natural pensar que esos conjuntos tienen la misma cantidad de elementos?

- Sí, yo creo que sí.

- Me alegro. Porque esto nos servirá ¡para el caso infinito! Si revisamos todo lo que hemos dicho verás que no necesitamos que los conjuntos sean finitos para hablar de correspondencia biunívoca. Y que es natural pensar que cuando se puede establecer una correspondencia biunívoca entre dos conjuntos, estos tienen la misma cantidad de elementos. Tomaremos esto como punto de partida, como *definición* de lo que significará para nosotros que dos conjuntos infinitos tengan la misma cantidad de elementos. A partir de ahora, Clara, al oír "infinito" no te quedarás paralizada, sino que vas a poder pensar en las correspondencias biunívocas.

Definición: Dos conjuntos (infinitos) tienen la misma cantidad de elementos si se puede establecer una correspondencia biunívoca entre ellos. En símbolos, card **A** = card **B** si existe una correspondencia biunívoca **A** ↔ **B**. En este caso, se dice que los conjuntos **A** y **B** son **coordinables**.

Ahora, Clara comprendía mejor porqué el Maestro había usado los países y sus ciudades más habitadas, y los zapatos izquierdos y derechos. Estaba preparando el terreno para el caso infinito, aunque éste fuera totalmente distinto. Ahora podía imaginarse mejor las cosas. Estaba sumida en esos pensamientos cuando el Maestro continuó.

- Para hacer más cortos nuestros enunciados, te propongo que en lugar de decir que entre un conjunto y otro hay una correspondencia biunívoca, digamos que esos dos conjuntos son **coordinables**. ¿Qué te parece?

- No hay problema. Sólo me tengo que acordar de esta palabra, **coordinable**, que es nueva para mí.

- Así es. La repetiremos varias veces, te la vas a acordarte bien. También, tenés que recordar que llamábamos **cardinal** a la cantidad de elementos de un conjunto. O sea que ahora, si dos conjuntos son coordinables, estamos diciendo que **tienen el mismo cardinal**. No importa que no sepamos bien cuál es su cardinal, como en el caso de los conjuntos infinitos, pero igual podemos decir que tienen el mismo cardinal si hay una correspondencia biunívoca entre ellos. Ahora volvamos al comienzo. ¿Te acordás de la pregunta sobre la cantidad de elementos de **N** y de **Z**?

- Creo que sí. Era, si tenían la misma cantidad de elementos, o si el cardinal de **N** era menor que el de **Z**.

- Correcto. Ahora también podemos enunciarla preguntando ¿son **N** y **Z** coordinables? Me gusta enunciar las cosas de una manera sencilla. Si ya nos hemos puesto de acuerdo en lo que significa "ser coordinable a", entonces el enunciado se simplifica.

- Ahora, me gustaría saber la respuesta, Maestro, entenderla.

-¿Son **N** y **Z** coordinables? ¿O no lo son? Si no lo fueran, entonces el cardinal de **Z** debería ser mayor que el de **N**. En símbolos: card **Z** > card **N**. ¿Te parece que lo podrás resolver, Clara?

- Tal vez sí. Ahora tengo más elementos para pensarlo. Espero poder hacer algo.

- Sí. Confío que vas a poder porque te gusta pensar, y eso es todo lo que se necesita: interés, curiosidad, un poco de concentración. Clara, cada vez que te veo pensando siento que la llama de la curiosidad intelectual está viva en los niños y jóvenes del siglo XXI.

- Maestro, estoy recordando lo que me explicó sobre los números naturales y los números naturales pares. Son coordinables, ¿verdad?

- ¿Estás segura?

- Creo que sí. Usted mismo me mostró la correspondencia $n \mapsto 2n$. Es biunívoca, por lo tanto ¡los números naturales y los números naturales pares son coordinables!

- Así es. Por un lado, esto ha sido sencillo porque la correspondencia $n \mapsto 2n$ lo es. Sin embargo, como ya dijimos, la conclusión de que una parte propia de **N** sea coordinable a **N** podría resultar inquietante. Alguien podría confundirse y creer que esto significa que el todo es igual a la parte. No queremos tener problemas con los filósofos. En verdad, **no podemos** tenerlos porque lo que hacemos es matemática. En este sentido no hay ningún problema. Repitamos: no decimos que **N** es igual a **NP** sino que son coordinables, que no es lo mismo. En matemática debemos ser cuidadosos. Los detalles cuentan. A veces hay diferencias sutiles.

- Me parece sutil, pero creo que lo entendí. Sí, ahora lo veo bien: **N** y **NP** no son iguales, obvio, pero sí son coordinables.

- Absolutamente. Ahora, esto sólo puede ocurrir entre conjuntos infinitos y no entre conjuntos finitos. ¿Podrías decir, Clara, qué es un conjunto finito?

- Bueno, ya lo vimos, pero igual me parece difícil. Para mí, es cuando cuento sus elementos y en algún momento termino de contarlos.

- Bien. En otras palabras, estás diciendo que se puede establecer una correspondencia biunívoca entre el conjunto dado y alguno de los conjuntos {1}, {1, 2}, {1, 2, 3}, {1, 2, 3, 4}, etc. ¿Y cuándo un conjunto es infinito?

- Cuando no paro de contar sus elementos.

- Está bien. También podemos decir que es infinito cuando no es finito, o sea, cuando no es coordinable a ninguno de los conjuntos {1}, {1, 2}, {1, 2, 3}, {1, 2, 3, 4}, etc. Lo que estamos haciendo es dar una **definición formal** de lo que significa conjunto infinito.
Pero dejemos ahora la definición, y volvamos a la pregunta interesante. Estabas por responder sobre **N** versus **Z**.

Definición. Un conjunto es **finito** cuando es el conjunto vacío o es coordinable con alguno de los siguientes conjuntos: {1}, {1, 2}, {1, 2, 3}, {1, 2, 3, 4}, ... en general, el {1, 2, 3, 4,..., n}, donde n es algún número natural. Un conjunto es **infinito** cuando no es finito.

Clara se concentró durante unos minutos. El Maestro también pensaba, aunque no sabemos si en este problema o en otras cosas. Hasta que Clara respondió:

- Estoy lista. Ahora que comprendí el caso **N** versus **NP**, me da toda la impresión que esto es igual. Todavía no puedo escribir la correspondencia completa, pero estoy segura que **N** y **Z** son coordinables.

- Bien. Has dado un buen paso, Clara. Pudiste comenzar a escribir una correspondencia, ¿verdad? Me gustaría ver si te puedo ayudar. Una forma de estar completamente seguros de que son coordinables es poder escribir la correspondencia biunívoca.

- Eh, bueno, esto es lo que escribí:

1	2	3	4	5	6	7	8	9	10	11	...	
1	-1	2	-2	3	-3	4	-4	5	-5	6	...	

Y me gustaba como iba, salvo que al 0 del conjunto **Z** de los enteros no sé cómo ponerlo para que se corresponda con uno de los números naturales de arriba.

- Clara, afortunadamente puedo ayudarte en esto. Hay muchas formas de incorporar el cero. Un viejo y sencillo truco consiste en correr todo un lugar para la derecha en la segunda fila, y entonces queda el primer lugar libre y podés poner el cero allí. Si lo escribimos a tu manera, nos queda de la siguiente forma:

N	1	2	3	4	5	6	7	8	9	10	11	...
Z	0	1	-1	2	-2	3	-3	4	-4	5	-5	...

Fijate que sólo agregamos el 0 al comienzo de tu lista de números enteros, y los demás se corrieron un lugar.

- ¡Ese truco fue muy bueno! -dijo Clara entusiasmada, al ver que el Maestro había podido completar la correspondencia que ella había iniciado-. De modo que ¡**N** y **Z** son coordinables!

- Así es. Me alegro que hayamos respondido la pregunta inicial. Apuesto a que nunca oíste hablar del Hotel Hilbert.

- No Maestro. ¿Tiene algo que ver con esto?

- Sí, en particular con el truco que hicimos. Es un Hotel peculiar, muy interesante. Pero la semana que viene hablaremos sobre él. Hoy ya hemos tenido suficiente, ¿no crees?

- Sí. Todavía me queda tiempo para la merienda y más tarde tengo mis prácticas de vóley. Aunque me quedo con la intriga de saber el porqué un hotel puede ser tan especial para la matemática. Gracias Maestro. ¡Hasta la próxima clase!

- Adiós, Clara. Hasta la semana que viene. Que disfrutes de tu partido de vóley.

El Maestro se quedó pensando: "Esta niña me da mucha alegría. A veces me preocupa un poco ver que a los alumnos les cuesta sentarse a pensar con profundidad. Pero Clara lo hace. Le encantó pensar sobre el infinito. Quiere entender. ¡Le gusta aprender y superarse! ¿No es acaso el pensamiento abstracto y profundo algo que nos distingue de los demás seres vivientes de La Tierra? ¿No es acaso, el pensamiento matemático, algo maravillosamente profundo?

Para resolver

Problema 3.2. Ayudar a Clara a:

- Hallar una correspondencia biunívoca entre los números naturales y los números naturales impares. Denotaremos al conjunto que forman estos últimos con **NI**, es decir, **NI** = {1, 3, 5, 7, 9, 11, ...}. De modo que en este problema se demostrará que los conjuntos **N** y **NI** son coordinables.

- Hallar una correspondencia biunívoca entre los números naturales pares, **NP**, y los **cuadrados perfectos**, es decir aquellos números de la forma $n^2 = n \cdot n$, donde n es un número natural. Si denotamos este conjunto por **CP**, entonces:

CP = {1, 4, 9, 16, 25, 36, 49, 64, ...}.

3.2. Hotel Hilbert

- Maestro. ¿Me contaría sobre el hotel que mencionó la clase pasada?

- Por supuesto. Es un hotel muy sencillo, en algún sentido - aunque el Maestro sonreía mientras decía esto, como si escondiera una sorpresa detrás de sus palabras-. No tiene cosas especiales como pileta, cancha de tenis, gimnasio y todo eso que se estila en los grandes hoteles. Pero tiene una característica particular, sólo una: los números de sus habitaciones son 1, 2, 3, 4, 5, 6, 7,…

- ¿Quiere decir usted que sólo tiene una planta? ¿Que no tiene varios pisos? Una vez que estuve en un hotel así me tocó la habitación 22. Me gustaba porque ¡era un número capicúa!

- Clara, si te fijás bien en lo que dije, notarás que los números de las habitaciones son 1, 2, 3, 4, 5,…., y continúan, indefinidamente, es decir, ¡TODOS los números naturales! Sí, es un hotel con ¡una cantidad infinita de habitaciones! Tantas, como números naturales hay.

- Uaaauuuu. No me lo esperaba. Pero... ¿es posible?

- ¡Sí... en nuestra imaginación!

- Claro. Voy a empezar a imaginármelo.

Clara continuó:
- Pienso en un hotel que tiene sus habitaciones en una línea muy larga, como un tren, pero que no termina…

- Está bien, podés imaginarlo así, quizá te ayude para lo que viene.

- Estoy preparada para escucharlo, Maestro, me interesa.

- Muy bien, Clara. Lo que me gusta del Hotel Hilbert es que siempre encuentro lugar allí.

- Ah, claro, siempre hay habitaciones vacías, al ser infinitas -pensó Clara en voz alta.

- No exactamente. Un día llegué al hotel y estaba lleno. Todas las habitaciones estaban ocupadas. Yo no tenía otro lugar a donde ir y ya era de noche. Además, llovía. Pero el conserje fue muy amable conmigo. Levantó el teléfono y enseguida me dijo que yo disponía de la habitación número 1. Me quedé boquiabierto, era la primera vez que me sucedía una cosa así. ¿Te podés imaginar cómo me consiguió ese lugar?

- No. ¿Alguien dejó el hotel justo en ese momento?

- No, Clara. Nadie dejó el hotel, ni tampoco puso a dos pasajeros que estaban separados en una misma habitación. ¡Pero consiguió un lugar! Digamos que se trata de un "truco matemático". Pensalo un rato, a ver qué se te ocurre.

El Maestro la instó a que intentara hallar una solución antes de escuchar la respuesta. Clara se concentró mucho pensando en el problema. Y los dos estuvieron un rato en silencio. Ella pensaba en el problema y el Maestro en la existencia del infinito. Más tarde el Maestro explicó:
- Lo que hizo el conserje fue pedirle a los pasajeros que se mudaran a la habitación siguiente de la que estaban; es decir, quien estaba en la habitación número 1 debía cambiarse a la número 2; quien ocupaba la 2 a la 3; el de la 3 a la 4; y así sucesivamente. Como en este mundo imaginario todos eran muy amables accedieron gentilmente a mudarse, y así, enseguida se liberó la habitación número 1, que el conserje me ofreció. Como ves, ¡nadie se quedó sin habitación!

- ¡Qué bárbaro! Estaba lleno, pero le hicieron lugar. ¡Cuesta creerlo!

- Así es, Clara. Nuestra intuición está acostumbrada a *hoteles finitos*, es decir, con una cantidad finita de habitaciones. Por eso, esto nos sorprende tanto. Fijate que si además de llegar yo, esa noche llegaban varias personas, el conserje podía acomodarlas a todas. Simplemente, le pedía a los pasajeros que en lugar de moverse de una habitación a la siguiente, o sea, de la número n a la n+1, lo hicieran de la número n a la n+k, donde k es el número de personas que llegaron. De ese modo, quedaban las primeras k habitaciones libres para ser ocupadas por los nuevos pasajeros.

- ¡Increíble! Es un hotel fascinante. Usted dijo que sólo tenía una particularidad, pero es una muy especial.

- Es verdad... (risas). Ahora, Clara, ¿sabés cómo se relaciona esto con el 0 de **Z** en la correspondencia con **N**?

- Mmhh… déjeme pensarlo un poco, Maestro.

El Maestro nuevamente le dio tiempo a Clara para que piense sola el problema, antes de darle alguna explicación.

- Ya está -dijo Clara- lo entendí.

- Muy bien. ¡Contame lo que pensaste!

Y Clara dio una excelente explicación que alegró y asombró al Maestro en partes iguales. Entonces el Maestro agregó:

- ¡Excelente, Clara! Voy a repetir lo que dijiste, desde mi punto de vista: El 0 sería yo, que llegué al hotel donde ya estaban alojados todos los demás números enteros que serían los pasajeros. Como ves me hicieron lugar, simplemente corriendo a todos un lugar más adelante, y poniéndome a mí primero. Es lo mismo que hicimos con tu correspondencia biunívoca. Habías apareado los enteros distintos de cero con los naturales. Pero luego pusimos el cero al principio, corriendo todos los otros enteros un lugar hacia la derecha. Es como haberle hecho un lugarcito al cero en la habitación número 1 del hotel.

- ¡Por supuesto! Ahora veo que podría haberme dado cuenta de todo apenas comenzó a plantear el problema.

- Hay una cosa más en el Hotel Hilbert que te asombrará. Si aquella noche que llegué solo hubiera llegado un contingente de infinitas personas, numeradas 1, 2, 3, 4, 5,…., ¡el conserje también las habría alojado!

- ¡¿A infinitas, también?!

- Sí. En ese caso les habría dicho a los pasajeros que se corrieran de su habitación número n a la habitación número $2n$, y así, todas las habitaciones impares habrían quedado libres. ¿Me seguís? De este modo ubicaba a la persona número 1 en la habitación número 1, que estaba libre, a la persona 2 en la habitación 3, que también estaba libre, por ser impar, a la persona 3 en la habitación 5, a la 4 en la 7, la 5 en la 9, etc. En general, habría ubicado a la persona número k en la habitación número 2 k-1. ¡Esto es posible en nuestro gran Hotel Hilbert!

Para resolver

Problema 3.3. Si llegan al Hotel Hilbert dos contingentes, A y B, de infinitas personas cada uno, a las que podemos enumerar como $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, \ldots$ y $b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, \ldots$ ¿Podrá el conserje ubicar a todas estas personas, cada una en una habitación distinta?

Aclaración: el hotel ya está lleno, no se puede echar a ningún pasajero, ni juntarlo con otro en una misma habitación, pero sí se puede reubicar (es decir, mover de una habitación a otra) a los pasajeros que el conserje considere necesario, y no se debe dejar ninguna habitación vacía.

Problema 3.4. Si llegan al Hotel Hilbert infinitos contingentes A^1; A^2; A^3; A^4; A^5; A^6; A^7... de infinitas personas cada uno, a las que podemos denotar de la siguiente manera:

a las del contingente A^1 con $a_1^1, a_2^1, a_3^1, a_4^1, a_5^1, a_6^1, a_7^1, a_8^1, \ldots$
a las del contingente A^2 con $a_1^2, a_2^2, a_3^2, a_4^2, a_5^2, a_6^2, a_7^2, a_8^2, \ldots$
a las del contingente A^3 con $a_1^3, a_2^3, a_3^3, a_4^3, a_5^3, a_6^3, a_7^3, a_8^3, \ldots$; etc.

¿Podrá el conserje ubicar a todas estas personas, cada una en una habitación distinta?

3.3. La paradoja de Aquiles y la tortuga

- Maestro, ¿se acuerda que un día dijo: ¿"eso es filosofía"?

- Sí, Clara. La filosofía es la madre de las ciencias, de algún modo las engloba a todas.

- Aquel día me gustó mucho la clase. ¿Podría enseñarme un poco más?

- Disculpame, Clara, es que yo no sé mucho de filosofía. Sólo sé algo de matemática. Pero aprovechemos que estás interesada para contarte algo que ocurrió de verdad, y forma parte de la historia de la filosofía. Lo más interesante para nosotros será la parte matemática del asunto porque ayuda a comprender y resolver un problema filosófico.

- Suena superinteresante, Maestro.

- ¡Lo es! ¡Ya verás!
Hacia el siglo V a.C., los griegos hacían grandes progresos en casi todo, especialmente en filosofía. Parece mentira que un pueblo "antiguo" haya hecho avances tan profundos. Fue algo maravilloso. Seguramente habrás oído alguna vez sobre los tres grandes filósofos griegos: Sócrates, Platón y Aristóteles, ¿verdad?

- Sí, pero muy poco. Me gustaría saber más.

- Sólo para mencionar la importancia que daba a la matemática Platón -uno de los más célebres pensadores de la historia de la humanidad- hay que saber que se le atribuye haber tenido en la entrada de su gran escuela un cartel que decía: *no entre a esta escuela quien no sepa geometría*.

El Maestro hizo una pausa, y sus palabras quedaron resonando en la cabeza de Clara. Prosiguió.

- Conmovedor, ¿no te parece? Pero dejemos a Platón y pasemos a Zenón de Elea, filósofo griego también, apenas anterior a él. Zenón hizo una serie de razonamientos interesantes, elaborados inteligentemente, que llevaban a la conclusión de que ¡el movimiento no era posible!

- ¡¿Cómo?! ¿En serio? –preguntó Clara asombrada.

- Así es. Bueno, se trata de una paradoja.

- ¿Qué es una paradoja, Maestro?

- Es una afirmación que suena absurda. Es opuesta a lo que piensan casi todos, pero se presenta en forma lógica, e induce a pensar que es verdadera. Para mí, una buena paradoja es algo que si lo pensás de un modo, sacás una conclusión, y si lo pensás de otro modo, sacás otra que es contradictoria con la anterior. Por consiguiente, alguna de las formas en que estás pensando es errónea, no es válida. ¿Entendés?

- Creo que sí, pero no sé si conozco alguna.

- Bueno, te voy a contar una que planteó Zenón de Elea. Se llama la paradoja de **Aquiles y la tortuga.**

- Ah, ¡conozco a Aquiles porque leí la Ilíada para niños! -dijo Clara.

- Muy bien, es ese mismo Aquiles. Cuando se lo menciona en la Ilíada original, frecuentemente su nombre va acompañado por un adjetivo en griego que significa **el de los pies ligeros**. El fue un héroe de la guerra de Troya, historia que cuenta magistralmente Homero. Pero Aquiles también era muy veloz y por eso es el protagonista de esto que te voy a contar. En la antigua Grecia se celebraban los juegos olímpicos (los actuales están hechos a semejanza de aquéllos). Ah, ¡qué pueblo fantástico el griego! -y el Maestro hizo una pausa, se quedó un rato mirando hacia el infinito con cara de admiración, seguramente pensando en los griegos. Luego retomó.

- Perdón por distraerme. Volvamos a la paradoja. Zenón imaginó una carrera entre Aquiles, el de los pies ligeros, y una tortuga. ¿Quién creés que ganaría semejante carrera?

- Aquiles, obvio. Aunque en la fábula de la liebre y la tortuga, ¡pierde la liebre! En esta carrera, ¿pasa algo raro también?

- No, Clara -dijo el Maestro sonriendo-. Aquiles no se tiraría a dormir en medio de una carrera. Aquí, el único problema menor que él tiene es que debe darle una pequeña ventaja inicial a la tortuga. Es poca ventaja, así que todos asumen que la descontará en los primeros momentos, y luego ganará la carrera con total comodidad.

- ¿Y qué pasó? ¿Ganó Aquiles?

- Bueno, aquí viene lo interesante. ¡Aquiles no puede pasar a la tortuga!

- Pero ¿por qué? ¿No corre mucho más rápido?

- Sí, pero lo que Zenón plantea es que desde un punto de vista puramente abstracto y racional, Aquiles no podrá ni siquiera alcanzarla. Podríamos poner así el razonamiento: para superar a la tortuga, Aquiles, primero deberá llegar al lugar donde se encuentra la tortuga al instante de inicio de la carrera, ¿estás de acuerdo?

- Sí, claro.

- Eso le tomará un cierto tiempo. Durante ese tiempo, la tortuga también avanzó, y dejó atrás ese lugar. De modo que la tortuga sigue estando delante de Aquiles.

- Sí. Pero todavía no veo cuál es el problema.

- Paciencia, Clara, no estamos lejos. Nuevamente, para superar a la tortuga, Aquiles, primero deberá llegar al lugar donde ella se encuentra. Esto le tomará un cierto tiempo. Es el segundo intervalo de tiempo que se ha consumido. Pero nuevamente, la tortuga avanzó durante ese segundo intervalo de tiempo, y entonces, continúa delante de Aquiles.

Clara prestaba mucha atención a esta explicación. El Maestro continuó:

- Bien. Ahora la situación se repite por tercera vez. Aquiles debe llegar primero donde se encuentra la tortuga, y esto le toma un cierto tiempo, que es el tercer intervalo de tiempo que ha transcurrido. Pero mientras tanto, la tortuga avanzo nuevamente. Y así, la misma situación se repite, es decir, la tortuga está delante de Aquiles, y ya van tres intervalos de tiempo consumidos. Y así sucesivamente, esto se repite, y se repite, ¡indefinidamente!

- Creo que lo estoy siguiendo, Maestro.

- Si bien Aquiles y la tortuga están cada vez más cerca entre sí, Aquiles siempre está detrás. Y lo importante, es que ya se ha tomado muchos tiempos para acercarse, muchísimos. En verdad, ¡necesitaría infinitos tiempos para alcanzarla! Entonces, aquí viene la importante conclusión: si Aquiles necesita infinitos tiempos para alcanzar a la tortuga, es imposible que lo consiga. Por consiguiente, desde un punto de vista puramente racional ¡el movimiento no puede existir! Zenón de Elea continúa con su argumento, diciendo que quizás el movimiento esté sólo en nuestra imaginación. De acuerdo con este razonamiento, el movimiento no es posible, ya que se necesitaría tiempo infinito para lograr moverse. ¿Qué te parece?

- ¡Asombroso! -respondió Clara, desconcertada e intrigada.

- Zenón pensaba que quizá todo estuviera en nuestra mente. Que tal vez el mundo exterior no existía, sino en nuestra imaginación. El filósofo continuaba haciendo implicaciones, consistentes con su razonamiento, donde "*demostraba*" que el movimiento era imposible.

- ¿Y usted qué opina?

El Maestro sonrió y continuó sin responder la pregunta.

- Hay otras paradojas similares que planteó Zenón. Por ejemplo, una muy conocida dice que para llegar a un lugar, primero debes recorrer la mitad de la distancia, pero antes, debes recorrer la mitad de la mitad, y antes de esto, la mitad de la mitad de la mitad, y así sucesivamente, de modo que nunca puedes comenzar. Si bien los argumentos y las situaciones en sus paradojas son aparentemente distintos, los filósofos dicen que son esencialmente iguales, de manera que podemos quedarnos con la de Aquiles y la tortuga, y pensar sólo en ella.

- ¿Y qué sucedió con estas paradojas?

- Por empezar, algunos pensadores y filósofos quedaron asombrados con la paradoja de Zenón. Tal vez quedaron un poco desorientados.

En ese momento, Clara razonó así:

- Si Aquiles necesita infinitos tiempos para pasar a la tortuga, no entiendo cómo puede pasarla. Y yo creo que la pasa, ¡estoy segura que la pasa! Quiero decir, que el movimiento tiene que ser de verdad, no puede ser sólo una película en mi cabeza.

- Te entiendo, Clara. En aquel tiempo, un rey, dijo: "*el movimiento se demuestra andando*", y entonces salió de su palacio con gran pompa, hizo un paseo por las calles principales de la ciudad, y regresó muy satisfecho de sí mismo, creyendo que había acabado con la paradoja, y que todos podían olvidarse de ella. ¿Qué te parece?

- No sé, no me parece muy inteligente lo del rey, ¿no?

- Ciertamente no aportó nada para "desentrañar" la paradoja. Todos podemos movernos, o creer que lo hacemos -el Maestro rió al decir estas palabras- y que los demás coincidan con nosotros en esto. Pero de lo que se trata este problema es de encontrar cuál es el error en el razonamiento planteado. Por otra parte, si todo fuera un sueño, o una película en nuestra mente, ¿podríamos distinguirlo? ¿Cómo? Lo que los pensadores querían entender -y supongo que ahora vos también- era, desde el punto de vista racional, qué estaba sucediendo con el razonamiento de Zenón.

- ¿Y lo lograron?

- No en aquel momento. Bueno, no por muchísimos años, ¡por siglos! Como te dije, en parte fue la matemática la que proveyó argumentos para dar por tierra definitivamente con la paradoja. Como ves, Clara, aquí el infinito aparece como elemento fundamental. Y quizá la falta de comprensión del mismo, fue lo que llevó a no poder resolverla bien durante tanto tiempo. Pero vayamos ahora al argumento matemático. Zenón dijo que el problema era la suma de infinitos tiempos, ¿verdad?

- Sí, eso dijo… o al menos, eso dijo usted que él había dicho -respondió Clara riéndose.

- No es momento para chistes -bromeó también el Maestro-. ¡Mejor será que te concentres! Zenón asumió que al tener que realizar una acción en infinitos tiempos, eso significaba que le tomaría tiempo infinito, y por lo tanto no sería posible. Pasándolo a términos matemáticos, sería que al sumar infinitos tiempos, el resultado de la suma da una cantidad infinita de tiempo, y por eso resultaba imposible el movimiento. Sin embargo… ¡no es así!

- ¿Qué cosa no es así?

- La suma de infinitos intervalos de tiempo, ¡puede ser finita! No tiene por qué ser infinita. ¿Te sorprende?

- Sí, por supuesto. Creo que yo me imaginaba que si siempre seguía sumando, y sumando, entonces la suma se iba haciendo más y más grande, y no podía parar.

- Sí. Se va haciendo más y más grande, es verdad. Pero eso no significa que se haga ¡tan grande como uno quiera! Es decir, no significa que la suma deba ser infinita. Dicho en otras palabras, si los números a considerar se van haciendo muy pequeños, entonces la suma de infinitos números puede dar resultado finito. Es el caso de la suma de uno, más un medio, más un cuarto, más un octavo, etc. Lo que no debemos hacer es confundir *números* con *números naturales*. En nuestro caso, no estamos sumando números naturales, sino *números fraccionarios* o *números reales*, que pueden hacerse verdaderamente muy pequeños.

La suma de infinitos números (reales, o fraccionarios) positivos puede ser finita. Por lo tanto, la suma de infinitos tiempos, no tiene porqué ser infinita, puede ser finita.

- Entonces, cuando Aquiles necesitaba "infinitos tiempos" para pasar a la tortuga, en realidad no necesitaba "tiempo infinito". O sea que ¡¿la puede pasar sin problema?!

- Correcto. En la clase que viene, podríamos aprender bien las sumas infinitas, si te interesa. Hasta ahora, sólo te lo he dicho, pero podemos entenderlo bien, convencernos, *¡demostrarlo*!

- Sí, Maestro, me gustaría. –dijo Clara verdaderamente interesada en aprender sobre *sumas de infinitos términos*.

- En el tiempo que nos queda hoy, veamos un ejemplo interesante, donde sumamos infinitos términos y, sin embargo, la suma es finita. Los términos a sumar son, como dijimos, simplemente los inversos de las potencias de 2, o sea, números de la forma $\frac{1}{2^k}$, donde k es un número natural o el cero. Entonces, realizamos las siguientes sumas: primero sólo el 1, en segundo lugar hacemos $1+\frac{1}{2}$, luego $1+\frac{1}{2}+\frac{1}{4}$, seguimos con $1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}$, y continuamos haciendo sumas. La quinta suma es: $1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}$, y así seguimos. Por ejemplo, la décima suma es: $1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\frac{1}{32}+\frac{1}{64}+\frac{1}{128}+\frac{1}{256}+\frac{1}{512}$. Y continuamos, nunca paramos. ¿Cuánto dará la suma total?

- Lo estoy pensando, Maestro.

- Más que saber cuánto da la suma total, lo que me gustaría saber, es si se va haciendo muy grande o no. ¿Qué creés?

Y Clara comenzó a escribir los resultados de las sumas anteriores.

- Maestro, las sumas van dando $1, \frac{3}{2}, \frac{7}{4}, \frac{15}{8}, \frac{31}{16}, \frac{63}{32}, \ldots$

-Y estos números, ¿se van haciendo tan grandes como uno quiera, o no? El resultado de la suma total ¿será infinito?

- Parece que no se hacen muy grandes, Maestro. Hasta ahora, son todas fracciones menores que 2.

- ¡Muy bien! Te diré el resultado, para que vos pienses el porqué. Esta suma infinita da 2. Exactamente 2. Con este ejemplo, podemos comprender bien el porqué la paradoja provenía de haber asumido, erróneamente, que el resultado de sumar infinitos tiempos, o números positivos, era infinito.

Dicho esto, Clara y el Maestro se despidieron. Ella se fue pensando en la última suma, aunque a mitad de camino, ya con ganas de llegar de vuelta a su casa, pensó que era una suerte que el movimiento fuera posible, y que lo de Zenón no fuera correcto. Había sido una clase muy provechosa.

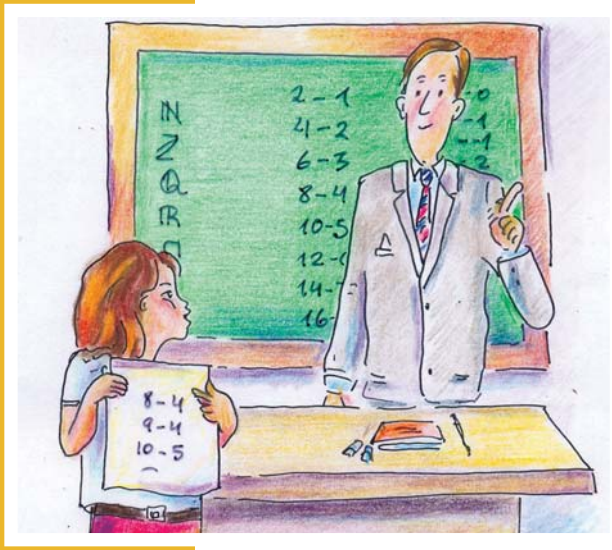
Problema 3.5. Ayudar a Clara a calcular la suma infinita anterior:

Para resolver

Se puede usar calculadora o computadora (aunque no es necesario). Para cada número natural n, consideremos las *sumas parciales* S_n de los primeros n términos, es decir, $S_n = 1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\cdots+\frac{1}{2^n}$.

Calcular S_{10}, S_{20} y S_{100}. Más adelante, veremos que esta suma infinita es una *serie geométrica* y, por lo tanto, no hace falta sumar para obtener los resultados, porque se cumple que $S_n = 2 - \frac{1}{2^n}$. Probar esta igualdad, sacando común denominador en la expresión de S_n recordando que $1 + 2 + 2^2 + 2^3 + \ldots + 2^{k-1} = 2^k - 1$. Observar que esa identidad muestra que $S_n < 2$ para todo n, y en consecuencia la suma infinita no es mayor que 2. Por otra parte, las sumas parciales S_n calculadas para $n = 10$, 20 y 100 muestran que al crecer n, las S_n se acercan tanto como uno quiera a 2.

□ 3.4. Sumas infinitas



Aquel día, el Maestro y Clara, se hallaban enfrascados en la cautivadora y difícil tarea de sumar infinitos números. A Clara le costaba entender lo que esto significaba. El Maestro le mostraba nuevos ejemplos para que ella comprendiera mejor las cosas. Si bien no estaba del todo convencida, lo aceptaba de buen grado. En ese momento, Clara le dijo al Maestro:

- ¿Me lo podría explicar de nuevo, por favor?

- Por supuesto, con todo gusto. Antes, quiero hacerte notar que estamos aprovechando la conversación que tuvimos sobre la paradoja de Aquiles y la tortuga para adentrarnos en un mundo apasionante, el de las "sumas infinitas", donde aparecen conceptos que los matemáticos han llamado *sucesiones, series, límites,…* ah las series infinitas.... qué interesante, ¡qué interesante!

- Mmmhh, veremos.

- ¡Ya vas a ver! Ahora, comencemos con una sucesión infinita de números, una bien sencilla, por ejemplo la de los números naturales impares. Escribamos la *sucesión* de este modo, Clara, que así se la ve muy bien:

1, 3, 5, 7, 9, 11, 13, 15, ...

- No termina nunca, ¿verdad, Maestro?

- Así es. Los puntos suspensivos al final significan eso. Es una tira de números que sigue y sigue, no termina. Tiene comienzo, pero no tiene fin. En este caso sabemos cómo continúa. Por ejemplo, si te pido que me digas cuál es el décimo término de esta sucesión, ¿qué contestás?

- A ver... el 19.

- Bien. ¿Y el término ubicado en el lugar número 100?

Clara comenzó a hacer unos garabatos en su libretita, y bastante rápidamente respondió:
- es el 199.

- Muy bien. Lo estás entendiendo. ¿Cómo lo calculaste? ¿A mano, o con alguna fórmula?

- No sé bien, Maestro; pero no fue difícil.

- ¿Sabrías reconocer una fórmula general para los términos de esta sucesión?
Si te doy la fórmula $2n - 1$, con n variando en los números naturales, ¿podés reconocer ahí una sucesión?

El primer término es el $2 \times 1 - 1$, o sea, el 1. El segundo término es el $2 \times 2 - 1$, o sea el

3. Y si seguimos así, ¿qué tenemos?

- Es la misma sucesión que teníamos, la de los números impares -respondió Clara.

- ¡Por supuesto! La única diferencia es la forma de presentarla, pero es la misma sucesión. Por eso, si te pido el décimo término de la sucesión, basta con reemplazar n por 10 en la "fórmula" que tenemos, $2n - 1$, para obtener $2 \times 10 - 1 = 19$.

- Y para el término número 100, Maestro, también se puede hacer así, ¿no?, o sea $2 \times 100 - 1 = 199$, ¿está bien?

- Sí, muy bien. Ahora tenemos un modo de calcular fácilmente los términos de esta sucesión. Pero continuemos con la suma infinita, a la que también llamaremos *serie* o *serie infinita*. Vayamos sumando los términos, uno por uno. Comencemos con el primer término: tenemos 1. Sigamos, hagamos ahora el primero más el segundo, es decir, $1 + 3$, y el resultado que obtenemos es 4. Sumemos ahora los tres primeros términos de nuestra sucesión, es decir, $1 + 3 + 5$. Obtenemos 9. Ahora los cuatro primeros, $1 + 3 + 5 + 7$, ¿cuánto da? 16. Fijate, que para sumar los cuatro primeros términos, también podríamos sumar el cuarto término al resultado de la suma de los tres primeros, o sea hacer $9 + 7$, y llegaríamos igualmente a 16. Ahora, ¿cuánto da la suma de los primeros cinco términos?

- Es fácil. Da.... $1 + 3 + 5 + 7 + 9 = 25$, o también podía hacer $16 + 9$ y llegar al 25.

- Perfecto. Esto es muy fácil. Pero ahora viene una pregunta diferente. ¿Qué sucede si sumamos *todos* los términos, en el orden en que lo venimos haciendo? ¿Cuánto dirías que da esta "suma", o mejor dicho, esta "serie"?

- Al ir sumando, se va haciendo algo demasiado grande, ¿verdad? A ver, dan 1, 4, 9, 16, 25, y luego 36, 49,... Las sumas se agrandan cada vez más, ¡y no van a parar!

- ¡Así es! Y si estas *sumas parciales* se van haciendo *tan grandes como uno quiera*, entonces vamos a decir que la suma total, o sea la serie, *tiende a infinito*.

- ¿Por qué se dice así? ¿No se podría decir que la suma total da infinito?

- Bueno, sí, sólo que hay que tener cierto cuidado. Te estás adelantando un poco, Clara, eso no es malo. Usamos la palabra "*tiende a*" porque pensamos en cómo van evolucionando las sumas parciales, en su tendencia. También se expresa esto diciendo que el *límite* (de las sumas parciales) es infinito. Aunque esto pueda sonarte un poco raro, te vas a acostumbrar apenas calcules el resultado de dos o tres series, como estamos haciendo. Ahora me gustaría que comparemos esta serie, con la anterior que vimos. ¿Te acordás? En ambas, siempre vas sumando cosas positivas, y por lo tanto las sumas parciales van creciendo cada vez más. Pero hay una diferencia esencial: mientras que aquéllas no superaban el 2, éstas crecen tanto como

se quiera, y tienden a… -y el Maestro hizo una pausa para que Clara contestara.

- ¡Infinito!

- Muy bien. Entonces debemos ser rigurosos, ya que el sólo hecho que las sumas parciales vayan creciendo y creciendo no significa que tiendan a infinito.

- Creo que lo entiendo, Maestro, aunque me gustaría entender mejor qué significa lo de "tan grande como uno quiera".

- A ver, Clara decime un número grande.

- Mil –dijo Clara, con cierto temor a decepcionarse si el Maestro le hacía el chiste tonto de decirle "1.001, te gané". Afortunadamente, el Maestro la sorprendería con otra "gracia" mucho mejor.

- Bien. Sumemos los primeros 32 términos de nuestra sucesión. ¿Cuánto es, Clara?

Ella sacó su calculadora y comenzó a manipularla hábilmente. Al cabo de un rato dijo

- ¡Da 1.024!

Y al terminar de pronunciarlo, se asombró cuando se dio cuenta de que este número era apenas mayor que 1.000, el que ella había elegido.

- Ves, Clara. Dijiste un número, y nuestra serie, lo superó. No sólo eso, sino que si sumamos los primeros 33 términos también supera, o los primeros 100 también, o con mayor generalidad, si $k \geq 32$, entonces la suma parcial de los primeros k términos es mayor que 1.000. Además, si hubieras dicho otro número grande, distinto de 1.000, también podríamos haber descubierto cuántos términos necesitábamos para superar tu número. ¿Hacemos otra prueba?

- Bueno, digo 10.000.

- Entonces yo digo 101. Si hacemos la suma parcial de los primeros 101 términos, da 10.201, que es mayor que diez mil. ¿Querés hacer una prueba más?

- No, Maestro, le creo.

- Eso es lo que significa "tan grande como uno quiera", o lo mismo, "que tiende a infinito". ¿Qué ocurre, no se entiende? -preguntó el Maestro al ver a Clara algo desconcertada.

- No, no es eso. Entiendo que esta suma "tiende a infinito". Lo que no descubro aún, es cómo hizo para saber que la suma de los primeros 32 términos daba mayor que 1.000, sin calcularlo. Porque además, si sumamos los primeros 31 términos, da 961, que es menor que 1.000. O sea, que 32 es el menor número de términos que sumados superan al número 1.000. Y lo mismo pasa con el 101 y el diez mil ¡Estoy sorprendida!

- Bueno, Clara, el cálculo que hice se basa en un lindo truco. Si te acordás de cuánto daban las sumas parciales y pensas en ellas lo vas a descubrir.

- A ver, daban 1, 4, 9, 16, 25, 36, 49,.... ¡Ah! ¡Son los cuadrados perfectos! Entonces, cuando tenemos k términos, la suma parcial es k^2.

- Así es, ya estás muy cerca.

- Ahora tengo que ver qué número k al elevarlo al cuadrado da mayor que 1.000. Sé que 30 por 30 es 900, y con una cuentita más, llego a que el primer número que cumple esto es el 32.

- Muy bien, me alegro que lo hayas descubierto. Lo único que no hiciste fue demostrar que las sumas parciales dan realmente los cuadrados perfectos. Esto se logra, por ejemplo, verificando que si a la suma parcial de los primeros k términos le sumamos el siguiente término, que es $(2k+1)$, entonces se obtiene $(k+1)^2$, pues $k^2 + (2k+1) = k^2 + 2k + 1 = (k+1)^2$. Ahora estamos seguros que las sumas de los primeros números impares da siempre un cuadrado perfecto.

- Maestro, creo que me están empezando a gustar las series.

- Me alegro. ¡Veremos más!

3.5. La serie geométrica y la serie armónica

- ¿Clara te acordás de la serie $1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots + \frac{1}{2^n} + \dots$?

- Sí, la vimos hace poquito. Dijimos que "tiende a 2" ¿verdad?

- Así es. Vimos que sus valores se acercaban tanto a 2 como uno quería, por lo tanto, tiende a 2, o también, decimos que su límite es 2. Lo que quería contarte ahora, es que si bien esta serie nos ha resultado muy especial, porque nos ha mostrado por primera vez que la suma de infinitos números positivos puede ser finita, en realidad, desde otro punto de vista, no es rara, inclusive es un caso particular de algo más general.

Clara miraba intrigada. El Maestro continuó.

- Se trata de las series geométricas, donde se toma el parámetro r igual a un medio. En general, r puede ser cualquier número entre cero y uno. Se considera la suma de las potencias de r :
$1 + r + r^2 + r^3 + r^4 + r^5 + r^6 + \dots$ la **serie geométrica** (de razón r) y se demuestra que tiende a $\frac{1}{1-r}$.

- Ah, ya veo, Maestro: si $r = \frac{1}{2}$, entonces $\frac{1}{1-r} = \frac{1}{1-\frac{1}{2}} = \frac{1}{\frac{1}{2}} = 2$.

- Bien. Ahora te propongo que me ayudes a *demostrar* que realmente la serie geométrica de razón r tiene límite finito igual a $\frac{1}{1-r}$. Será sólo una manipulación algebraica. ¡Manos a la obra! Escribimos $S_n = 1 + r + r^2 + r^3 + r^4 + r^5 + r^6 + \dots + r^n$. Multiplicamos ambos miembros por r, ¿qué nos queda?

- Creo que $r \,.\, S_n = r + r^2 + r^3 + r^4 + r^5 + r^6 + \dots + r^n + r^{n+1}$.

- Bien. Ahora restamos miembro a miembro la primera identidad de la segunda. Clara, ¿podés escribirlo?, por favor.

- A ver ..., se simplifica casi todo a la derecha del signo igual ¿no? Queda $r \cdot S_n - S_n = r^{n+1} - 1$.

- Bien. Ahora sólo hay que despejar S_n de esta ecuación. ¿Podrás hacerlo?

- Sí. Me queda $(r-1) \cdot S_n = r^{n+1} - 1$, y entonces $S_n = \dfrac{r^{n+1}-1}{r-1}$.

- Te quiero recordar que para hacer el último paso r - 1 debe ser distinto de cero, y esto es así porque habíamos tomado r menor que 1. También podemos escribir esto así: $S_n = \dfrac{1-r^{n+1}}{1-r} = \dfrac{1}{1-r} - \dfrac{r^{n+1}}{1-r}$, y ahora sólo nos queda decir que cuando r satisface que $0 < r < 1$, entonces r^{n+1} se va haciendo cada vez más chico a medida que n crece, de modo que $\dfrac{r^{n+1}}{1-r}$ tiende a cero cuando n tiende a infinito. Y así llegamos a que la serie tiende a $\dfrac{1}{1-r}$, como queríamos mostrar.

- Maestro, voy a escribir bien todo para poder revisarlo en mi casa.

- Muy bien. Quizá te gustaría calcular cuánto da la serie geométrica de razón un tercio, o sea $r = \dfrac{1}{3}$. Escribila, por favor.

Y Clara escribió $1 + \dfrac{1}{3} + \left(\dfrac{1}{3}\right)^2 + \left(\dfrac{1}{3}\right)^3 + \left(\dfrac{1}{3}\right)^4 + \left(\dfrac{1}{3}\right)^5 + \left(\dfrac{1}{3}\right)^6 + \cdots$

Para resolver

Problema 3.6. Calcular cuánto da esta serie, es decir, el valor de la suma total.

- Qué lindo. Nunca pensé que en un ratito iba a poder calcular varias sumas infinitas.

- Bueno, justo éstas que hemos visto se pueden calcular bien, pero otras pueden ser extremadamente difíciles. Hasta ahora, mirando cuánto van dando las sumas parciales, pudimos intuir o vislumbrar si la seria tiende a infinito o no.

- ¿Y no siempre es así?

- No, Clara, para nada. Lo veremos ahora mismo. Analizaremos una serie que es bastante distinta de las anteriores, por lo que deberás estar muy atenta. En lugar de tomar los números naturales, tomemos sus inversos, y consideremos la sucesión que forman, que la escribimos así:

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \ldots$$

Como siempre, los puntos suspensivos indican que sigue indefinidamente. También se puede describir como la sucesión $\dfrac{1}{n}$ donde n varía en el conjunto de los números naturales. El primer término es $\dfrac{1}{1}$, el segundo, $\dfrac{1}{2}$, el tercero, $\dfrac{1}{3}$, y en general, el término n-ésimo es el número $\dfrac{1}{n}$, para cada número natural n. ¿Alguna pregunta?

- No, está clarito cuál es la sucesión.

- Bien. Ahora pensemos en la serie, conocida como serie armónica. Es decir:

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \ldots$$ ***la serie armónica***

Comencemos a calcular las llamadas sumas parciales de la serie, que van dando los siguientes números: primero el 1; segundo tenemos 1 + 1/2 = 3/2; luego hacemos 1 + 1/2 + 1/3, que da 11/6; continuamos con 1 + 1/2 + 1/3 + 1/4 = 25/12; etc. Apuntamos a saber si

tiende a infinito o a algún número finito.

- Maestro, ¿se puede hacer alguna de las manipulaciones algebraicas de la clase pasada para tener una expresión de las sumas parciales?

- No, que yo sepa. Por eso, esto se presenta, a priori, como difícil. Primero vamos a analizar la serie *numéricamente*, es decir, calculando cuánto van dando aproximadamente las sumas parciales, y tratando de ver si crecen mucho o no.

- ¿Saco mi calculadora, Maestro?

- Sí, claro, la vamos a usar, y también necesitamos una computadora, aunque me temo que no serán suficientes- comentó el Maestro en voz apenas audible-. Comencemos, Clara. Al principio las sumas parciales van creciendo relativamente a buen ritmo a medida que sumamos los términos. Al comenzar, pasamos de 1 a 3/2, o sea, a 1,5, luego al $\frac{11}{6} \cong 1{,}833$, luego a $\frac{25}{12} \cong 2{,}0833$. Pero cuando ya hemos sumado muchos términos, al sumar el siguiente no logramos modificar mucho la suma. Por ejemplo, el término número 1.000 es 1/1.000, o sea, 0,001. De modo que sólo modificamos la suma en el tercer dígito después de la coma. Si pensás en el millonésimo término, el número a sumar será 1/1.000.000, o sea 0,000001, que es muy pequeño, y sólo modificarás el sexto dígito a la derecha de la coma, ¿estás de acuerdo?

- Sí. Se está complicando, pero creo que lo entiendo. Siga, Maestro, por favor.

- Si sumamos los diez primeros términos, tenemos 1+1/2+1/3+1/4+...+1/10. ¿Por favor, podés calcular su valor numérico aproximado?

Usando velozmente su calculadora, Clara respondió:

- Da 7.381/ 2.520, que es aproximadamente 2,928968254.

- Bien. Aumentó, pero no mucho. Si seguimos sumando, tantos términos como queramos, ¿hasta dónde podremos llegar? ¿Podremos superar cualquier número grande, por más grande que éste sea? Por ejemplo, ¿podremos alcanzar el 10? ¿Y el 100? ¿Qué te parece? Dicho de otro modo, la gran pregunta es si esta serie tiende a infinito o no.

- Parece muy interesante. Pero no lo sé. Esto es nuevo para mí.

- Es verdad. Tenés que tomarte tu tiempo para asimilarlo. Recordá que lo que tenemos es una tira muy larga de números, tan larga, que no termina, y que los debemos ir sumando, ordenadamente. Y tenemos que intentar deducir si esa suma puede llegar a superar el número 100 o no.

- Maestro, entiendo la pregunta. Pero tengo que hacer muchas cuentas para ver qué va sucediendo con esta serie.

- Clara, no es difícil escribir un programa que haga estas sumas. Sólo lleva unas pocas líneas. Por ejemplo:

> n := 10 (n representa la cantidad de términos que vamos a sumar)
> sum := 0
> Para j desde 1 hasta n hacer sum := sum + $\frac{1}{j}$
> mostrar el valor de "sum"
> mostrar el valor de "sum" en notación decimal.

Clara escribió el programa (de sólo cinco líneas) en su computadora.
- Hagamos correr el programita -dijo el Maestro.

- La respuesta en la pantalla es: 7.381/ 2.520 ≅ 2,928968254.

- Debemos interpretar el resultado así: los primeros diez términos de nuestra serie suman 7.381/ 2.520 que es igual, o aproximadamente igual, a 2,928968254. Ahora, simplemente cambiando el valor de *n* en la primera línea del programa, por ejemplo de 10 a 100, obtendremos el valor de la suma parcial de los primeros cien términos de la serie armónica. ¿Querés hacerlo Clara?

Clara puso *n*=100 y obtuvo la respuesta
14.466.636.279.520.351.160.221.518.043.104.131.447.711 /
/ 2.788.815.009.188.499.086.581.352.357.412.492.142.272 igual (aprox.) a 5,187377518

Luego, fueron calculando los valores aproximados de las sumas parciales para los primeros 1.000 términos, los primeros 10.000 y el primer millón de términos. Al principio, la computadora respondió rápidamente, pero luego empezó a demorarse bastante. Se dieron cuenta que tardaría mucho intentar con 10 millones. Escribieron los resultados en una tabla:

cantidad de términos	10	100	1.000	10.000	100.000	1millón
valor suma parcial	2,92896	5,18737	7,48547	9,78760	12,0901	14,3927

- Tarda mucho, Maestro. Y solo hemos logrado sumar algo menos que 15, con el primer millón de términos.... ¡Es poquísimo!

- Me alegro que hayamos escrito el programita y la tabla, Clara, aunque los resultados en este caso no nos permiten saber la respuesta, ni siquiera intuirla.

- Mirando la tabla no soy capaz de decir nada, porque le está costando muchísimo crecer. Superó el 10, pero está lejísimos del 100. Aunque la serie sigue creciendo un poco, creo que no vamos a poder contestar su pregunta Maestro.

- ¡Podremos Clara! Esta es otra maravilla de la matemática. Es capaz de mostrarte cosas que parecen muy difíciles, pero cuando encuentras un buen camino, se tornan sencillas. Como ves, en este caso el conocimiento de las primeras sumas parciales no nos ha servido de mucho. Seguimos desorientados. Pero una idea ingeniosa nos dará la respuesta de si la serie armónica tiende a infinito o no. ¿Qué crees que ocurre?

- Crece muy poco, parece que no va a tender a infinito, pero realmente no lo sé.

- Mirá, si sumamos el tercer término y el cuarto término, da algo que es mayor que $\frac{1}{2}$, pues $\frac{1}{3} > \frac{1}{4}$, luego $\frac{1}{3}+\frac{1}{4} > \frac{1}{4}+\frac{1}{4} = \frac{1}{2}$. Hacemos lo mismo con los siguientes cuatro términos. Sabemos que $\frac{1}{5} > \frac{1}{8}$, $\frac{1}{6} > \frac{1}{8}$ y $\frac{1}{7} > \frac{1}{8}$, por lo tanto tenemos que $\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8} > \frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8} = \frac{1}{2}$.
¿Te das cuenta cómo va funcionando?

- Más o menos.

- Espero que el siguiente gráfico sea muy ilustrativo:

$$1+\underbrace{\frac{1}{2}}_{\geq\frac{1}{2}}+\underbrace{\frac{1}{3}+\frac{1}{4}}_{>\frac{1}{2}}+\underbrace{\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}}_{>\frac{1}{2}}+\underbrace{\frac{1}{9}+\frac{1}{10}+\frac{1}{11}+\frac{1}{12}+\frac{1}{13}+\frac{1}{14}+\frac{1}{15}+\frac{1}{16}}_{>\frac{1}{2}}+\cdots$$

Si vas juntando los términos de a dos, de a cuatro, de a ocho, de a dieciséis,…, siempre se consigue sumar por lo menos un medio.

- Ahora lo entiendo ¡Qué bárbaro, Maestro! Entonces llega a 100!

- Sí. La suma supera el cien, y también el mil, y también el 10 mil, etc. Por lo tanto, esta serie tiende a infinito. Como vimos, lo hace muy lentamente, pero lo hace. ¿Te ha sorprendido la *demostración*?

- Sí, no me la esperaba. Ahora, ¿no es raro, Maestro, que sume tan poquito, y sin embargo se agrande tanto como queramos?

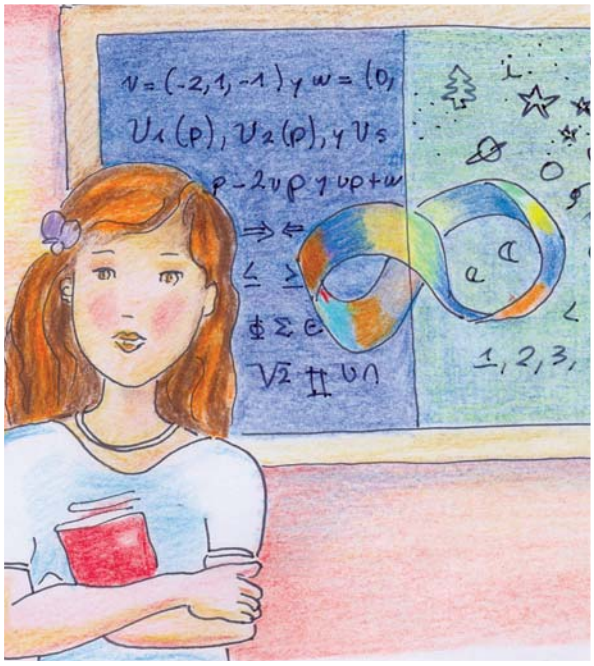
- Sí, es un caso bastante especial. Pero fijate que son infinitos términos. Si bien se van haciendo muy chiquitos, ellos alcanzan para sumar mucho, como vimos. Esta serie armónica es una de las series más interesantes que hay.

Para resolver

Problema 3.7. Hallar un número n tal que la suma de los primeros n términos de la serie armónica sea mayor que 25.

[Ayuda: juntar 50 pedacitos de la serie como en el dibujo, de modo que cada uno sume un medio o mayor que un medio.]

3.6. ¡Los números racionales son numerables! ... ¿y los reales?



- Antes de comenzar, Clara, te propongo que llamemos *numerable* a cualquier conjunto cuyos elementos se puedan numerar como primero, segundo, tercero, cuarto, quinto,…, y de ese modo se llegue a numerar o nombrar a todos sus elementos, es decir, un conjunto coordinable con el conjunto de los números naturales **N**. Por ejemplo, el conjunto de los números enteros **Z** es numerable.

Definición. Un conjunto se dice numerable si es coordinable con **N**, es decir, si se puede establecer una correspondencia biunívoca entre los números naturales y sus elementos

La palabra "numerable" tiene sentido para un conjunto coordinable a **N**, porque a través de la correspondencia

biunívoca entre **N** y el conjunto, se puede hacer una lista con los elementos del conjunto, que comienza y no tiene fin, donde van apareciendo todos los elementos de dicho conjunto. Si alguien fuera leyendo en voz alta la lista, entonces estaría *nombrando* a todos los elementos del conjunto. ¿Se entiende? A ver, ¿podrías decir otro conjunto numerable que no sea **N** ni **Z**?

- Eh… sí. Vimos que los naturales pares eran así, ¿no es cierto?

- Sí, así es. Hoy y la clase que viene me gustaría que conversáramos sobre algo verdaderamente nuevo para vos. Primero, quiero que nos introduzcamos en los números racionales (o fraccionarios), y que averigüemos si se los puede enumerar a todos. Luego, con cierta audacia, iremos por los números reales. Nos vamos a encontrar con que no es posible nombrar uno por uno a todos los números reales, o dicho en otras palabras, que el conjunto **R** *no es numerable*, lo que significa que no es coordinable con el conjunto **N**.

- Bien, Maestro. Ojalá pueda entender todo lo que ha dicho, que parece muy interesante.

- Estoy seguro que sí. No sólo eso, sino que tengo la esperanza de que termines maravillada por la importancia y la belleza de los resultados que veremos hoy.

Clara sonrió ante estas palabras. Si bien apreciaba mucho estas clases, le resultaba difícil creer que le podría pasar lo que el Maestro esperaba.

- ¿Le parece, Maestro, que estos resultados son *bellos*?

- ¡Por supuesto! Comencemos ahora mismo. Recordemos que los números fraccionarios son de la forma $\frac{m}{n}$ donde m y n son números enteros, y n es distinto de cero. También se los llama *números racionales*, y se denotan con una **Q**. Por ejemplo, tenemos $\frac{2}{3}, -\frac{24}{7}, \frac{7}{5}, \frac{6}{1}$, etc. Si tomamos $n = 1$, entonces $\frac{m}{n}$ no es otra cosa que un número entero. Esto nos muestra que los enteros son racionales, o equivalentemente, que el conjunto de los números enteros está contenido en el de los números racionales. En símbolos podemos escribir $\mathbf{Z} \subset \mathbf{Q}$. De este modo, está claro que hay infinitos racionales, ¿verdad? Ahora, una pregunta muy interesante es si los números racionales son numerables o no. Es decir, si **Q** es un conjunto coordinable a **N** o, si por el contrario, no existe una correspondencia biunívoca entre ambos conjuntos, en cuyo caso, resultaría ser mayor en cardinal, o sea, card **Q** > card **N**. Es la misma pregunta que nos planteamos hace tiempo entre **Z** y **N**, ¿te acordás?

- Sí me acuerdo, Maestro.

- Bien. Claro que el conjunto **Q** es muy distinto a los anteriores en algunos aspectos. Mientras que los números enteros están espaciados por intervalos de longitud uno, los racionales están por todas partes, son increíbles, se meten en todos los intervalos. Si realizamos la representación usual de los números reales en una recta, entonces no importa en qué punto de la recta te pares, tendrás números racionales tan cerca como quieras.

- La verdad es que **Q** parece mucho más grande que **N**. Si pienso, por ejemplo, solamente en los medios enteros, o sea 1/2, 2/2=1, 3/2, 4/2=2, 5/2,…, parece que se corresponden con los naturales, ¿no es así? Y solamente he usado los que tienen denominador igual a 2. Después, puedo pensar en los que tienen denominador igual a 3, luego los con denominador 4, etc. Pero creo que con esto todavía no voy a poder contestar su pregunta.

- Está muy bien tu observación, Clara. De modo que una parte de **Q** -los racionales con

denominador igual a 2- es coordinable a todo **N**. Pero como señalaste, eso no contesta la pregunta, porque lo mismo sucedía con **Z**, que resultó ser numerable. Si me dejás que te ayude, te diría que intentaras *nombrar* a todos los números racionales. Es decir, que hagas una lista ¡donde vayan apareciendo todos!

- Me está diciendo que trate de ver que **Q** es numerable. ¡Es sorprendente!

- Así es. Lo que estamos diciendo, es que es posible dar una lista -infinita, por cierto- con todos los números racionales. Al principio, asombra que puedas poner tantos números en una lista, pero si se piensa mejor, no hay mucha diferencia con el Hotel Hilbert, donde el conserje era capaz de "meter" todos esos contingentes de infinitas personas en las habitaciones del hotel. Los contingentes serían como los números racionales, cada contingente un denominador distinto, y las habitaciones del hotel como los números naturales.

- Es un problema muy lindo, Maestro, y en este caso, me gustaría verlo bien, o como a usted le gusta decir, ver una "demostración".

- Excelente. Esa es la forma en que realmente vas a entenderlo. Antes de escribir la correspondencia biunívoca entre **N** y **Q**, sería mejor hacerla entre **N** y $\mathbf{Q}^+$, los números racionales positivos. Luego, veremos sin dificultad que $\mathbf{Q}^+$ y **Q** son coordinables, y de las dos cosas resultará que **N** y **Q** son coordinables. ¿Estás de acuerdo?

- Creo que sí.

- Bien. Entonces ayudame a hallar un modo de nombrar a todos los racionales positivos, uno por uno, sin que nos olvidemos de ninguno. Hagamos un cuadro bien grande, con filas y columnas. Primero ponemos los números 1, 2, 3, 4, … en la fila de arriba y también en la columna de la izquierda. Estos números serán los que encabezan las filas y columnas. Luego, en cada lugar del cuadro ponemos una fracción, cuyo numerador es el número que está encabezando la columna y el denominador el número que está encabezando la fila. Fijate, Clara, que en el cuadro van apareciendo todos los racionales positivos. Por ejemplo, el $\frac{7}{3}$ está en la tercera fila y séptima columna. Si te digo el $\frac{12}{2.009}$ ¿dónde estará?

	1	2	3	4	5	6	7	8	9	…
1	$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{1}$	$\frac{4}{1}$	$\frac{5}{1}$	$\frac{6}{1}$	$\frac{7}{1}$	$\frac{8}{1}$	$\frac{9}{1}$	…
2	$\frac{1}{2}$	$\frac{2}{2}$	$\frac{3}{2}$	$\frac{4}{2}$	$\frac{5}{2}$	$\frac{6}{2}$	$\frac{7}{2}$	$\frac{8}{2}$	$\frac{9}{2}$	…
3	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{3}{3}$	$\frac{4}{3}$	$\frac{5}{3}$	$\frac{6}{3}$	$\frac{7}{3}$	$\frac{8}{3}$	$\frac{9}{3}$	…
4	$\frac{1}{4}$	$\frac{2}{4}$	$\frac{3}{4}$	$\frac{4}{4}$	$\frac{5}{4}$	$\frac{6}{4}$	$\frac{7}{4}$	$\frac{8}{4}$	$\frac{9}{4}$	…
5	$\frac{1}{5}$	$\frac{2}{5}$	$\frac{3}{5}$	$\frac{4}{5}$	$\frac{5}{5}$	$\frac{6}{5}$	$\frac{7}{5}$	$\frac{8}{5}$	$\frac{9}{5}$	…
6	$\frac{1}{6}$	$\frac{2}{6}$	$\frac{3}{6}$	$\frac{4}{6}$	$\frac{5}{6}$	$\frac{6}{6}$	$\frac{7}{6}$	$\frac{8}{6}$	$\frac{9}{6}$	…
7	$\frac{1}{7}$	$\frac{2}{7}$	$\frac{3}{7}$	$\frac{4}{7}$	$\frac{5}{7}$	$\frac{6}{7}$	$\frac{7}{7}$	$\frac{8}{7}$	$\frac{9}{7}$	…
8	$\frac{1}{8}$	$\frac{2}{8}$	$\frac{3}{8}$	$\frac{4}{8}$	$\frac{5}{8}$	$\frac{6}{8}$	$\frac{7}{8}$	$\frac{8}{8}$	$\frac{9}{8}$	…
9	$\frac{1}{9}$	$\frac{2}{9}$	$\frac{3}{9}$	$\frac{4}{9}$	$\frac{5}{9}$	$\frac{6}{9}$	$\frac{7}{9}$	$\frac{8}{9}$	$\frac{9}{9}$	…
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

Clara pensó un poco. Este número no aparecía en el cuadro que habían dibujado, porque no entraba en el pizarrón. Entonces dijo:

- El $\frac{12}{2.009}$ se encontraría en la decimosegunda columna y en la fila 2.009. Aunque no lo hayamos escrito, es como si estuviera ahí.

- ¡Bien! Dije $\frac{12}{2.009}$ pero podría haber dicho cualquier otro número racional positivo. De modo que todos ellos se encuentran en este cuadro infinito. Por supuesto que hay repeticiones. Por ejemplo, en la diagonal, encontramos siempre $\frac{m}{m} = 1$, son todos unos. Pero lo importante para nosotros no son estas repeticiones, sino que en el cuadro

están todos los racionales positivos. Ahora, ¿habrá alguna forma de nombrarlos? Es decir, ¿cómo se podría organizar la tarea de ir nombrando a todos, uno por uno?

- A ver…. si voy nombrando los medios enteros, o sea, los de la segunda fila, creo que voy a estar en problemas, porque la fila no se termina nunca, y todavía no he empezado a nombrar los números de la tercera fila, o sea los "tercios", ni los "cuartos" de la cuarta fila, etc. Por eso, estoy pensando si lo puedo hacer de otra forma.

- Vas a poder. Lo que tenés que evitar es quedarte en una fila o en una columna.

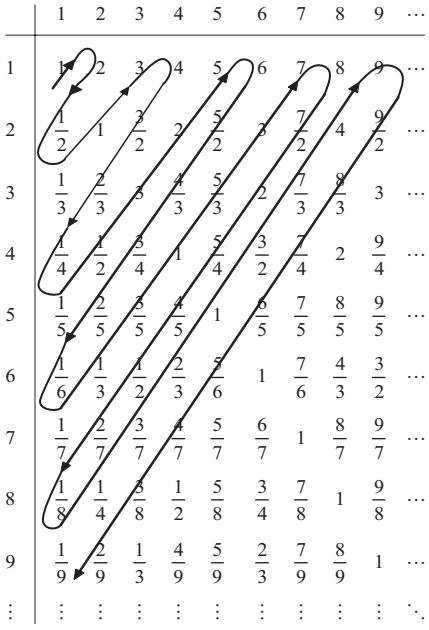
- Quizás… si voy nombrando primero el $\frac{1}{1}$, después el $\frac{2}{1}$ y el $\frac{1}{2}$, luego $\frac{3}{1}$, $\frac{2}{2}$ y $\frac{1}{3}$, y sigo así, ¿podría ser?

Clara marcó diagonales en el cuadro, unas iban desde abajo a la izquierda hacia arriba a la derecha y otras en sentido opuesto. El maestro sonrió gratamente y dijo:
- Sí. Comenzás desde el primer lugar, luego pasás a la primera fila segunda columna y recorrés la diagonal que señalaste, luego vas a la tercera fila primera columna y subís por tu diagonal, y así seguimos. Cada vez que se termina una diagonal, continuamos por la siguiente, alternando el modo de recorrerla. ¡Ésta es una forma de ir nombrando todos los números del cuadro!

- ¡Qué lindo!

- Si no hubiera repeticiones, ya habríamos demostrado que $\mathbf{Q}^+$ es numerable.

- Pero ¿qué pasa con los repetidos? -preguntó Clara queriendo entender esto-. ¿Como sería la correspondencia biunívoca?



- Bueno, los repetidos no son importantes, aunque molestan, es verdad. Pero vamos a sacárnoslos de encima. Una forma de establecer la correspondencia biunívoca que buscamos, es nombrar todos los racionales, por las diagonales, como lo estábamos haciendo, pero ahora *sin repetirlos*. Es decir, simplemente tenemos que saltear los que se repiten. Cada vez que llegamos a una casilla de nuestro cuadro con un número racional, antes de nombrarlo en voz alta, debemos verificar que no lo hayamos nombrado antes. Recuerda para este fin que $\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \frac{4}{8} = \ldots$; también $\frac{3}{2} = \frac{6}{4} = \frac{9}{6} = \ldots$, etc., de modo que si bien es una tarea fácil, no es inmediato decidir si un número ya apareció antes o no. Pero puede hacerse, y sólo requiere unas cuantas comparaciones. ¿Lo entendiste, verdad? ¿Podrías nombrar los primeros racionales de nuestra lista sin repeticiones?

- Sí. A ver. 1, 2, $\frac{1}{2}$, $\frac{1}{3}$, ahora no pongo el $\frac{2}{2}$ porque es 1, que ya está, así que sigo con 3, 4, $\frac{3}{2}$, $\frac{2}{3}$, $\frac{1}{4}$, $\frac{1}{5}$, (salteo el $\frac{2}{4}$, lo mismo que al $\frac{3}{3}$ y al $\frac{4}{2} = 2$) sigo con 5, 6, $\frac{5}{2}$, $\frac{4}{3}$, $\frac{3}{4}$, $\frac{2}{5}$, $\frac{1}{6}$, ¿sigo? Ya me estoy cansando.

- No es necesario que sigas. Ya hemos tenido una muestra, pequeña pero suficiente, de cómo se pueden ir nombrando todos los racionales positivos, eventualmente a cada número le llegará su turno.
Hay un gran teorema matemático, llamado *Teorema de Cantor-Bernstein-Schroeder*, que permite ahorrar inconvenientes como el de las repeticiones, y muchísimos más. Es de gran importancia y utilidad. Primero voy a tratar de mostrártelo intuitivamente, y luego lo podremos enunciar formalmente. Ahora, recordemos esto: si tenemos dos conjuntos A y B que satisfacen que A está contenido o es igual a B, y a su vez B está contenido o es igual a A, entonces, ¿cómo deben ser A y B ?

- A y B tienen que ser iguales -contestó Clara.

- Por supuesto. En símbolos, si $A \subseteq B$, $B \subseteq A$, entonces $A = B$. Lo que nos dice el teorema es una variación, más general y sutil, de lo anterior. En lugar de tener como hipótesis $A \subseteq B$, vamos a suponer que hay asignación de A en B que no repite elementos. Es decir, a cada elemento de A se le asigna (o se le hace corresponder) un elemento de B, y no se le puede asignar el mismo de B a dos elementos distintos de A. Es como estar "metiendo" el conjunto A en B, a través de dicha asignación ¿no te parece?

- Sí, pero todavía no sé qué dice el gran teorema.

- Paciencia, Clara. La otra hipótesis que cambiamos es la de $B \subseteq A$ por la de que haya una asignación de B en A que no repita elementos de A, es decir, a cada elemento de B se le asigna uno de A, y a elementos distintos de B se les asignan elementos distintos de A. Si tenemos estas dos hipótesis, ¿cuál será la conclusión del teorema?

- Lo estoy pensando.

- Bien. En otras palabras, lo anterior es equivalente a decir que de nuestros conjuntos A y B sabemos que A es coordinable a una parte de B, y que B es coordinable a una parte de A. ¿Qué te parece que ocurre entonces? ¿Cómo son A y B ?

- Bueno, al principio es como si A fuera más chico que B, pero después es como si B fuera más chico que A, así que creo que A y B son iguales.

- ¿A qué te referís con "iguales"? ¿Querés decir coordinables?

- Sí, claro, quiero decir que A y B tienen que ser coordinables.

- ¡Bravo! Lo comprendiste. Ésta es una de las formas de enunciar el teorema, hay muchas más. No vamos a hacer una demostración formal del mismo, pero lo vamos a usar, por ejemplo, para demostrar nuevamente que $\mathbf{N}$ y $\mathbf{Q}^+$ son coordinables. A pesar de que no hemos enunciado todas las versiones de este teorema, me gustaría remarcarte lo esencial: si tenemos dos conjuntos A y B, y hay algún modo de ver que A es "más chico" que B, y otro de ver que B es "más chico" que A, entonces se puede concluir que A y B son coordinables. Me gustaría que intentes aplicar el teorema al caso de $\mathbf{N}$ y $\mathbf{Q}^+$. ¿Te animás?

Teorema de Cantor-Bernstein-Schroeder. Si A y B son conjuntos tales que A es coordinable a una parte de B y B es coordinable a una parte de A, entonces A y B son coordinables, o lo que es lo mismo, card A = card B.

- Sí, pero no sé si voy a poder completar la demostración.

- Vas a ver que sí.

- Bueno, lo intento. Hay una forma natural de meter los naturales en los racionales positivos, así que ya sabemos que es como si **N** fuera más chico que $\mathbf{Q}^+$. Después, el recorrido que hicimos de las diagonales del cuadro nos dice que es como si **N** fuera "más grande" que $\mathbf{Q}^+$, ¿verdad?

- Sí. Continúa

- Entonces, según lo que dijo usted sobre lo esencial del teorema, tenemos que **N** y $\mathbf{Q}^+$ son coordinables.

- Lo has hecho muy bien. Ahora te dejo un problema para que pienses en tu casa, con él se completa la demostración de que **N** y **Q** son coordinables.

Para resolver

Problema 3.8. Hallar una correspondencia biunívoca entre el conjunto de los números racionales **Q** y el conjunto de los racionales positivos $\mathbf{Q}^+$.

[Ayuda: considerar una numeración $q_1, q_2, q_3, q_4, q_5, \ldots$ de $\mathbf{Q}^+$, luego **Q** consiste del 0 y de $\pm q_j$, con j = 1, 2, 3, 4, 5, ...]

El Maestro estaba contento de ver cómo Clara lograba completar algunas demostraciones complicadas. Luego de una pausa continuaron.

- Ahora, veamos otras formas de expresar el resultado de que **Q** es numerable. Creo que te gustarán. Una forma es mostrando que "la unión numerable de conjuntos numerables es numerable".

- ¿¡Cómo es eso!? -dijo Clara confundida, casi quejándose por lo difícil que le sonaba lo enunciado.

- Te acordás de la unión de conjuntos, ¿verdad? Si consideramos dos conjuntos numerables A y B, entonces su unión, $A \cup B$, también será numerable. Es decir, si hay una forma de ir nombrando los elementos de A, y otra de nombrar los de B, entonces habrá una forma de nombrar todos los elementos que estén en cualquiera de esos dos conjuntos. ¿Estás de acuerdo?

- Sí, eso lo entiendo bien. Por ejemplo, puedo ir nombrando primero el primer elemento de A, después el primer elemento de B, luego el segundo elemento de A, sigo con el segundo de B, ahora el tercero de A, el tercero de B, y así sigo.

- Bien, Clara. En símbolos, podríamos ponerlo así: si $A = \{a_1, a_2, a_3, a_4, a_5, \ldots\}$ y $B = \{b_1, b_2, b_3, b_4, b_5, \ldots\}$, entonces $a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4, a_5, b_5, \ldots$ es una forma de nombrar todos los elementos de la unión de A y B. Nuevamente, podemos tener el problema de las repeticiones, puesto que puede haber elementos en A y en B simultáneamente que estaríamos nombrando dos veces. Pero eso se arregla, como lo hicimos con las repeticiones en $\mathbf{Q}^+$ en el cuadro.

Lo que te estaba diciendo antes, era que si en lugar de hacer la unión de sólo dos conjuntos numerables A y B, hacemos la unión de tres, cuatro, o de una lista infinita de conjuntos numerables $A_1; A_2; A_3; A_4; A_5; \ldots$ entonces esta unión también será un conjunto numerable.

- Ahora sí entiendo lo que quiere decir.

La unión finita o numerable de conjuntos numerables es numerable.

- No es difícil demostrar esta afirmación. En rigor de verdad, ya lo hemos hecho, sólo que puede haber pasado desapercibido porque no era exactamente eso lo que estábamos demostrando, sino algo análogo. En este caso, Clara, podemos proceder con las diagonales del cuadro ¿te acordás?

- Bueno. Voy a pensar que los conjuntos A_1, A_2, A_3, A_4, A_5, ..., son todos numerables, y tengo que ver que puedo numerar la unión de estos conjuntos. Entonces voy a dibujar un cuadro como el que hicimos antes. En la primera fila pongo los elementos de A_1, en la segunda los de A_2, en la tercera los de A_3, etc. Ahora, si los voy nombrando como hicimos antes con el cuadro de $\mathbf{Q}^+$, creo que voy a nombrar a todos los elementos, ¿no?

- Sí, muy bien. Veo que has entendido que la unión de conjuntos numerables es numerable, cuando tenés una lista de conjuntos, o sea, una cantidad finita o infinita numerable de conjuntos a unir. Es un resultado que puede sorprender. Entusiasmados, podríamos llegar a pensar, erróneamente, que todos los conjuntos son numerables. Pero pronto veremos que el conjunto de los números reales, **R**, no lo es. Por consiguiente, tendremos al menos dos tipos distintos de infinitos, el llamado *infinito numerable*, que corresponde a la cantidad de números naturales, y un nuevo infinito, correspondiente a la cantidad de números reales, a veces llamado el *continuo*, que es más grande que el anterior. Ya los hindúes distinguían entre estos dos tipos de infinito ¡hace más de dos mil años!

- ¡Qué interesante! ¿Cuándo veremos el infinito de los números reales?

- La semana que viene, Clara. Mientras tanto, podés tratar de resolver los siguientes problemas. ¡Adiós!

Para resolver

Problemas. Ayudar a Clara a resolver los siguientes problemas.

Problema 3.9. Probar que el producto cartesiano de dos conjuntos numerables es numerable.

[Nota: dados dos conjuntos A y B se define el producto cartesiano $A \times B$ como el conjunto de los pares ordenados (a, b), donde a pertenece a A y b pertenece a B. En símbolos: $A \times B = \{(a,b) : a \in A \ y \ b \in B\}$.]

[Ayuda: escribir una numeración de A y otra de B y hacer un cuadro como el que se hizo para $\mathbf{Q}^+$.]

Problemas más avanzados.

Problema 3.10. Si se hace el producto de 3 conjuntos numerables, ¿es numerable también? [Ayuda: $A \times B \times C = \{(a,b,c) : a \in A, b \in B, c \in C\}$ se puede pensar también como $(A \times B) \times C$.]

Problema 3.11. Mostrar que el *producto finito de numerables es numerable*. Es decir, mostrar que el producto cartesiano de una cantidad finita de conjuntos numerables es un conjunto numerable.

Problema 3.12. Demostrar que el conjunto de los polinomios de grado 2 con coeficientes enteros es numerable.

[Ayuda: estos polinomios son de la forma $a \,.\, x^2 + b \,.\, x + c$, donde a, b y c son enteros, $a \neq 0$. De modo que están totalmente determinados por los valores de a, b y c.]

Problema 3.13. Demostrar que el conjunto de todos los polinomios con coeficientes enteros son numerables.

[Ayuda: este conjunto consta de los polinomios de grado 0, 1, 2, 3, 4,… por lo tanto es la unión de conjuntos como el del problema anterior, que es numerable.]

Problema 3.14. Demostrar que el conjunto de los números algebraicos, **A**, es numerable.

[Nota: los números algebraicos son las raíces de polinomios con coeficientes enteros. Contienen a los números racionales, es decir $\mathbf{A} \supset \mathbf{Q}$, pues todo racional $\frac{m}{n}$ es raíz del polinomio de primer grado $n \,.\, x - m$ en la variable x. Además, por ejemplo, $\sqrt{2}$, que no es racional, también es un número algebraico, pues es raíz de $x^2 - 2$, que es un polinomio de segundo grado con coeficientes enteros.]

[Ayuda: se sabe que un polinomio de grado n, con $n \in \mathbb{N}$, tiene a lo sumo n raíces. Probar primero que los números algebraicos que son raíces de polinomios de grado n, con n fijo, son numerables. Luego notar que el conjunto de los números algebraicos es la unión, variando n, de los algebraicos que son raíces de un polinomio de grado n.]

3.7. ¡Los números reales no son numerables!

- Clara, hoy es un día importante, veremos que hay más de un tipo de infinito en esta teoría de cardinalidad que estamos considerando. Demostraremos que los números reales no son numerables. Primero, con un argumento que involucra longitudes de intervalos. Más adelante, con otras dos maneras de demostrar el mismo hecho, que los reales no son numerables, y entonces vas a poder elegir cuál es la que más te gusta.

- Me conformaría con entender una, Maestro.

- Bien. En esta primera demostración, además de los intervalos, necesitaremos usar el argumento llamado "reducción al absurdo", que consiste en suponer que la afirmación que se quiere demostrar es falsa, y a partir de ahí llegar mediante razonamientos válidos a algo absurdo, a una contradicción. Entonces la afirmación no podía ser falsa, y por lo tanto se concluye que la afirmación debe ser verdadera. ¿Lo entendés?

- Más o menos.

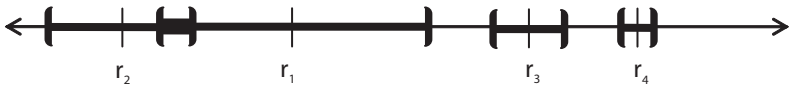
- Clara, cuando lo usemos en ejemplos concretos, lo aprenderás en seguida. Hay un punto muy sutil al final del razonamiento que generalmente pasa inadvertido. En ese último paso del razonamiento se está usando el llamado *principio del tercero excluido*, que dice que entre una afirmación y su negación una de las dos debe ser verdadera. Si bien casi todos aceptan este principio, algunas personas lo cuestionan. Nosotros vamos a aceptarlo, porque es lo más razonable, y además, nos permite avanzar mucho. Pero te repito que podés olvidarte de todo esto, porque si bien suena complicado en abstracto, será sencillo usarlo.

- Espero que sí. ¡Sigamos!

- Bien. Supongamos que los números reales son numerables. O sea, que hay una enumeración r_1, r_2, r_3, r_4, r_5, ... de los mismos. En ella aparecen todos los números reales sin repetirse. Entonces, le asociamos alrededor de cada número r_j un pequeño intervalo en la recta real, moviéndonos a partir de r_j un espacio de longitud $\frac{1}{2^j}$ hacia la izquierda y lo mismo hacia la derecha. O sea, estamos tomando el intervalo de los números reales x que satisfacen $r_j - \frac{1}{2^j} < x < r_j + \frac{1}{2^j}$, es decir, el intervalo de la forma $\left(r_j - \frac{1}{2^j}, r_j + \frac{1}{2^j}\right)$, para cada $j = 1, 2, 3, 4, 5, \ldots$. La longitud de cada pequeño intervalo es el doble de $\frac{1}{2^j}$, o sea $2 \cdot \frac{1}{2^j} = \frac{1}{2^{j-1}}$. Fijate que, de acuerdo a nuestra suposición inicial, todo número real pertenece por lo menos a uno de estos intervalos, puesto que todo número real es un r_j para algún j, y obviamente r_j pertenece al intervalo $\left(r_j - \frac{1}{2^j}, r_j + \frac{1}{2^j}\right)$. Por consiguiente, toda la recta real está contenida en la unión de estos pequeños intervalos. ¿Estás de acuerdo?

- Sí, pero tengo dudas sobre cómo es la unión de los intervalos.

- Es simplemente la unión de ellos como conjuntos. Podés unir tantos intervalos como quieras. En este caso hay una cantidad numerable de intervalos a unir, y su unión da toda la recta real. En símbolos lo podríamos expresar así: $R = \bigcup_{j \in N} \left(r_j - \frac{1}{2^j}, r_j + \frac{1}{2^j}\right)$, donde el símbolo $\bigcup$ significa unión, y debajo de él, $j \in \mathbf{N}$, significa que j varía tomando todos los valores de los números naturales. Por otra parte, la longitud de la unión de dos intervalos cualesquiera, es menor o igual que la suma de las longitudes de cada uno de ellos. Por ejemplo, en este dibujo



ocurre que la longitud de la unión de los intervalos alrededor de r_1 y de r_2 es estrictamente menor que la suma de las longitudes de dichos intervalos, mientras que la longitud de la unión de los intervalos alrededor de r_3 y r_4 es igual a la suma de las longitudes de estos intervalos. En símbolos:

$$\text{long}\left(\left(r_1 - \frac{1}{2}, r_1 + \frac{1}{2}\right) \cup \left(r_2 - \frac{1}{2^2}, r_2 + \frac{1}{2^2}\right)\right) < \text{long}\left(r_1 - \frac{1}{2}, r_1 + \frac{1}{2}\right) + \text{long}\left(r_2 - \frac{1}{2^2}, r_2 + \frac{1}{2^2}\right)$$

De este modo, la longitud de la unión de todos los intervalos es menor o igual que la suma de todas las longitudes, o sea, que la suma de los números $\frac{1}{2^{j-1}}$, para $j = 1, 2, 3, 4, \ldots$ ¿Sabés cuánto da esta suma?

- ¿Cómo es lo que hay que sumar?

- Simplemente $1+\frac{1}{2}+\frac{1}{2^2}+\frac{1}{2^3}+\frac{1}{2^4}+\frac{1}{2^5}+\cdots$

- ¡Ah! ¡Esto da 2! Lo vimos después de "Aquiles y la tortuga".

- Sí, claro. También vimos que era la serie geométrica de razón un medio. Lo importante es que da un número finito. Volviendo a los pequeños intervalos, estamos mostrando que la longitud de la unión de todos ellos no supera al 2. ¿No te parece que hay algo extraño?

- A ver… la suma da 2, pero al mismo tiempo estos intervalos cubren la recta de los números reales, ¿no? Entonces sí hay algo raro. ¡Muy raro!

- Por un lado, la longitud de la unión debería ser igual a la longitud de la recta real, que como sabés no es finita. Por otro lado, recién dijimos que la longitud de esta unión es menor o igual que 2. O sea que algo tan largo como la recta real nos ha dado menor que dos. Esto es un absurdo. ¡Una contradicción! Escribámoslo en símbolos, así no nos quedan dudas. Te recuerdo que el símbolo Σ significa suma o sumatoria:

$$\text{long}\,(\mathbf{R}) = \text{long} \bigcup_{j\in N}\left(r_j - \frac{1}{2^j}, r_j + \frac{1}{2^j}\right) \qquad (1)$$

pero

$$\text{long} \bigcup_{j\in N}\left(r_j - \frac{1}{2^j}, r_j + \frac{1}{2^j}\right) \le \sum_{j\in N} \text{long}\left(r_j - \frac{1}{2^j}, r_j + \frac{1}{2^j}\right)$$

$$\sum_{j\in N} \text{long}\left(r_j - \frac{1}{2^j}, r_j + \frac{1}{2^j}\right) = \sum_{j\in N} \frac{1}{2^{j-1}}$$

$$= 1+\frac{1}{2}+\frac{1}{2^2}+\frac{1}{2^3}+\frac{1}{2^4}+\frac{1}{2^5}+\cdots$$

$$= 2$$

por lo tanto

$$\text{long} \bigcup_{j\in N}\left(r_j - \frac{1}{2^j}, r_j + \frac{1}{2^j}\right) \le 2 \qquad (2)$$

De (1) y (2) resulta long (**R**) <= 2. Esto es absurdo, puesto que la longitud de **R**, la recta real, es mayor que dos. ¿Estás de acuerdo, Clara?

- Sí, claro, pero… ¿por qué pasa esto, Maestro?

- Esta contradicción se produjo, justamente, por haber supuesto que los números reales eran numerables. Por lo tanto, ¡los reales no pueden ser numerables! De modo que estamos frente a un nuevo tipo de infinito, mayor al infinito de los números naturales, o sea mayor al infinito de los conjuntos numerables. ¿Qué te parece?

- Me gusta. Creo que entendí lo del "ab-sur-do". ¡Estoy contenta por aprender esto!

- Bien. Ahora, sabemos que **N** y **R** son ambos infinitos pero no son coordinables, es decir que card **N** < card **R**. Esto nos invita a hacer nuevas preguntas, nos abre el universo de "los infinitos".

- ¿Hay otros infinitos?

- Hablaremos de eso en otra clase, Clara. Hoy, para terminar, te contaré sobre la pregunta o el problema más famoso en este tema, llamado la *hipótesis del continuo*[2]. Sabemos que card **N** < card **R**, ¿verdad? Entonces naturalmente surge la inquietud: ¿Existirá algún conjunto cuyo cardinal esté entre medio de estos dos? ¿La entendés?

- Creo que sí.

- Hemos visto, por ejemplo, que el conjunto de los números racionales **Q** está "entre" **N** y **R** y tiene el mismo cardinal que **N**. Si empezás a pensar en conjuntos candidatos a contestar afirmativamente la pregunta, pronto verás que todos tienen cardinal igual al de **Q** o al de **R**, pero nunca entre medio de los dos. Veamos otro ejemplo, el conjunto de los números algebraicos, **A**, ¿cómo era su cardinal?

- Vimos que era el mismo que el de **N**.

- Bien, y eso que a primera vista **A** parece ser un conjunto muy grande, y cuesta encontrar números reales que no sean algebraicos. En los problemas, tendrás que demostrar que el conjunto de los números irracionales tiene el mismo cardinal que el de **R**. La *hipótesis del continuo*, Clara, afirma que no puede existir un conjunto cuyo cardinal esté entre el de **N** y el de **R**. Cantor -el creador de la teoría de cardinales que estamos estudiando- intentó demostrarla durante mucho tiempo, pero no lo consiguió. Nadie lo ha logrado, ni tampoco se ha podido mostrar lo contrario.

- Debe ser entonces un problema muy difícil.

- Sí. Es más difícil de lo que se pensó originalmente, *demasiado* difícil -el Maestro enfatizó la palabra demasiado, lo que hizo pensar a Clara que se trataba realmente de algo excepcional-. Es tan difícil que…

Hipótesis del continuo: no existe un conjunto Y cuyo cardinal esté estrictamente entre el de **N** y el de **R**, es decir, que cumpla que card **N** < card Y < card **R**.

Y se hizo un silencio por unos segundos, que a Clara le pareció larguísimo, luego el Maestro dijo:
- ¡Es una pregunta imposible de contestar!

- ¿Cómo? ¿En serio? ¿Por qué?

- Se debe a ciertos resultados muy profundos de la lógica matemática. Kurt Gödel demostró, a mediados del siglo pasado, que siempre habrá afirmaciones *indecidibles*, es decir, que no podrán ser demostradas, ni refutadas, o equivalentemente, que no podremos decidir si son verdaderas o falsas. Tal vez esto nos deje con una sensación de vacío o inseguridad. Sin embargo, podemos asumir una de las dos opciones, que es verdadera, o que es falsa, y en ninguno de los dos casos encontraremos contradicciones. Luego Paul Cohen completó la demostración de que la "hipótesis del continuo" es una de estas "afirmaciones indecidibles".

- Me cuesta entenderlo, Maestro. Yo pensaba que, con tiempo, todas las afirmaciones podrían ser contestadas. ¿No es así?

---

[2] La **Hipótesis del Continuo** fue formulada en el siglo XIX por el célebre matemático alemán Georg F. L. Cantor, quien también fue el creador de la idea de cardinalidad de conjuntos que estamos siguiendo aquí. En el año 1900, Hilbert propuso éste como el primero en su famosa lista de 23 problemas.

- Te comprendo porque a mí me sucedía lo mismo. Uno tiende a pensar que todo enunciado es susceptible de ser verificado. Pero Gödel dejó boquiabiertos a todos con semejante conclusión. La hipótesis del continuo no es verdadera ni falsa. Notable, ¿no creés?

- Sí, seguro. Entonces Cantor estuvo trabajando muchísimo en algo que jamás iba a poder contestar.

- Así es. Hay que saber que la matemática, maravillosa como es, también puede dar grandes frustraciones, y no solamente por estos casos tan elevados.

- Y además de los cardinales de **N** y **R**, ¿hay otros infinitos?, ¿o eso tampoco se podrá saber nunca?

- ¡Claro que esto se puede saber! ¡Y se sabe! ¡Hay infinitos tipos distintos de infinito! Lo averiguaremos juntos dentro de un par de clases.

- ¡Qué bueno! ¡Hasta la semana que viene!

Clara se fue pensando en lo que había aprendido. Sentía que eran cosas importantes, porque finalmente el infinito comenzaba a retirar ese enorme velo que lo había cubierto durante tanto tiempo, para que ella pudiera admirarlo, y comprender algunos de sus aspectos. Ahora, ya sabía bien que había dos conjuntos infinitos cuyos infinitos eran esencialmente distintos. ¡Y esperaba seguir aprendiendo!

Para resolver

Problema 3.15. Demostrar que el conjunto **I** de los números irracionales no es numerable. [Nota: recordar que todo número real es racional o irracional, y no puede ser ambas cosas a la vez. Es decir, $\mathbf{R} = \mathbf{Q} \cup \mathbf{I}$, donde la unión es disjunta].

[Ayuda: razonar por el absurdo, es decir, suponer que **I** fuera numerable, y llegar a que entonces **R** sería numerable].

Problema 3.16. (Difícil). Demostrar que **I** es coordinable a **R**.

[Nota: esto es en realidad un caso particular de un Teorema que vale para cualquier conjunto infinito D no numerable al que le quitamos un subconjunto B numerable. Es decir, el teorema afima que: si $B \subset D$, siendo B infinito numerable y D infinito no numerable, entonces $D - B$ y D son coordinables].

[Ayuda. Realizar los siguientes pasos:
(i) considerar una numeración $b_1, b_2, b_3, b_4, b_5, \ldots$ de B;
(ii) considerar otro subconjunto numerable C de D disjunto de B, y una numeración $c_1, c_2, c_3, c_4, c_5, \ldots$ de C;
(iii) definir una correspondencia biunívoca entre C y $B \cup C$;
(iv) definir la correspondencia de $D - B$ a D mediante la siguiente regla: si el elemento de $D - B$ no está en C, entonces se le asigna el mismo elemento en D; y si está en C, se le asigna el elemento de $B \cup C$ de acuerdo a la correspondencia hallada en (iii);
(v) demostrar que la asignación definida en (iv) es una correspondencia biunívoca].

Problema 3.17. Los números reales que no son algebraicos son llamados números *trascendentes*,

de modo que **R** es la unión disjunta de los algebraicos y los trascendentes. Demostrar que los trascendentes son coordinables con los reales.

3.8. El método de la diagonal de Cantor

- Clara, ¿qué te pareció la demostración que hicimos de que los números reales no son numerables?

- Me costó al principio, pero después la entendí. ¡Me gustó!

- A mí también me gusta esa demostración. Es elemental, aunque tiene sus dificultades, porque asume que se pueden identificar totalmente los números reales con los puntos de una recta y aparecen conceptos geométricos, como longitudes de segmentos. Hoy abordaremos el mismo problema, aunque usando otros elementos, como la escritura decimal de los números reales y una idea muy ingeniosa, llamada el **método de la diagonal**. La propuso Cantor y mostró por primera vez que los conjuntos **N** y **R** tienen distintos cardinales. Es posible que te guste más que la demostración anterior.

- ¿Es como las diagonales que usamos para ver que **Q** era numerable?

- No. Ésta es otra diagonal. Es **la diagonal** - dijo el maestro con cierto orgullo por `presentarla'-. Pero es bueno que te acuerdes de las otras porque el cuadro es el mismo. Esta diagonal es una sola, la principal, que comienza en la esquina superior izquierda del cuadro, va hacia abajo a la derecha, y continúa indefinidamente. ¿Estás lista para comenzar?

- Sí, claro. Lo único que me preocupa es que no sé bien lo de la escritura decimal de los números reales que usted dijo que me va a hacer falta.

- No te preocupes. Veremos lo necesario para comprender esta demostración. Comencemos por la idea básica que es tan simple como ingeniosa. Hagamos un cuadro como los anteriores, aunque en principio lo haremos finito, digamos de 4×4. Ahora en lugar de completarlo con números racionales o con pares ordenados, como hicimos antes, lo llenamos con símbolos, sólo dos para comenzar: O y X. Es decir, cada lugar o entrada en el cuadro será O o X. Cuando un cuadro esté lleno, nuestra tarea será armar una nueva fila fuera del cuadro, que sea distinta a todas las filas del cuadro. El método de la diagonal nos provee una forma poderosa de hacerlo: se arma una fila que se distingue de la primera fila del cuadro en el primer elemento, de la segunda fila en el segundo elemento, de la tercera fila en el tercer elemento, y de la cuarta en el cuarto. Por ejemplo, en este cuadro 4×4, ¿podrías armar una nueva fila como dijimos?

O	X	X	X
X	X	O	O
O	O	O	X
X	O	X	O

- Creo que sí. Tengo que armar mi fila que empiece con X para que sea distinto de O, que es el primer elemento de la primera fila. Después, como en la segunda fila aparece X en el segundo lugar, tengo que poner O. Después pongo X, y al final de nuevo X. Queda así: X O X X. ¿Está bien?

- Muy bien. Ahora quiero que pienses por qué la fila que hiciste es distinta a las filas del cuadro. ¿Puede ser igual a la primera fila?

- ¡No!

- ¿Por qué?

- Porque mi fila empieza con X y la del cuadro con O.

- ¡Bien! ¿Y a la segunda fila del cuadro, puede ser igual?

- No, porque mi fila tiene O en el segundo lugar, y la del cuadro tiene X.

- Así es. En general, la fila armada mediante el método de la diagonal no puede ser igual a ninguna de las filas del cuadro, porque al compararla con la primera fila, sabemos que tienen el primer elemento distinto, al compararla con la segunda, tienen el segundo elemento distinto, y así sucesivamente. De modo que la fila que construiste es distinta a todas las anteriores. ¿Esto también valdría en un cuadro con infinitas filas y columnas en lugar de un cuadro 4×4 como el que dibujamos?

- A ver… sí, creo que sí, ¿por qué no?

- Sí, funciona de la misma manera. Sólo debemos seguir el mismo procedimiento. Ahora, si en lugar de tener únicamente los símbolos O y X tuviéramos más símbolos, por ejemplo, los dígitos decimales ¿funcionaría también? ¿Podrías construir una fila distinta de las demás?

- Sí, y hay más posibilidades para armar mi fila. Con dos símbolos tenía una sola posibilidad de armar la fila en la forma que usted quería.

- Muy bien. Este es el "método de la diagonal", Clara, ¡así de simple!

- ¿Y nos va a servir para algo tan importante?

- Sí, claro. A veces una combinación de ideas simples como ésta, puestas en el orden apropiado, logran grandes resultados Ahora, en lugar de completar los casilleros del cuadro infinito con los símbolos O y X los llenaremos con dígitos, o sea con los símbolos 0, 1, 2, 3, 4, 5, 6, 7, 8 y 9. Además, en lugar de mirar cada fila como una simple hilera infinita de dígitos, la identificaremos con un número real en el intervalo [**0,1**]. Si la fila es de la forma $a_1\ a_2\ a_3\ a_4\ a_5$ ... entonces se identificará con el número real $\alpha = 0, a_1\ a_2\ a_3\ a_4\ a_5$ ... Recíprocamente, si tenemos un número real α en el **[0,1]**, es decir, $0 \leq \alpha \leq 1$, entonces α tiene una expresión o desarrollo decimal de la forma $\alpha = 0, a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7$..., donde a_1, a_2, a_3, a_4, ... son dígitos y los podemos poner en una fila del cuadro, entonces la fila representará al número α. ¿Lo entendés?

- Creo que sí. ¿No importa que no aparezcan en el cuadro el cero y la coma que van al principio del número?

- Bueno, ellos no son necesarios cuando solo estamos hablando de números reales entre 0 y 1. Si sabemos que el número comienza siempre con un cero, la coma, y luego los dígitos, entonces podemos olvidarnos del cero y la coma y escribir solo los dígitos. Vale la pena mencionar que el desarrollo decimal se corresponde con una serie. El dígito a_j que uno ve en el lugar j después de la coma, corresponde a la fracción $\frac{a_j}{10^j}$, y se cumple que α es igual a la

suma infinita de las fracciones $\frac{a_j}{10^j}$, es decir $\alpha = \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \frac{a_4}{10^4} + \frac{a_5}{10^5} + \frac{a_6}{10^6} + \frac{a_7}{10^7} + \cdots$.
En un caso extremo, como sería tomar todos los dígitos iguales a 9, esta suma infinita sería la serie geométrica de razón $\frac{9}{10}$, que vimos y sabemos que suma 1. Es decir, se cumple que 0,999999...=1 ¿Te sorprende?

- Sí. Parece mentira que un número empiece con "cero coma" y termine dando uno. Aunque me estoy acostumbrando, Maestro, porque con aquella serie que sumaba 2 también pasaba lo mismo: siempre la suma finita estaba por debajo de 2, pero usted dijo -y me convenció- que daba 2.

- Bien. Pero entonces, ¡el uno tiene dos desarrollos decimales distintos!

- ¡Claro! No me había dado cuenta de eso. Creo que pensaba que cada número tenía una expresión decimal y no más.

- Hay números que admiten dos desarrollos decimales distintos. Otro ejemplo es el $\frac{1}{2}$, ¿cómo se escribe en notación decimal?

- Se escribe como 0,5. Sí. Sin embargo, también vale que $\frac{1}{2}$ = 0,49999999... con infinitos nueves.
Casi todos los números reales tienen un único desarrollo decimal y sólo algunos tienen dos. Nunca tienen más de dos. Además, los números que tienen dos desarrollos son aquellos con un desarrollo decimal finito que se corta, como por ejemplo 0,24 , y entonces el otro desarrollo es simplemente cambiar el último dígito no nulo por uno menos y poner infinitos nueves a continuación. ¿Te animás a dar el otro desarrollo decimal de 0,24?

- ¿Puede ser 0,2399999... ?

- Muy bien. De modo que los números que admiten dos desarrollos decimales distintos tienen infinitos nueves a partir de un momento, o infinitos ceros. Pero conviene que dejemos los desarrollos decimales para otra oportunidad, luego te dejaré un lindo problema para tu casa, que será pensar cuáles son los números reales que tienen desarrollo decimal que se corta.

- Lo haré, Maestro, me gustaría entender bien eso.

- Ahora, volvamos al cuadro, llenémoslo con una lista (infinita) de números reales α, β, γ, δ, ε, … , que tienen desarrollos decimales $\alpha = 0, a_1\, a_2\, a_3\, a_4\, a_5\, a_6\, a_7 \ldots$, $\beta = 0, b_1\, b_2\, b_3\, b_4\, b_5\, b_6\, b_7$, $\gamma = 0, c_1\, c_2\, c_3\, c_4\, c_5\, c_6\, c_7 \ldots$ y continúan indefinidamente.

De modo que nuestro cuadro infinito representa ahora una sucesión de números reales, cada uno de ellos en el intervalo **[0,1]**. ¿Se podrá elegir otro número real entre 0 y 1 distinto a todos los del cuadro? Esto, Clara, es parecido a lo que te pedí de armar una fila distinta a las del cuadro 4 × 4.

α	a_1	a_2	a_3	a_4	a_5	⋯
β	b_1	b_2	b_3	b_4	b_5	⋯
γ	c_1	c_2	c_3	c_4	c_5	⋯
δ	d_1	d_2	d_3	d_4	d_5	⋯
ε	e_1	e_2	e_3	e_4	e_5	⋯
⋮	⋮	⋮	⋮	⋮	⋮	⋱

- Con lo que vimos de la diagonal principal se puede elegir una fila distinta de todas estas, ¿verdad?

- Sí, se puede.

- Y el número real correspondiente a esa fila va a ser distinto a los demás, salvo que justo pase eso raro de los dos desarrollos distintos.

- Dejame que te ayude, Clara. Para armar nuestra fila infinita en cada paso podemos elegir un dígito que sea distinto al de la diagonal y también distinto de 0 y de 9, y así nos aseguramos que la fila construida representará un número distinto de los demás, sin importar lo de uno o dos desarrollos decimales. ¿Estás de acuerdo?

- Sí, aunque después lo voy a pensar de nuevo en mi casa.

- Sigamos con la idea de la demostración. En otras palabras, cada vez que alguien haga una lista $\alpha, \beta, \gamma, \delta, \varepsilon, \ldots$de números reales en el intervalo **[0,1]** nosotros seremos capaces de encontrar otro número real entre 0 y 1 que no está en dicha lista. En consecuencia, no se puede hacer una lista completa de los números reales del **[0,1]** o, equivalentemente, ¡el **[0,1]** no es numerable!

- ¡Qué bueno! Creo que esta demostración me gusta más que la anterior. Pero, todo el tiempo usamos el **[0,1]**. ¿Cuándo aparece **R**?

- Pensá y te vas a dar cuenta. Si no podés enumerar los números reales del intervalo **[0,1]**…

- ¡Claro! Me podría haber dado cuenta antes. El **[0,1]** está contenido en **R**, así que si no se pueden enumerar los elementos del conjunto más chico, entonces tampoco se pueden enumerar los del más grande.

- Muy bien. Eso es suficiente para completar la demostración de que **R** no es numerable por el método de la diagonal. Voy a agregar sólo una cosa más: para este fin, un intervalo de la recta real como el **[0,1]** y el conjunto **R** completo es como si fueran iguales porque veremos en uno de los problemas que son coordinables entre sí. ¡Adiós Clara!

- Adiós Maestro, hasta la semana que viene.

Para resolver

Problema 3.18. Si los símbolos permitidos son I, O y X, decidir cuál de estas tres filas ha sido obtenida aplicando el método de la diagonal (ver cuadro).

X	I	I	X	O
X	O	O	I	X
O	O	X	I	O
I	O	X	I	X
X	I	X	O	X

(i) O O X I O (ii) X X O O I (iii) O X I O I

Problema 3.19. (a) Hacer el desarrollo decimal de los siguientes números fraccionarios: $\frac{1}{3}$; $\frac{17}{20}$; $\frac{1}{7}$; $\frac{13}{4}$; $\frac{96}{25}$; $\frac{21}{12}$.
(b) Notar que si al descomponer el denominador los únicos números primos que aparecen son 2 y 5 entonces el desarrollo es finito. Por ejemplo: $\frac{17}{20}$ tiene denominador $20 = 2^2 \times 5$.
(c) En los otros casos el desarrollo es infinito. Cuando en el denominador aparece un factor primo distinto de 2 y 5 como 3, 7, 11, 13, 17, etc. y la fracción está escrita en forma irreducible (o sea, no se puede simplificar nada entre el numerador y el denominador).
(d) Concluir que los únicos números reales que admiten un desarrollo decimal finito son los fraccionarios cuyo denominador (ya escrito en forma irreducible) es de la forma $2^j \cdot 5^k$, con j y k enteros no negativos.

Problema 3.20. (i) Probar que los intervalos reales **(0,1)** y **(0,2)** son coordinables.

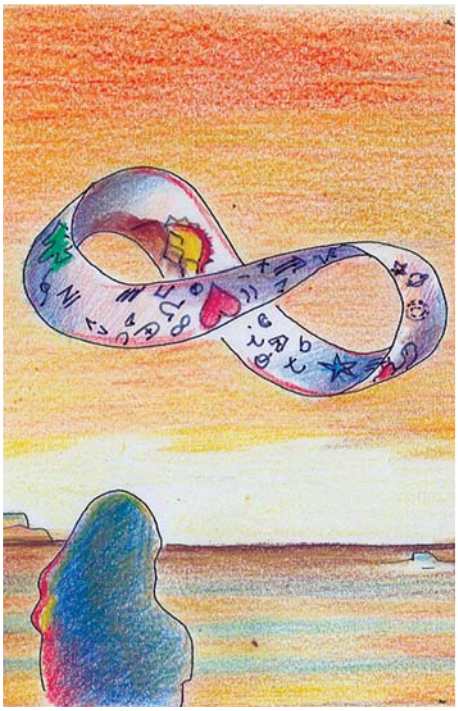
[Ayuda: considerar la correspondencia del **(0,1)** en el **(0,2)** que a cada x en **(0,1)** lo multiplica por dos, es decir $x \mapsto 2 \,.\, x$].

(ii) Probar que el **(0,1)** es coordinable al $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$.

[Ayuda: usar la correspondencia $x \longmapsto \pi \cdot x - \frac{\pi}{2}$].

(iii) Aceptar que hay correspondencias, como por ejemplo la función trigonométrica llamada **tangente**, que llevan el intervalo real $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ en el conjunto **R** en forma biunívoca. Concluir, que el **(0,1)** y **R** son coordinables.

□ 3.9. ¡Hay infinitos tipos de infinito!



- Clara, ¿sabés lo que significa **partes de *X***, cuando X es un conjunto cualquiera?

- No. ¿Debería saberlo?

- No, no deberías. Pero nos será de gran utilidad. Tenés que pensar en los subconjuntos de X, en todos ellos. Esto incluye al conjunto vacío y al mismo X, llamado el **conjunto total**. El conjunto de las partes de X, o dicho brevemente "**partes de *X***", es simplemente el conjunto formado por todos los subconjuntos de X. Hay que ser cuidadosos porque lo que eran conjuntos -los subconjuntos de X- ahora pasan a ser elementos de este nuevo conjunto. Por ejemplo: si X es el conjunto formado sólo por dos elementos, digamos p y q, es decir, $X = \{p, q\}$, ¿cómo será el conjunto "partes de X"?

- Bueno, tengo que pensar en todos los subconjuntos de X, así que $\{p\}$ es uno, y $\{q\}$ es otro. Estos tienen solamente un elemento cada uno.

- Bien. Te faltan.

- Sí. Usted dijo que el vacío y el mismo X debían estar, ¿verdad?

- Sí. La convención es ponerlos como subconjuntos de X. Con esos cuatro terminaste. Es decir que partes de X, denotado $P(X)$, es un conjunto con cuatro elementos en este caso que son los que mencionaste: $\{p\}$, $\{q\}$, el conjunto vacío, que se denota con el símbolo Ø, y X, el conjunto **total**. En símbolos podemos escribir:

$$P(\{p, q\}) = \{\emptyset, \{p\}, \{q\}, \{p, q\}\}$$

Definición. Dado un conjunto X, se llama **partes de X** al conjunto formado por todos los subconjuntos de X. En símbolos, $P(X) = \{A : A \subseteq X\}$

Si ahora X tuviera tres elementos, ¿cuántos tendría $P(X)$? Supongamos que: $X = \{p, q, r\}$

- Hay muchos ahora. Están $\{p\}$, $\{q\}$, $\{r\}$, $\{p, q\}$, $\{p, r\}$, $\{q, r\}$, $\{p, q, r\}$, además del vacío. Creo que no hay más.

- Muy bien. ¿Cuántos son entonces?

- Son 8, Maestro.

- Quiere decir que cuando el cardinal de X es 2, el de $P(X)$ es 4, y cuando el de X es 3, el de $P(X)$ es 8. ¿Qué pasa si X tiene n elementos? ¿Cuál será el cardinal de $P(X)$?

- A ver. Va creciendo muy rápido. No estoy segura.

- Pensá el caso en que X tiene 4 elementos, por favor.

- En ese caso, hay 4 subconjuntos con un solo elemento, hay 6 con dos elementos, hay 4 con tres elementos y 1 con cuatro elementos, que es el mismo X, y como siempre, el vacío. O sea que son $1 + 4 + 6 + 4 + 1 = 16$.

- Bien, voy a hacer un pequeño cambio en lo que escribiste. -el Maestro cambió el 16 por 2^4, y continuó- ¿Esto te dice algo? El cardinal de X era 4, y el de $P(X)$ resultó ser 2^4. Antes teníamos cardinales de $P(X)$ iguales a $4 = 2^2$ y $8 = 2^3$.

- Ah, claro. Parece que siempre da así. O sea, si X tiene n elementos, entonces $P(X)$ tiene 2^n. Estoy haciendo las cuentas con los siguientes números y dan bien.

- Así es. Esto se puede demostrar, por ejemplo, usando el principio de inducción, o si prefieres, la combinatoria que nos ofrece una demostración preciosa. Hagámosla para el caso $X = \{p, q, r\}$, pero vale en general. Cuando tomaste el subconjunto $\{p\}$, podemos pensar que asignaste un 1 a p, un 0 a q y un 0 a r. Cuando tomaste el subconjunto $\{p, q\}$, pensamos que asignaste un 1 a p, otro 1 a q, y un 0 a r. Es decir:

$$\{p\} \to (1,0,0)$$
$$\{p,q\} \to (1,1,0)$$

En general, dado un subconjunto se asignan **unos** a los elementos del subconjunto y **ceros** a los que no pertenecen al subconjunto. De este modo, los subconjuntos de X están en correspondencia biunívoca con las -en este caso- ternas de ceros y unos. Es decir:

$$P(X) \leftrightarrow \{\text{ternas de 0 y 1}\}$$

Es fácil contar cuántas ternas así hay: tenemos dos posibilidades, 0 ó 1, para el primer lugar en la terna; también dos posibilidades, 0 ó 1, para el segundo lugar; y lo mismo para el tercero. Estas posibilidades son independientes entre sí, es decir, tener 0 ó 1 en una posición, no afecta al número que aparezca en las otras posiciones. Por lo tanto, hay $2 \times 2 \times 2 = 2^3$ ternas distintas de ceros y unos. En general, si el cardinal de X es n, entonces habrá $\underbrace{2 \times 2 \times \cdots \times 2}_{n} = 2^n$ posibilidades de elegir 0 ó 1 en cada una de las n posiciones, y por lo tanto hay 2^n elementos en $P(X)$. ¿Lo entendiste, o fuimos demasiado rápido?

Clara contestó que lo había entendido, a pesar de la velocidad, mientras el Maestro escribía el siguiente recuadro en el pizarrón:

$$\text{card } P(X) = 2^{card\, X}$$

y continuaba diciendo:

- También se puede escribir así lo que dijimos. ¿De acuerdo?

- Sí. Es un poco abstracto así, pero no hay problema.

- Ahora, que ya sabés el significado de partes de un conjunto, vamos a considerar conjuntos infinitos. Cuando X es infinito, es obvio que $P(X)$ será también un conjunto infinito. Por ejemplo, siempre están los subconjuntos formados por un solo elemento de X, o sea los de la forma $\{x\}$, donde x pertenece a X. Así que, si X es infinito, $P(X)$ también. Además, si comparamos sus tamaños, vemos que X es como si estuviera dentro de $P(X)$, mediante los subconjuntos $\{x\}$. Naturalmente, nos podemos preguntar si $P(X)$ será esencialmente más grande que X, o si podrían llegar a ser coordinables. ¿Tenés alguna intuición sobre esto, Clara?

- En el caso finito vimos que el cardinal de $P(X)$ es igual a $2^{card\, x}$, o sea, mucho más grande que el de X. Pero en el caso infinito se complica, tal vez siga valiendo que card $P(X)$ > card X, pero la verdad es que no sé la respuesta.

- De acuerdo a lo que dijiste, estás muy cerca de adivinarla. El primer -y muy interesante- ejemplo que podemos pensar es cuando X es **N**. Veremos bien cómo es P (**N**) y su cardinal. Comencemos por hacer la observación de que a cada subconjunto S de **N** se lo puede identificar con una sucesión infinita de **ceros** y **unos**, al igual que como hicimos recién con los subconjuntos de X en el caso en que el cardinal de X era 3. Más precisamente, S en P (**N**) se identifica con una sucesión $t_1\, t_2\, t_3\, t_4\, t_5\, t_6\, t_7 \ldots$ donde cada t_k vale cero o uno para cada k, de acuerdo a la siguiente regla: t_k es 1 si el elemento k pertenece al subconjunto S, y t_k es 0 si k no pertenece a S. En símbolos:

$$S \leftrightarrow t_1, t_2, t_3, t_4, t_5, t_6, t_7, \ldots \quad \text{donde}$$
$$t_k = 1 \text{ si } k \in S, \text{ y } t_k = 0 \text{ si } k \notin S$$

Por ejemplo, si S es el subconjunto de los números pares, entonces la sucesión que le asociamos será la 0; 1; 0; 1; 0; 1; 1; 0..., si S es el subconjunto vacío, en la sucesión asociada son todos ceros; si S es el total, **N**, entonces la sucesión que le corresponde tiene todos unos; si S ={3, 4, 5, ...}, la sucesión es 0; 0; 1; 1; 1; 0; 0; 0; ...y siguen todos ceros. Ahora cada una de estas sucesiones de ceros y unos puede considerse como un número real entre cero y uno, ¿sabés cómo?

- Bueno, ¿podría ser como antes, o sea, asociarle el número 0, $t_1\, t_2\, t_3\, t_4\, t_5\, t_6\, t_7 \ldots$?

- ¡Por supuesto! Y ahora viene algo interesante, Clara. Estas sucesiones de ceros y unos, que parecen ser **algunos** de los números reales en el intervalo **[0,1]**, resultan ser **todos** estos números reales si consideramos la escritura en el **sistema binario**, donde los únicos

dos caracteres que aparecen son el 0 y el 1. Es decir, todo número real en el intervalo **[0,1]** puede escribirse -en escritura binaria- como una sucesión de la forma 0, $t_1\ t_2\ t_3\ t_4\ t_5\ t_6\ t_7$... donde los t_k son dígitos 0 ó 1. Este es el desarrollo decimal de un número escrito en el sistema binario. De este modo, dejando de lado algunos detalles -como las repeticiones de los números que admiten dos desarrollos decimales binarios distintos- se alcanza a ver que el conjunto de estas sucesiones de ceros y unos, y por lo tanto P (**N**), es coordinable al intervalo real **[0,1]**. ¿Me seguís?

- A ver, me gustaría repetir lo que dijo. Empezó con P (**N**), o lo mismo, los subconjuntos S de los naturales **N**. A cada uno de estos subconjuntos lo pensó como una sucesión infinita de ceros y unos. Después, a cada una de estas sucesiones la pensó como un número real mayor o igual que cero y menor o igual que uno. Al final, concluyó que partes de **N** y el **[0,1]** son coordinables. ¿Es así?

- ¡Sí! Sólo agrego que las identificaciones que hacemos son correspondencias biunívocas, por lo tanto los conjuntos en cuestión resultan ser coordinables. Y en el caso de las repeticiones, se puede proceder igual que en ocasiones anteriores para obtener la coordinabilidad. Sigamos. El **[0,1]** es a su vez coordinable a todo **R**. Por consiguiente, partes de **N** y el conjunto de los números reales son coordinables. Equivalentemente:

$$\text{card } P(\mathbf{N}) = \text{card } \mathbf{R}$$

Aquí tenemos el primer cálculo del cardinal de las partes de un conjunto infinito, y como ves, ha resultado ser más grande que el cardinal del conjunto.

- Claro, porque ya sabíamos que card **R** > card **N**, entonces ahora tenemos que card P (**N**) > card **N**.
¿Y qué va a pasar con los otros conjuntos, Maestro? Porque todavía no sabemos que esto valga para todos los conjuntos, ¿verdad?

- No, **todavía** no, pero ¡muy pronto sí! Demostremos que siempre ocurre que card P (X) > card X.

- No se me ocurre cómo pensar en esto, porque no sabemos qué conjunto es X. Qué difícil. ¿La demostración es parecida a alguna que ya hayamos visto?

- Es una demostración corta y el argumento muestra, por reducción al absurdo, que X nunca puede ser coordinable a P (X), con una idea como la de la diagonal de Cantor. A pesar de lo abstracto del tema, creo que no tendrás problema en entenderla. ¡Comencemos!

- Bueno, si se usa lo del absurdo, entonces creo que va a empezar diciendo "supongamos que X y P (X) son coordinables" –dijo Clara, adelantándose y sorprendiendo al Maestro.

- ¡Así es! Me alegro que estés comprendiendo cómo funcionan las pruebas por el absurdo. Se comienza negando lo que se quiere probar y se debe llegar a una contradicción. Supongamos, como dijiste, que X y P (X) son coordinables. Entonces, existe una correspondencia biunívoca Φ entre ambos conjuntos, es decir Φ asigna a cada $x \in X$, un elemento $\Phi(x) \in P(X)$, o lo que es lo mismo, $\Phi(x)$ es un subconjunto de X. Además, si $x \neq y$ entonces $\Phi(x) \neq \Phi(y)$. Por último, todo subconjunto de X debe ser igual a $\Phi(x)$ para algún x en X. Ahora viene la clave del asunto. Definimos el subconjunto C de X formado por los x en X tales que x no pertenece a $\Phi(x)$. En símbolos:

$$C = \{x \in X : x \notin \Phi(x)\}$$

- Disculpe, me cuesta entender bien cómo es C.

- Vamos a construir C como un subconjunto de X. Tomamos un elemento cualquiera x en X, y puesto que $\Phi(x)$ es un subconjunto de X podemos hacernos la siguiente pregunta: ¿Pertenece x a $\Phi(x)$? Si la respuesta es afirmativa, entonces incluimos este x en C, si es negativa lo dejamos fuera de C. Hacemos lo mismo con cada uno de los elementos x de X.

- Ahora sí lo entiendo.

- Bien. Ahora afirmamos que el conjunto C es distinto de todos los conjuntos $\Phi(x)$. Fijate que esto es como lo de la diagonal. Antes había muchas filas, y construíamos una distinta a todas. Ahora hay muchos subconjuntos de X, los $\Phi(x)$, y construimos uno distinto a todos ellos. Debemos probar que:

$$C \neq \Phi(x) \quad \text{para todo } x \text{ en } X$$

ésta es nuestra **afirmación**.

- ¿O sea que C no va a poder ser ninguno de los subconjuntos $\Phi(x)$?

- Exacto. Y esto muestra que Φ no puede ser una correspondencia biunívoca entre X y $P(X)$ porque ha dejado elementos de $P(X)$, como C, sin ninguno que le corresponda en X. ¿Estás de acuerdo?

- Sí. ¡Qué bueno! Pero todavía no terminó la demostración.

- No. Nos falta demostrar nuestra afirmación. Para ello, nuevamente usaremos el razonamiento por el absurdo. Tratá de hacerlo sola.

- Podría intentarlo, aunque, ¿no será demasiado complicado?

- Lo sabrás al final. Debes comenzar negando la afirmación. Si la misma dice que "C es distinto de todos los $\Phi(x)$", entonces ¿qué es lo contrario de esto?

- Que hay un $\Phi(x)$ que es igual a C.

- Bien. Llamemos y al elemento de X que satisface esta igualdad. Es decir, tenemos que:

$$\text{existe } \; y \in X \quad \text{tal que } \; \Phi(y) = C$$

Ahora, debemos buscar una contradicción, un absurdo. Piensa que hay dos casos distintos a considerar: (1) $y \in C$ o (2) $y \notin C$. Recuerda cómo definimos C.

- A ver… en el caso (1) $y \in C$. Entonces, la definición de C nos dice que $y \notin \Phi(y)$, pero también sabemos que $\Phi(y) = C$, entonces $y \notin C$.

Clara se quedó callada. El Maestro la auxilió diciendo:
- Estás en el caso (1) donde $y \in C$, pero llegaste a que $y \notin C$, eso es una contradicción, un absurdo. Ahora debes analizar el segundo caso.

- En el caso (2) tenemos que $y \notin C$ y la definición de C nos dice que no pasa que $y \notin \Phi(y)$, entonces lo que pasa es que $y \in \Phi(y)$.

- Ahora podés continuar como en el caso (1) -interrumpió el Maestro.

- Sí, porque sabemos que $\Phi(y) = C$, entonces $y \in C$, y habíamos empezado con $y \notin C$, esto es una contradicción, ¡un absurdo! -dijo Clara, riéndose al usar esta palabra.

- Muy bien. Recuerda que comenzamos negando la afirmación y llegamos a absurdos en los dos casos, por lo tanto, podemos concluir que la afirmación debe ser verdadera, que era lo que debíamos probar. De modo que hemos terminado la demostración de que no existe una correspondencia biunívoca entre X y $P(X)$. Por lo tanto, el cardinal de X es estrictamente menor que el de $P(X)$, que es lo que nos habíamos propuesto averiguar. ¿Qué te ha parecido?

- Estoy muy impresionada por los resultados. Me cuesta mucho pensar en X sin saber qué conjunto es, pero he tratado de imaginarme que era **N**, y así creo que más o menos lo he entendido. Déjeme que anote bien todo lo que hemos visto hasta ahora.
Luego de una pausa, el Maestro y Clara retomaron la conversación.

- Fijate que hemos demostrado que siempre se cumple que card $P(X)$ > card X, en particular, vale que card $P(\mathbf{N})$ > card **N**, y como también vimos hoy que card $P(\mathbf{N})$ = card **R** ¿qué podemos concluir?

- Que card **R** > card **N**, aunque ya lo sabíamos.

- Sí, pero podemos tomarlo como la tercera forma distinta de haber demostrado este hecho. ¿Te acordás que te había dicho que podrías elegir cuál te gustaba más? ¿Cuál de las tres preferís?

. si X es finito, card P (X) = $2^{\text{card X}}$;
. card P (**N**) = card **R**;
. card P (X) > card X, en particular, card P (**N**) > card **N** y por lo tanto card **R** > card **N**

- A ver…la primera fue con las longitudes de los pequeños intervalos alrededor de cada número real, la segunda fue la de la diagonal…, las dos me encantaron. Esta última me resulta más difícil, aunque no haya sido larga.

- Me alegro que te hayan gustado las dos primeras. Aunque la tercera es muy importante, por lo que veremos ahora.

- ¿Vamos a ver algo más?

- Sí, lo último, porque realmente vale la pena. Hasta ahora sólo hemos distinguido entre dos tipos de infinitos: uno es el cardinal de los conjuntos numerables, que se denota $\aleph_0$ y se lee **aleph cero**, y el otro es el cardinal del conjunto de los números reales, llamado **el continuo**. Dicho sea de paso, el símbolo del infinito es este: ∞. Recuerda que no debemos buscar conjuntos de cardinal entre estos dos porque la hipótesis del continuo dice que no hay, y es indecidible. La versión generalizada de la hipótesis del continuo dice que lo mismo ocurre si se toma cualquier conjunto X en lugar de **N**, es decir, que no hay conjuntos cuyo cardinal esté estrictamente entre el de X y el de $P(X)$. Pero podría haber conjuntos con cardinalidades cada vez más grandes. ¿Qué crees, Clara? Debes tener en cuenta que probamos que card $P(X)$ > card X, para cualquier conjunto X, o sea que para cualquier conjunto, por más grande que sea, sus partes forman un nuevo conjunto que tiene mayor cardinal.

Hipótesis del continuo generalizada: dado cualquier conjunto X, no existe un conjunto Y cuyo cardinal esté entre el de X y el de P (X), en símbolos:

no existe Y tal que card X < card Y < card P (X).

- Entonces hay muchísimos infinitos.

- ¿Qué significa “muchísimos”?

- ¡Que hay infinitos infinitos!

- ¡Bien! Podrías explicarlo.

- Creo que sí. Si empiezo con **N** tengo un primer tipo de infinito. Después $P(\mathbf{N})$ me da otro infinito, mayor que el primero. Después, puedo tomar partes del segundo conjunto, y según vimos, va a dar otro conjunto con cardinal mayor, sería un tercer tipo de infinito, ¿no?, y así sigo, pero no estoy segura que esté bien.

- Sí, está bien. Como dijiste, podemos armar una sucesión de conjuntos con cardinales cada vez más grandes. Solamente sabiendo que card $P(X)$ > card X, se deduce que los conjuntos:

$$\mathbf{N},\ P(\mathbf{N}),\ P(P(\mathbf{N})),\ P(P(P(\mathbf{N}))),\ P(P(P(P(\mathbf{N})))),\ \ldots$$

satisfacen que:

$$\text{card } \mathbf{N} < \text{card } (P(\mathbf{N})) < \text{card } (P(P(\mathbf{N}))) < \text{card } (P(P(P(\mathbf{N})))) < \ldots$$

De modo que, en efecto, hay infinitos tipos distintos de infinito. De hecho, no era necesario poner el conjunto **N** para tomar sus partes, sino que esto mismo funciona con cualquier conjunto X.

- Maestro, se ve muy linda la última línea con todos esos cardinales distintos.

- ¡Qué suerte que te gusta!

Éste era el último día de las clases sobre el infinito. Ya casi despidiéndose dijeron:

- ¿Valió la pena el esfuerzo, Clara?

- ¡Sin dudas! Usted tenía razón: no me ha contestado qué es el infinito, pero lo que me ha enseñado es muy interesante. ¡Estoy muy contenta!

- Cuando algo es tan difícil y misterioso como el infinito, yo valoro cada paso que se pueda dar hacia su comprensión. Los nuestros han sido pasos pequeños, quizás ínfimos, pero al menos nos han dicho algo sobre el infinito, y algo lindo y bien construido.

- Una última pregunta, Maestro, que me intriga. En la realidad, ¿existe el infinito?

Se produjo un largo silencio. El Maestro mostró evidentes signos de estar en aprietos. Quizá estuviera dudando entre contar a Clara sus pensamientos al respecto, o dejar que ella se formara los suyos propios, sin su influencia; o quizá no sabía la respuesta.

Entonces dijo:

- Es demasiado difícil para mí, Clara, contestar a tu pregunta. Confío que podrás responderla sola algún día.

Problema 3.21. Se definen las **partes finitas** de un conjunto cualquiera X como el con-

Para resolver

junto formado por todos los subconjuntos finitos de X. En símbolos:
Si X es finito, entonces "partes finitas de X" coincide con "partes de X". Pero si X es infinito,

$$P_f(X) = \{A \subseteq X : A \text{ es finito}\}$$

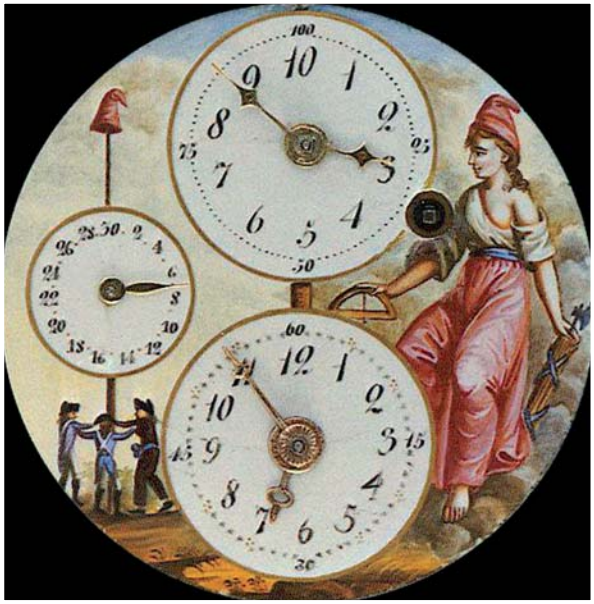
estos dos conjuntos pueden ser muy distintos. Por ejemplo, si $X = \mathbf{N}$, vimos que $P(\mathbf{N})$ es coordinable con $\mathbf{R}$. Demostrar ahora que $P_f(\mathbf{N})$ es coordinable a $\mathbf{N}$, o sea, es numerable.

[Ayuda. Considerar los subconjuntos de $\mathbf{N}$ de un elemento, luego los de dos, luego los de tres, etc., y recordar que la unión numerable de conjuntos numerables es un conjunto numerable].

La aritmética de los relojes

4.

Por Paulo Tirao



4.1. Introducción

El médico:

Ahora son las 10 de la mañana. Tome la próxima pastilla a las 2 de la tarde, y luego una cada 8 horas.

El paciente:

OK. Entonces tomo la próxima a las 2 de la tarde, luego a las …. 2 más 8 … eso es a las 10 de la noche, otra a las 10 más 8 … a las 6 de la mañana, después a las 6 más 8 … 14, ¡ah! de nuevo a las 2 de la tarde. Entonces sigo así: a las 2 de la tarde, a las 10 de la noche y a las 6 de la mañana. Muchas gracias (ver **figura 4.1**). Hasta luego.

¡Qué manera de sumar! ¿Así que 10 + 8 = 6? ¡Qué bonito! Bueno…. Sí, en la aritmética del reloj sí.

No es difícil encontrar otras situaciones donde esta aritmética: la aritmética del reloj, cíclica o modular, aparece naturalmente.

El médico:

Bueno, hoy es martes. A ver…, vuelva entonces en 10 días.

El paciente:

Muy bien. No hay problema. Hoy es martes, en 10 días será…, perfecto viernes. Estaré desocupado. Muchas gracias.

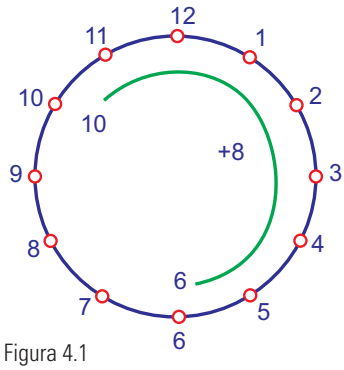


Figura 4.1

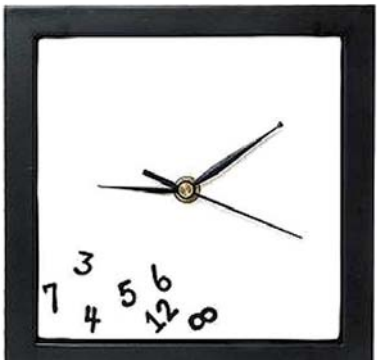
¡Qué manera de sumar! Así que martes +10 = viernes. ¡Qué bonito! Bueno…. Sí, en la aritmética de la semana sí.

Si le ponemos números a los días de la semana, empezando con domingo = 0, lunes = 1, martes = 2, etc., resulta que martes + 10 = 2 + 10, que ya sabemos da viernes = 5. Es decir, en la aritmética de la semana 2 + 10 = 5.

A esta altura también podemos contestar correctamente cuánto es 2 + 10 en la aritmética del reloj, y cuánto es 10 + 8 en la aritmética de la semana.

Recopilando

En la aritmética del reloj	**10 + 8 = 6**	**2 + 10 = 0.**
En la aritmética de la semana	**10 + 8 = 4**	**2 + 10 = 5.**



El resultado cambia cuando pasamos de la aritmética del reloj, que tiene 12 horas, a la aritmética de la semana, que tiene 7 días. De hecho, podemos ubicar los días de la semana como las horas de un reloj de 7 horas. Dispuestos así, vemos que la aritmética de la semana y la de este reloj de 7 horas, son muy parecidas.

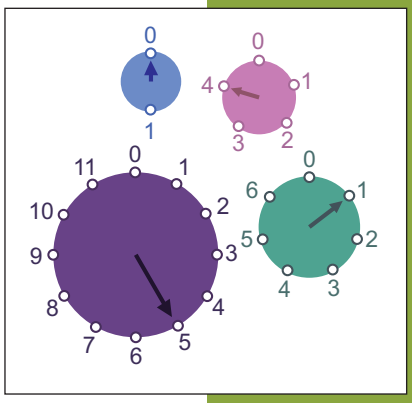
Como veremos más adelante esta **aritmética cíclica o modular** aparece como herramienta útil en situaciones en las que, quizá, no lo sospechábamos. Sin embargo, esto no sorprende demasiado a un matemático. En efecto, una vez que comprendemos una situación dada, entendemos su estructura y sus leyes, entonces podemos crear una teoría que cobra vida propia. Es frecuente, que no sólo sirva para explicar el fenómeno original que le dio vida, sino que encuentre utilidad en muchas otras situaciones preexistentes, o en situaciones y modelos creados basados en esta teoría.

En este capítulo nos familiarizaremos con estas aritméticas hasta ser capaces de hacer cuentas como sumas, restas y multiplicaciones, de la misma manera que lo hacemos en la aritmética tradicional. Daremos un marco formal y riguroso con ideas matemáticas sencillas, pero fundamentales. Marco que permite que esas ideas se puedan extender y generalizar a otras aritméticas dentro de la matemática.

Más adelante, veremos aplicaciones más sofisticadas como las reglas de divisibilidad.

También incluiremos una sección dedicada a la teoría de códigos. Desde muy temprano en la historia, la aritmética modular estuvo ligada a la construcción de códigos para el envío de mensajes secretos. Se le atribuye a Julio César el invento de uno de los primeros códigos que usaron los ejércitos romanos por largo tiempo de forma efectiva y exitosa. Estos códigos se basan en la aritmética modular.

4.2. La aritmética del reloj



Todos tenemos alguna experiencia en hacer cuentas con horas o con los días de la semana. Por esto exponemos directamente el tema y en la próxima sección veremos los aspectos formales y más rigurosos.

La aritmética del reloj de 12 horas

Comencemos repasando la aritmética del reloj usual. Supongamos que queremos sumar 9 más 7. Empezamos sumando "normalmente". Si

9 =
7 =

Entonces, 9 + 7 =

Ahora, para ver el resultado en el reloj enroscamos esa recta, y vemos que el resultado es 9+7=4 (ver **figura 4.2**).

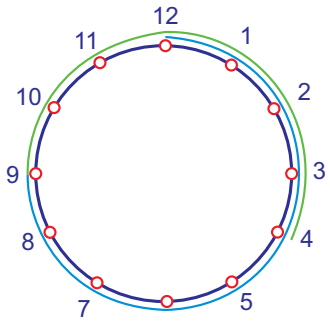


Figura 4.2

Regla. Para sumar dos horas primero se suman normalmente y si este número es más grande que 12, el resultado final es sólo lo que se pasa de 12.

Es decir, se suman las dos horas normalmente, y luego si es necesario se resta una vez 12.

Ejemplos

$2 + 8 = 10$ $\quad 3 + 11 = 2$ $\quad 5 + 7 = 0$ $\quad 3 + 8 = 11$ $\quad 9 + 11 = 8$

Para evitar confusiones, acordamos que las 12 horas son: **0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10** y **11**, es decir usaremos la hora 0 y no la hora 12.

Antes de continuar, introducimos una nueva notación para indicar que estamos usando la aritmética del reloj, u otra tan rara como ésta, y así evitar lo extraño que resulta por ejemplo la igualdad **9 + 7 = 4**.

Notación. Usaremos el símbolo $\equiv$ para denotar igualdad en esta aritmética. Así $\mathbf{9} + \mathbf{7} \equiv \mathbf{4}$ en la aritmética del reloj.

Intentemos sumar tres o más números en esta aritmética.

Ejemplos

$2 + 8 + 3 = (2 + 8) + 3 \equiv 10 + 3 \equiv 1$

$3 + 11 + 4 = (3 + 11) + 4 \equiv 2 + 4 \equiv 6$

$5 + 7 + 7 = (5 + 7) + 7 \equiv 0 + 7 \equiv 7$

La suma de varios sumandos se hace paso a paso, al igual que la suma usual de enteros. Esta suma de varios sumandos también se puede hacer así:

Regla. Para sumar varios números en la aritmética del reloj, se suman todos los sumandos normalmente, y si este número es más grande o igual que 12, se resta 12 la cantidad de veces necesaria hasta obtener un número entre 0 y 11.

Veamos cómo se resta. Para esto es útil pensar en el reloj y en la resta de horas. Por ejemplo, si ahora son las 4, ¿qué hora era hace 6 horas?

Ejemplos

$4 - 6 \equiv 10$ $9 - 5 \equiv 4$ $1 - 4 \equiv 9$ $7 - 6 \equiv 1$ $2 - 2 \equiv 0$

La resta se hace normalmente y, si es necesario, se suma 12 para obtener un número entre 0 y 11, y tener así una de las 12 horas posibles.

Volviendo al reloj, podemos decir que la suma se realiza en sentido horario y la resta en sentido antihorario. Si nos abstraemos del reloj, tanto la suma como la resta se hacen de la misma forma.

Regla. La suma y resta de varios sumandos en la aritmética del reloj se hace normalmente, y luego se suman o restan múltiplos de 12 hasta obtener un número entre 0 y 11.

Ejemplos

$6 + 9 - 3 \equiv 0$ $4 - 11 + 2 - 1 \equiv 6$ $10 + 8 - 7 + 5 \equiv 4$ $4 + 11 - 3 - 9 \equiv 3$ $1-10+1-3 \equiv 1$

Hasta aquí un primer acercamiento a la aritmética del reloj. Ahora, podríamos preguntarnos: ¿qué pasaría en un reloj de 8 horas? ¿Y en uno de 10 horas? Por suerte, nada raro.

La aritmética de otros relojes y la aritmética de la semana

El hecho de que hayamos comenzado con un reloj de 12 horas no es determinante, porque podríamos haber desarrollado una aritmética similar en cualquier otro reloj. No sólo en uno que marque las 24 horas, sino también en relojes que no existen como tales, como por ejemplo uno de 9 horas u otro de 17 horas.

Ejemplos

En la aritmética de un reloj de 9 horas

$6 + 8 \equiv 5$ $4 + 11 + 2 \equiv 8$ $3 + 4 - 5 \equiv 2$ $4 - 7 \equiv 6$ $8 + 4 - 6 \equiv 6$

Ejemplos

En la aritmética de un reloj de 17 horas

$6 + 8 \equiv 14$ $4 + 11 + 2 \equiv 0$ $3 + 4 - 5 \equiv 2$ $4 - 7 \equiv 14$ $8 + 4 - 6 \equiv 6$

En ambos ejemplos usamos el signo $\equiv$ para denotar igualdad en estas dos aritméticas distintas como lo habíamos usado en la aritmética del reloj de 12 horas. En todos estos casos estaba claro de cuántas horas eran los respectivos relojes, por eso el uso del mismo símbolo no causa ninguna confusión. Si el contexto no es claro usaremos una notación más completa.

Notación. Para decir que "**6** + **8** es igual a **5** en la aritmética de un reloj de 9 horas", diremos "**6** + **8** es congruente a **5** módulo **9**". Y escribiremos "**6** + **8** ≡ **5 mod** (**9**)".

Otro ejemplo conocido, es el de la ***aritmética de la semana***. En esta aritmética sabemos sumar martes + 2 días, domingo + 3, y sabemos restar miércoles – 1. En efecto, sabemos hacer esto porque esta aritmética es la misma que la aritmética de un reloj de 7 horas. Basta convenir en cómo ordenar los días de la semana en un reloj de 7 horas. Convengamos entonces en poner: domingo = 0, lunes = 1, martes = 2, miércoles = 3, jueves = 4, viernes = 5 y sábado = 6.

Entonces:

Martes + 5 días = 2 + 5 ≡ 0 mod (7). Entonces, si hoy es martes en cinco días será 0 = domingo.

Martes + 11 días = 2 + 11 ≡ 6 mod (7). En once días será **6** = sábado.

Para resolver

4.1 Hacer las siguientes sumas y restas: **4** + **3** - **2 mod** (**6**) **10** + **9** – **4 mod** (**11**)

4.2 Calcular **10** + **6** – **3** + **11** en las aritméticas módulo **12**, **15**, **18** y **22**.

4.3 Sumar **10** + **10** + **10** +….., diez veces en la aritmética módulo **11**, **12** y **20**.

4.4 Calcular **1** + **2** + **3** +…+ **98** + **99** + **100 mod** (**2**). Ayuda: en la aritmética módulo **2** hay sólo dos números **0** y **1**.

4.5 Calcular **3** + **3** +…+ **3 mod** (**9**). Ayuda: el resultado depende de la cantidad de sumandos. Más aún hay sólo tres respuestas posibles.

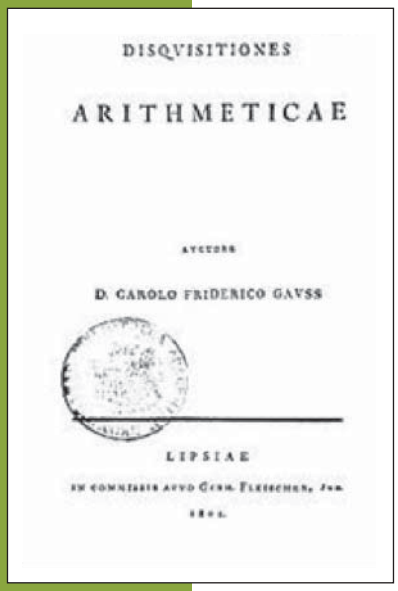
4.6. Demostrar que si *m* es impar, entonces **1** + **2** + **3** +…+ (*m* – **1**) + *m* ≡ **0 mod** (***m***)

□ 4.3. Los enteros módulo *m*

En esta sección presentaremos la construcción formal de la aritmética modular, que es el marco adecuado para describir el contenido de la sección anterior. Este marco también permite ampliar nuestras capacidades para definir otras operaciones, por ejemplo: la multiplicación modular.

Karl Friederich Gauss, el príncipe de las matemáticas, concibió y desarrolló sistemáticamente estos conceptos. Una de sus obras maestras, *Disquisiciones Arithmeticae* está dividida en siete secciones, de las cuales varias están dedicadas o relacionadas con la aritmética modular.

I. Números congruentes en general.
II. Congruencias de primer grado.


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

III. Residuos de potencias.
IV. Congruencias de segundo grado.
V. Formas y ecuaciones indeterminadas de segundo grado.
VI. Varias aplicaciones de las discusiones precedentes.
VII. Ecuaciones definiendo secciones de un círculo.

Múltiplos y divisores

Tomemos para empezar el número **5.** Los múltiplos enteros de **5** son: **5, 10, 15, 20, 25, 30, 35, ...** el **0** y también **–5, –10, – 15, –20, –25, –30, –35, …**

Los primeros, resultan de multiplicar **5** por **1, 2, 3, 4, 5, 6, 7,** etc; el **0** es múltiplo de **5** porque **5 . 0 = 0,** y los últimos se obtienen multiplicando **5** por **–1, –2, –3, –4, –5, –6, –7,** etc. Recordamos que el conjunto de los números enteros es:

$$Z = \{\cdots -4, -3, -2, -1, 0, \cdots 1, 2, 3, 4, \cdots\}$$

Formalmente, el conjunto de todos los múltiplo de **5** es:

$$I_5 = \{k.5 : k \in Z\}$$

El conjunto de todos los múltiplos de un entero ***m*** cualquiera es:

$$I_m = \{k.m : k \in Z\}$$

Observaciones

1) El conjunto de múltiplos de ***m*** y el conjunto de múltiplo de - ***m***, son iguales. Es decir, $I_m = I_{-m}$

2) El conjunto de múltiplos del **0** tiene un sólo elemento, el **0**. El conjunto de múltiplos del **1** es el de todos los enteros. Es decir, $I_0 = \{0\}$ y $I_1 = Z$.

3) Los conjuntos I_m, con ***m*** distinto de **0**, son todos *coordinables*, es decir tienen la misma cantidad de elementos. En efecto la función ***F*** de ***Z*** en los múltiplos de ***m*** que le asigna al entero ***k*** el múltiplo de ***m***, ***km*** es claramente una *biyección*. Es decir, es una asignación biunívoca que asigna a cada entero uno y sólo un múltiplo de ***m***, y tal que todo múltiplo es asignado a algún entero. Así podemos referirnos sin ambigüedad al tercer múltiplo de **21**, el **63**, o al séptimo múltiplo de **13**, el **91**.

4) Si dibujamos los múltiplos de distintos ***m*** en la recta, veremos que los dibujos resultan del mismo tipo. De hecho, si lo miráramos desde muy lejos diríamos que son iguales. La única excepción es el caso de los múltiplos del **0**.

Si graficamos los múltiplos de un número dado en la recta (**Figura 4.3**), cualquiera sea el número, el gráfico se ve así:

Figura 4.3

De la definición de múltiplos, se sigue que un entero r es múltiplo de otro m, si $r \in I_m$, es decir si existe un entero k tal que $r = k\,m$. Esta definición alternativa de múltiplo de un número nos permite definir de manera similar el concepto de divisor.

Definiciones. Un entero r es múltiplo de otro m, si existe un entero k tal que $r = k\,m$.
Un entero s es divisor de otro m, si existe un entero k tal que $m = k\,s$.

Notar que s es divisor de m exactamente cuando $m \in I_s$.

El conjunto de múltiplos de un entero fijo m tiene propiedades respecto de las operaciones de suma y producto de números enteros que hay que destacar. Cuando decimos suma consideramos también la resta como parte de la suma, ya que a menos b es lo mismo que a más $-b$.

Proposición. Sea m un entero fijo. entonces:

1. la suma de dos múltiplos de m, es un múltiplo de m,
2. el producto de un múltiplo de m por un entero cualquiera r, es un múltiplo de m.

Es decir, el conjunto I_m de múltiplos de m es cerrado para la suma (y la resta) y es absorbente para el producto, ya que basta que un factor esté en I_m para asegurar que el producto también esté.

Demostración. Tomemos dos múltiplos de m. Supongamos que estos son am y bm. Luego, su suma es $am + bm = (a + b)\,m$, que es también múltiplo de m. Además, el producto de uno de ellos am y un entero cualquiera c, es $(am)\,c = (ac)\,m$, que es múltiplo de m.

Los días de la semana

Volvamos a la aritmética de la semana. El siguiente dibujo representa un período de tiempo en el que cada punto es un día. Hemos pintado los domingos color rojo, los lunes de color azul y el resto de los días de la semana de un color distinto cada uno. Así todos los días quedan repartidos en siete subconjuntos, cada uno formado por los puntos de un mismo color (**Figura 4.4**) . Es decir, el primer subconjunto es el de los días domingos, el segundo el de los días lunes, etc.

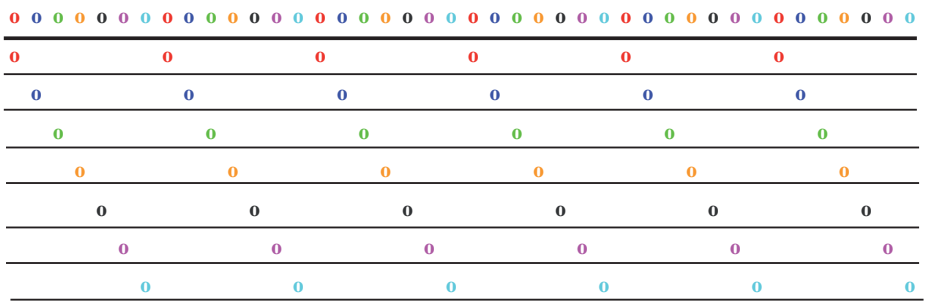


Figura 4.4

Si numeramos los días comenzando con domingo = 0, lunes = 1 y así hasta sábado = 6 entonces, este dibujo muestra una partición del conjunto de todos los enteros en siete subconjuntos. Desde el punto de vista de los múltiplos, los días domingo ó puntos rojos del dibujo son exactamente todos los múltiplos de 7; mientras que los días lunes ó puntos azules son todos múltiplos de 7 más 1. Los días lunes están en las posiciones 1, 8, 15, 22, 29, etc. Los días martes en verde son todos dos unidades más grandes que un múltiplo de 7, éstos son 2, 9, 16, 23, 30, etc. Recíprocamente, si estamos en una posición dada para determinar qué día de la semana corresponde basta medir cuánto se pasa de un múltiplo de 7. Si estamos en la posición 67 hacemos: $\mathbf{67 = 7 \cdot 9 + 4}$, y vemos que estamos en el día **4** de la semana, es decir en miércoles.

Conclusión. El resto de la división de m por **7**, determina el día de la semana (o el color) que le corresponde a m en este dibujo.

La división entera

Antes de seguir avanzando es necesario recordar qué es la división entera. Es aquella división con resto.

Teorema. Dado dos enteros m y n, n distinto de **0**, existen únicos enteros q y r, con $0 \leq r < |n|$ tales que $m = qn + r$. El entero q es el cociente de m dividido n y r es el resto.

Demostración: Si $m = 0$, ya está. Basta tomar $q = 0$ y $r = 0$ independientemente de n. Además, esta es la única elección posible. Supongamos ahora que tanto m como n son naturales, es decir mayores que **0**. En este caso, consideremos los múltiplos positivos de n : n, $2n$, $3n$, $4n$, … etc. y seleccionemos sólo los menores o iguales que m, supongamos que son n, $2n$, $3n$, …., qn. Entonces, $m - q\,n$ es mayor o igual que **0** y menor que n, de lo contrario el siguiente múltiplo de n, $(q + 1)\,n$, sería todavía menor o igual que m. Así, si tomamos $r = m - q\,n$ resulta lo que queremos: $m = q\,n + r$ en las condiciones requeridas (ver **figura 4.5**).

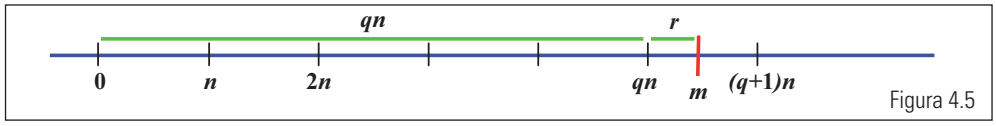


Figura 4.5

Ahora, si el divisor n es negativo, dividimos m por $-n$ que es positivo; así tendremos que $m = q\,(-n) + r$. Pero entonces tenemos que $m = (-q)\,n + r$, es decir el cociente es $-q$ y el resto el mismo r.

Si m es negativo, dividimos $-m$, que es positivo, por n que podemos suponer positivo; así tendremos $-m = q\,n + r$. De aquí resulta $m = -q\,n - r$, con $-r$ negativo; como $0 \leq r < n$ tenemos que $0 < n - r \leq n$.

Si $n - r < n$ ponemos $m = -q\,n - n + n - r = (-q - 1)\,n + (n - r)$ y vemos que ésta es la expresión deseada con $r' = n - r$. Si, en cambio, es $n - r = n$, es decir si $r = 0$, no hacemos nada y escribimos $m = -q\,n$.

Finalmente, veamos que q y r son únicos en las condiciones exigidas. Supongamos que $m = q\,n + r$ y que también $m = p\,n + s$, entonces tendremos $q\,n + r = p\,n + s$. Entonces, $q\,n - p\,n = s - r$, pero esto no es posible ya que $s - r$ es en valor absoluto menor que n, mientras que $q\,n - p\,n = (q - p)\,n$ es en valor absoluto siempre mayor que n, salvo que sea **0**. En este caso es $q = p$, y luego resulta $s = r$.

Observaciónes

En la división entera:

- el resto es siempre positivo o **0**;
- el cociente puede ser un entero negativo;
- no hay restricciones sobre el signo de ***m*** y ***n***. Es decir, podemos dividir un número positivo por uno negativo, uno negativo por uno positivo o uno negativo por otro negativo;
- ***n*** es múltiplo de ***m***, si y sólo si el resto de la división de ***n*** por ***m*** es **0**.

Dados dos enteros ***m*** y ***n*** cualesquiera (***n*** distinto de **0**), dividir ***m*** por ***n*** es encontrar los enteros ***q*** y ***r*** que da el Teorema. Como ambos son únicos, en las condiciones del Teorema, toda vez que se haga la división se obtendrá el mismo resultado. Esto que parece una trivialidad, es una trivialidad. Por lo tanto, cuando dos personas obtengan resultados distintos para una misma división, al menos uno ¡está equivocado!

Ejemplo

- La división de **13** por **3** es: **13** = **4** . **3** + **1**
- La división de **13** por – **3** es: **13** = (– **4**) .(– **3**) + **1**
- La división de – **13** por **3** es: – **13** = (– **5**). **3** + **2**
- La división de – **13** por – **3** es: – **13** = **5** .(– **3**) + **2**

Para resolver

4.7 Calcular: **3** dividido **13** ; – **3** dividido **13** ; **3** dividido – **13** ; – **3** dividido – **13**.

4.8 Supongamos ***n*** es un entero distinto de **0**. Calcular: **0** dividido ***n***; ***n*** dividido ***n***; – ***n*** dividido ***n***; ***n*** dividido – ***n***; – ***n*** dividido – ***n***. Notamos que – ***n*** es el opuesto de ***n***, que no necesariamente es negativo. El signo de – ***n*** es el opuesto que el de ***n***. Si ***n*** = – **13**, entonces – ***n*** = **13**.

4.9 Supongamos que ***n*** es un entero distinto de **0**. Calcular: ***n*** dividido **2*n***; – ***n*** dividido **2*n***; **2*n*** dividido ***n***; – **2*n*** dividido ***n***.

El máximo común divisor

Presentamos a continuación una definición formal de máximo común divisor y enunciamos algunas propiedades básicas que necesitaremos más adelante, y que quizá no resulten tan familiares.

Definición. Sean ***a*** y ***b*** enteros no nulos. El máximo común divisor de ***a*** y ***b*** es el mayor natural ***d*** que divide a ambos. Se denota ***d*** = (***a*** , ***b***).

Algunas observaciones y propiedades elementales sobre esta definición.

- El máximo común divisor es simétrico, es decir (***a, b***) = (***b, a***).
- Se puede tomar máximo común divisor de enteros positivos y negativos.
- El máximo común divisor de dos enteros es siempre mayor o igual que 1.
- (**1**, ***b***) = **1**, para todo entero ***b*** no nulo.
- (***a, b***) = (– ***a, b***)
  = (***a,*** – ***b***)

$= (-a, -b)$, para todo par de enteros a y b. Recordamos una vez más que $-a$ es el opuesto de a y, por lo tanto, no es necesariamente negativo; puede ser $a = -4$ y así $-a = 4$.

Ejemplos

Calculemos el máximo común divisor de **21** y $-$ **12**. Comenzamos listando los divisores positivos de cada uno de ellos.

Los divisores positivos de **21** son: **1**, **3**, 7 y **21**.
Los divisores positivos de $-$ **12** son: **1**, **2**, **3**, **4**, **6** y **12**.

Ahora, listamos los divisores positivos comunes; estos son: **1** y **3**. Por lo tanto, y de acuerdo a la definición, el máximo común divisor de **21** y $-$ **12** es (**21** , $-$ **12**) = **3**.

Proposición. Sean a y b enteros no nulos. Sea d un entero positivo que divide a ambos, tal que si d' es otro divisor común positivo de ambos, d' divide a d. Entonces d es el máximo común divisor de a y b.

Demostración. Por hipótesis, d es un divisor natural común. Más aún, como es divisible por cualquier otro divisor común positivo se sigue que es el mayor de éstos. Luego, d satisface la definición de máximo común divisor.
Continuamos con otro resultado que caracteriza al máximo común divisor de otra manera y que nos será útil más adelante.

Proposición. Sean a y b enteros no nulos. El máximo común divisor de a y b es el menor entero positivo que es combinación lineal entera de a y b. Es decir, el menor entero positivo que se puede escribir de la forma $d = ma + nb$ con m y n enteros.

Demostración. Veamos primero que d divide a a y divide a b, es decir que es un divisor común de a y b. Dividiendo a por d tenemos que $a = qd + r$ con r positivo y menor que d o igual a **0.** Dividiendo b por d tenemos que $b = pd + s$ con s positivo y menor que d o igual a **0**.

Supongamos que r es distinto de **0**, entonces $r = a - qd$ es positivo y menor que d, y además

$$\begin{aligned} r &= a - qd \\ &= a - q(ma + nb) \\ &= a - qma - qnb \\ &= (1 - qm)a - (qn)b \end{aligned}$$

Así, d no es el menor entero positivo que se escribe como combinación lineal entera de a y b. Luego $r = 0$ y d divide a a. Análogamente, se muestra que $s = 0$ y d divide a b.

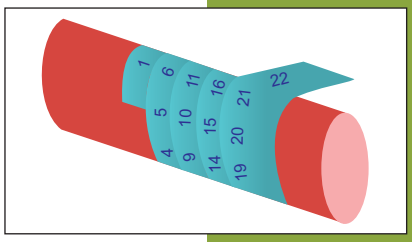
Finalmente, si d' es un natural que divide a a y b, entonces divide a d, pues si $a = d'e$ y $b = d'f$, entonces:

$$\begin{aligned} d &= ma + nb \\ &= md'e + nd'f \\ &= d'(me + nf) \end{aligned}$$

Ahora, la proposición anterior asegura que ***d*** es el máximo común divisor de ***a*** y ***b***.

Los enteros módulo *m*: Z_m

Recordemos el caso de los días de la semana. Pintamos cada día con un color distinto: los domingos de rojo, los lunes de azul, etc. En ese caso el número relevante era el **7**. Ahora, en vez de **7** tomaremos cualquier entero ***m*** mayor que **1**. Es decir ***m*** puede ser **2**, **3**, **17**, **24** ó **1.245**.



Para los días de la semana habíamos partido el conjunto de todos los enteros en los siete subconjuntos de días posibles. El conjunto de todos los días resultó ser la unión disjunta del subconjunto de todos los domingos, unión de todos los lunes, unión de todos los martes, etc.

Ahora, si en vez de **7** tenemos ***m***, el conjunto de todos los enteros queda partido como unión disjunta de ***m*** subconjuntos: el subconjunto de múltiplos de ***m,*** el subconjunto de múltiplos de ***m*** corrido en **1** o múltiplos de ***m*** más **1**, el subconjunto de múltiplos de ***m*** más **2**, etc., hasta terminar con el subconjunto de múltiplos de ***m*** más ***m* – 1**.

Ejemplo

Supongamos ***m*** = 5. Entonces:

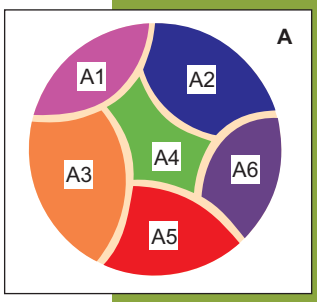
$$Z = \{..,-15,-10,-5,0,5,10,15,20,...\} \cup \{..,-14,-9,-4,1,6,11,16,21,..\} \cup$$
$$\{..,-13,-8,-3,2,7,12,17,22,...\} \cup \{..,-12,-7,-2,3,8,13,18,23,...\} \cup$$
$$\{..,-11,-6,-1,4,9,14,19,24,...\}$$

En general, para un ***m*** cualquiera tendremos, como ya dijimos, ***m*** subconjuntos. El primero es el de los múltiplos de ***m,*** el segundo es el de todos los enteros cuyo resto en la división por ***m*** es **1,** el tercero es el de los enteros con resto **2** en la división por ***m***, y así sucesivamente.

Particiones y equivalencia

Regla. El resto de la división por ***m*** decide en qué subconjunto estará un entero dado.

Tener una partición de un conjunto y tener, en ese conjunto, una relación de equivalencia es lo mismo.



Recordemos

- Una *partición* de un conjunto ***A*** es una familia de subconjuntos A_i no vacíos y disjuntos, tales que su unión es todo el conjunto. En el dibujo, vemos una partición de ***A*** en seis partes.
- Una *relación de equivalencia* en ***A***, es una relación binaria reflexiva, simétrica y transitiva.

Dada una partición de ***A***, definimos la relación ~ diciendo que ***a*** ~ ***b*** si ***a*** y ***b*** están ambos en una misma parte. Es muy fácil verificar que esta relación es reflexiva, simétrica y transitiva.

Recíprocamente, dada una relación de equivalencia ~ en A, las partes de A son las clases de equivalencia de la relación. Es decir, cada parte está formada por todos los elementos relacionados con uno dado.

La relación de congruencia módulo m

Definición. Dado un entero $m > 1$ diremos que dos enteros a y b son equivalentes módulo m, si a y b tienen el mismo resto en la división por m. En este caso escribiremos $a \equiv b \bmod (m)$.

Esa definición es equivalente a esta otra.

$$a \equiv b \bmod (m) \text{ si } a - b \text{ es múltiplo de } m.$$

Demostración. En efecto, si a y b tienen el mismo resto en la división por m, entonces tenemos que $a = q_1 m + r$ y que $b = q_2 m + r$, luego $a - b = q_1 m - q_2 m = (q_1 - q_2) m$. Esto muestra que $a - b$ es un múltiplo de m.

Recíprocamente, si a tiene un resto r_1 en la división por m y b tiene resto r_2, y $a - b$ es múltiplo de m, entonces tenemos que $a = q_1 m + r_1$ y que $b = q_2 m + r_2$, luego $a - b = (q_1 - q_2) m + (r_1 - r_2)$. Pero como $a - b$ es múltiplo de m, entonces $a - b - (q_1 - q_2) m = (r_1 - r_2)$ es múltiplo de m, pero esto es sólo posible si $r_1 - r_2 = 0$ y luego $r_1 = r_2$ como queríamos.

Proposición. La relación $\equiv \bmod (m)$ es de equivalencia. Las clases de equivalencia están formadas por los enteros con el mismo resto en la división por m.

Demostración. La relación de congruencia módulo m es claramente reflexiva y simétrica, ya que a tiene el mismo resto que a en la división por m y, si a tiene el mismo resto que b entonces b tiene el mismo resto que a. Veamos que es transitiva. Sean a y b con el mismo resto en la división por m y sea c con el mismo resto que b en la división por m. Entonces el resto de a y el resto de c en la división por m son iguales.

Con lo que sabemos ahora, podemos afirmar que para el caso de los días de la semana, la partición de todos los días, en días domingo, lunes, martes, etc. es la misma que da la relación de equivalencia $\equiv \bmod (7)$.

El conjunto de clases de equivalencia de la relación $\equiv \bmod (m)$ se denota Z_m.

Llamaremos conjunto de enteros módulo m al conjunto Z_m. Este conjunto sólo tiene m elementos. Cada elemento de este conjunto es un subconjunto infinito de enteros, es toda una clase de equivalencia de la relación $\equiv \bmod (m)$.

Los enteros $0, 1, 2, 3, \ldots, m-1$ pertenecen a clases distintas y, por lo tanto, son un conjunto de representantes de todas las clases. Usualmente elegiremos estos representantes. Como notación

usaremos simplemente a para referirnos a su clase (esto no causará confusión porque del contexto quedará claro si nos referimos al entero a o la clase de congruencia de a módulo m). De todas formas, para referirnos a la clase de un entero cualquiera a también podemos usar $[a]$.

Para el caso de los días de la semana, tomar clase es preguntarse qué día de la semana cae un cierto día. Identificar si ese día es lunes o miércoles es determinar su clase de congruencia módulo 7.

Veamos otros casos. Tomemos $m = 15$ y analicemos qué es Z_{15}. Sabemos que Z_{15} es un conjunto con 15 elementos, cada uno de sus elementos es un subconjunto infinito de enteros que tienen un mismo resto en la división por **15**. Así los enteros **1, 16, 31** y **46** están en un mismo subconjunto. Esto se resume diciendo que:

$$\begin{aligned} 1 &\equiv 16 \\ &\equiv 31 \\ &\equiv 46 \bmod (15) \end{aligned}$$

Cada uno de estos 15 conjuntos tiene un miembro distinguido. Estos son: **0, 1, 2, …, 14**. Luego, para identificar a qué clase pertenece un entero dado basta decir con cuál de éstos comparte clase. Así, para identificar la clase a la que pertenece el **1.542**, basta decir $1.542 \equiv 12 \bmod (15)$.

Veamos algunos ejemplos simples. Tomemos los números **247** y **– 58** y calculemos sus clases de congruencia módulo 2, 3, 5, 9 y 11.

Aclaración que aclara. Cuando decimos calcular la clase de congruencia de un entero dado a módulo un m dado, debemos encontrar el único de los enteros 0, 1, 2,…, $m – 1$ que es congruente con a módulo m. Esto no es otra cosa que calcular el resto de la división de a por m.

$$\begin{aligned} 247 &\equiv 1 \bmod (2) \\ 247 &\equiv 1 \bmod (3) \\ 247 &\equiv 2 \bmod (5) \\ 247 &\equiv 4 \bmod (9) \\ 247 &\equiv 5 \bmod (11) \end{aligned} \qquad \begin{aligned} -58 &\equiv 0 \bmod (2) \\ -58 &\equiv 2 \bmod (3) \\ -58 &\equiv 2 \bmod (5) \\ -58 &\equiv 5 \bmod (9) \\ -58 &\equiv 8 \bmod (11) \end{aligned}$$

Para resolver

4.10 Calcular las clases de congruencia módulo **7** de los siguientes enteros: **13** , **– 18** , **1.743**.

4.11 Encontrar un número entre **23** y **29** que sea congruente a **1** módulo **5**.

Suma y producto módulo m

De la misma forma en que sumamos horas en el reloj de 12 horas y días de la semana podremos sumar enteros módulo m. Más aun, podremos también multiplicarlos.

Para sumar o multiplicar dos enteros módulo m se toma un representante de cada uno, se suman o multiplican, y finalmente se considera la clase del resultado.

Definición. Dado un entero m mayor que **1** y dados $[a]$ y $[b]$ en Z_m, definimos la suma de enteros módulo m por $[a] + [b] = [a + b]$, y el producto de enteros módulo m por $[a] . [b] = [a . b]$.

Ejemplos

$6 + 5 \equiv 3 \bmod (8)$ $\quad 6 + 5 \equiv 1 \bmod (5)$ $\quad 6 + 5 \equiv 2 \bmod (3)$
$6 \cdot 5 \equiv 6 \bmod (8)$ $\quad 6 \cdot 5 \equiv 0 \bmod (5)$ $\quad 6 \cdot 5 \equiv 0 \bmod (3)$

Para resolver

4.12 Decir si es correcto o no:

$23 \equiv 3 \bmod (8)$ $\quad 42 \equiv 1 \bmod (7)$ $\quad -37 \equiv 1 \bmod (3)$

4.13 En todos los casos encontrar el menor x no negativo que verifique la identidad planteada:

$76 \equiv x \bmod (8)$ $\quad 83 \equiv x \bmod (7)$ $\quad -22 \equiv x \bmod (3)$

4.4. La aritmética modular

La suma y el producto de los enteros módulo m son operaciones heredadas de la suma y el producto de los enteros. Lo mismo sucedió con la aritmética del reloj o la aritmética de la semana. Las propiedades básicas, que listamos a continuación, son heredadas de las correspondientes propiedades de la aritmética de los enteros.

Propiedades

Sea m un entero, $m > 1$. Entonces, la suma y el producto de enteros módulo m tienen las siguientes propiedades.

1. La suma es asociativa.
2. La suma es conmutativa.
3. La clase del **0**, [**0**], es el elemento neutro para la suma.
4. Toda clase $[a]$ tiene un opuesto para la suma $[m - a]$ que llamamos $-[a]$.
5. El producto es asociativo.
6. El producto es conmutativo.
7. La clase del **1**, [**1**], es el elemento neutro o identidad para el producto.
8. El producto es distributivo respecto a la suma.

A modo de ejemplo, veamos cómo se demuestran algunas de esas propiedades.

Para la suma (el resto se deduce de manera análoga):

* asociatividad de la suma:

$$\begin{aligned}([a] + [b]) + [c] &\equiv [a + b] + [c] \\ &\equiv [(a + b) + c] \\ &\equiv [a + (b + c)] \\ &\equiv [a] + ([b + c])\end{aligned}$$

* opuesto para la suma: $[a] + [-a] \equiv [a - a] \equiv [0]$. Además $[m - a] \equiv [-a]$.

Hasta aquí, las analogías con la aritmética de los números enteros. Ahora, veamos que hay algunas diferencias. Por ejemplo, en $Z_{12,}$ **6 + 6 = 0** . Esto no pasa en los enteros. Nunca obtenemos **0** sumando un mismo número dos veces. En general, en Z_m si sumamos ***m*** veces **1** obtenemos **0,** es decir **1 + 1 + …+ 1 = 0** si hay ***m*** sumandos. Por otro lado, por ejemplo en Z_5, **4 . 4 = 1,** es decir **4** al cuadrado es **1,** y también **3 . 2 = 1.** Hay números distintos de la identidad o su opuesto que son inversibles para el producto. En cambio, para el producto de enteros los únicos inversibles son el **1** y su opuesto el **– 1**.

Para los enteros, se puede aprender de memoria las tablas de multiplicar del 2, del 3, etc., hasta la del 10. Pero, como los enteros son infinitos, es imposible saber de memoria todas las tablas de multiplicar. En cambio, para los enteros módulo ***m,*** sólo hay una cantidad finita de tablas que aprender, porque es finita la cantidad de enteros módulo ***m.***

A continuación, mostramos las tablas de suma y multiplicación completas, es decir para todos los enteros módulo ***m*** juntos, para algunos valores pequeños de ***m.***
Tablas de suma y multiplicación de Z_m para ***m*** : 2 … 8

Z_2 :

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

Z_3 :

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Z_4 :

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Z_5 :

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Z_6 :

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

.	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Z_7 :

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

.	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Z_8 :

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

.	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Cada una de estas tablas tiene sus propias regularidades, que se distinguen a simple vista. Además, el conjunto de tablas tiene también otras regularidades que son algo más difíciles de explicitar.

Con las tablas a mano, discutamos sobre estas regularidades.

Pares y nones

Las tablas de Z_2 no son más que las reglas de sumar y multiplicar pares e impares. En efecto, los enteros pares son exactamente los congruentes a 0 módulo 2, y los impares son exactamente los congruentes a 1 módulo 2. Entonces, **par** + **par** = **par**, **par** + **impar** = **impar** e **impar** + **impar** = **par**. Esto se corresponde con que **0** + **0** = **0**, **0** + **1** = **1** y **1** + **1** = **0** en Z_2.

La situación con el producto es análoga. Es decir, **par** . **par** = **par**, **par** . **impar** = **impar** e **impar** . **impar** = **impar**. Esto se corresponde con que **0** . **0** = **0**, **0** . **1** = **0** y **1** . **1** = **1** en Z_2.

Regularidad en la tabla de la suma

Es evidente que en las filas de las tablas de la suma aparecen todos los números ordenados y en forma cíclica. Más aun, entre una fila dada y la próxima, la diferencia es un corrimiento a la derecha en una unidad. Claro, esta última fila se obtiene de la anterior sumando **1**.

Divisores de cero

En todas las tablas de multiplicación tenemos que en la primera fila y en la primera columna son todos ceros, esto es así pues **0** . a = **0** y a . **0** = **0** para todo a. Lo que llama

la atención es que en algunas tablas no hay más ceros que éstos (digamos obligatorios) y en cambio en otras hay más ceros. Por ejemplo, en la tabla de Z_4 vemos que $2 \cdot 2 = 0$. Un par de elementos distintos de cero que multiplicados dan cero, se llaman *divisores de cero*. Nos podemos hacer una primera pregunta:

¿qué tablas tienen divisores de cero?

Otra pregunta, más fina aún, es:

¿cuáles son exactamente todos los divisores de cero que hay en Z_m para cada m ?

Mirando las tablas, observamos que las que corresponden a $m = 4$, 6, y 8 tienen divisores de cero, mientras que las que corresponden a $m = 2$, 3, 5 y 7 no tienen divisores de cero. Estos últimos son números primos y los primeros son números compuestos. La respuesta a la primera pregunta es:

Si m es primo, entonces Z_m no tiene divisores de cero.
Si m no es primo, entonces Z_m tiene divisores de cero.

Supongamos que a y b son dos números distintos de 0 en Z_m con $a\ b = 0$. En primer lugar, podemos suponer que tanto a como b son menores que m, como lo son los elementos de la tabla. Luego $a\ b = 0$ en Z_m quiere decir que $a\ b$ es múltiplo de m, es decir $a\ b = k\ m$. Si m es primo, se sigue que m divide a a o m divide a b; pero como ambos son menores que m esto no es posible y m no es primo.

Por otro lado, si m no es primo, entonces $m = a.b$ con a y b menores que m, luego en Z_m tenemos que $a\ b = 0$. Es decir, Z_m tiene divisores de cero.

Unidades

En todas las tablas de multiplicación vemos algunas unidades. En todas vemos al 1 y al $m - 1$ como unidades. Esto es porque siempre $1 \cdot 1 = 1$, además siempre $m - 1 = -1$ en Z_m y $-1 \cdot -1 = 1$. Ahora en varias tablas aparecen más unidades.

¿Qué tablas tienen otras unidades?

Para aquellas tablas con otras unidades no triviales, es decir distintas de 1 y –1,

¿cuáles son todas las unidades no triviales?

Si hiciéramos muchas más tablas, veríamos que todas tendrán unidades no triviales. Sólo Z_2, Z_3, Z_4, y Z_6, no tienen otras unidades. Esto se puede deducir se la siguiente verdad.

Un a en Z_m es inversible si y sólo si $(a, m) = 1$.

Aclaración

a y m se dicen ***coprimos*** si el máximo común divisor de ellos (a, m) es 1.

En efecto, si a es inversible, entonces existe b tal que $a\ b = 1$, en Z_m. Es decir, $a\ b - 1 = k\ m$ o, equivalentemente, $1 = a\ b - k\ m$. Luego, si d es el máximo común divisor de a y m, tanto m como a son múltiplos de d. Así resulta que 1 es múltiplo de d, lo que sólo es posible si $d = 1$.
Recíprocamente, si a y m son coprimos, entonces $1 = a\ t + m\ s$ (recordemos que siempre el máximo común divisor de dos números se puede escribir como combinación lineal entera de ellos). Tomando clase de congruencia y dado que $m\ s$ es 0 en Z_m, resulta que $1 = a\ t$ en Z_m.

Cuadrados perfectos

Los cuadrados perfectos son aquellos números que aparecen en la diagonal de la tabla de multiplicación; son los resultados de hacer $a \cdot a = a^2$ para algún a. El estudio de estos cuadrados perfectos fue, en la historia de la teoría de números, un hito. Más adelante en este capítulo volveremos a esto bajo el título La Reciprocidad Cuadrática.

Para resolver

4.14 Mirando las tablas de multiplicación escritas más arriba, listar los cuadrados perfectos de de cada una de ellas.

4.15 Observar que en todos los casos el producto de unidades es otra unidad. ¿Cómo se explica esto?

4.5. Aplicaciones a la aritmética entera

La resolución de ecuaciones acaparó, desde tiempos remotos, mucha atención de la ciencia matemática y muchísimos matemáticos han dedicado vidas enteras a su estudio y al desarrollo de métodos para encontrar soluciones a las mismas. Hoy en día, sigue siendo un área de muy vasta de investigación y, a pesar de todos los resultados alcanzados, queda muchísimo por hacer.

Cuando decimos ecuaciones sin más aclaraciones, incluimos todo tipo de ecuaciones, es decir, consideramos aquellas con más de una variable, con coeficientes en distintos conjuntos de números y sistemas de ecuaciones de estos tipos. Además, dada una ecuación o dado un sistema de ecuaciones con coeficientes en cierto conjunto de números podemos buscar soluciones en el mismo conjunto donde viven los coeficientes, o restringir la búsqueda de soluciones a un conjunto más chico, o permitir soluciones en conjuntos más grandes. Muchas veces, sólo interesan las soluciones reales de una ecuación polinomial, aunque también tenga soluciones complejas; o sólo interesan las soluciones enteras que pueda tener esa misma ecuación. Otras veces, se consideran las soluciones reales o complejas de una ecuación polinomial con coeficientes enteros o racionales.

Repasemos algunos conceptos para ecuaciones polinomiales con una sola variable con coeficientes reales. Por ejemplo:

$x^2 + 1 = 0$; $3x^3 - 2x^2 + 1 = 0$; $5x^4 + x^3 - 2x + 3 = 0$; $ax^2 + bx + c = 0$.

Sabemos que:

1) algunas no tienen ninguna solución real, por ejemplo la primera,
2) todas tienen soluciones complejas. Más aún, tienen tantas como su grado, si se cuentan con multiplicidad,
3) las de grado impar siempre tienen al menos una solución real,
4) para las de grado 2 hay una fórmula para sus 2 soluciones complejas.

Las tres primeras ecuaciones del ejemplo tienen coeficientes enteros. Para éstas, podríamos preguntar si las soluciones son o no enteras. O simplemente, podríamos preguntar si tienen o no soluciones enteras, sin importar que tengan otras soluciones.

Ecuaciones enteras

La aritmética modular es una herramienta que ayuda a estudiar ecuaciones enteras.

No pretendemos dar ningún método sistemático para tratar estos problemas. Sin embargo, sí queremos reforzar la impresión de que la aritmética modular es una herramienta efectiva en diversos problemas con números enteros.

El principio general es que para estudiar un problema entero puede ser más fácil estudiar las versiones modulares del mismo problema. Cambiamos un problema por muchos problemas similares más fáciles.

Veamos este principio en algunos ejemplos.

Ejemplo

¿Tiene la ecuación $3X + 2Y = 1$ soluciones enteras? Si tiene, ¿cuáles son todas sus soluciones enteras?

Luego de contemplar esta ecuación y haciendo algunas pruebas podemos ver que $a = 1$ y $b = -1$ es solución, pues:

$$3 \cdot 1 + 2 \cdot (-1) = 3 - 2 = 1$$

Quizá sea un poco más difícil darse cuenta de que $a = 3$ y $b = -4$ también es solución, pues

$$3 \cdot 3 + 2 \cdot (-4) = 9 - 8 = 1$$

Podríamos continuar buscando, pero ¿hasta cuándo?

Por otro lado, el par $(0, 0)$ no es solución, ya que si $X = 0$ e $Y = 0$, entonces $3X + 2Y = 0$ y no $3X + 2Y = 1$.

Analicemos esta ecuación bajo algunas congruencias. Como **2** y **3** aparecen en ella, no parece absurdo empezar con **2** y **3**. Supongamos que el par (X, Y) es solución de la ecuación, entonces tendremos que $3X + 2Y \equiv 1 \bmod (2)$ y también $3X + 2Y \equiv 1 \bmod (3)$.

En el primer caso estaremos analizando cuestiones de paridad. Como $3X + 2Y \equiv X \bmod (2)$, pues $3X \equiv X \bmod (2)$ y $2Y \equiv 0 \bmod (2)$, si $3X + 2Y \equiv 1$, entonces debe ser $X \equiv 1 \bmod (2)$, es decir si hay solución ***X debe ser impar***.

En el segundo caso, como $3X + 2Y \equiv -Y \bmod (3)$ debe ser $-Y \equiv 1 \bmod (3)$, que es lo mismo que $Y \equiv -1 \bmod (3)$.

Resumiendo, si (X, Y) es solución debe ser $X = 2n + 1$, y debe ser $Y = 3m - 1$. Reemplazando en la ecuación resulta que :

$$3X + 2Y = 3(2n + 1) + 2(3m - 1) = 1$$

que es lo mismo que $6(n + m) = 0$. De aquí se deduce que $m = -n$. Recíprocamente, si tomamos n y m tales que $m = -n$ y a partir de ellos construimos $X = 2n + 1$ e $Y = 3m - 1 = -3n - 1$ éstos serán solución de la ecuación.

Como conclusión, tenemos que la ecuación $3X + 2Y = 1$ tiene soluciones enteras y todas las soluciones son de la forma $X = 2n + 1$ e $Y = -3n - 1$, donde n es un entero cualquiera. Podemos explicitar algunas.

Si $n = 0$	$X = 1, Y = -1$	Si $n = -1$	$X = -1, Y = 2$
Si $n = 1$	$X = 3, Y = -4$	Si $n = -2$	$X = -3, Y = 5$
Si $n = 2$	$X = 5, Y = -7$	Si $n = -3$	$X = -5, Y = 8$

Reglas de divisibilidad

La aritmética modular es particularmente adecuada para estudiar problemas de divisibilidad. Recordemos que un número entero n es divisible por m, si y sólo si $n = 0$ en Z_m es decir si n es congruente a **0** módulo m. Esto nos permitirá deducir y explicar las reglas de divisibilidad que conocemos y además obtener otras.

¿Qué reglas conocemos? Seguramente, las reglas de divisibilidad por **2** y por **5**. Quizá también la de divisibilidad por **3** y alguna más. Comencemos con algunos ejemplos.

Ejemplos

Ejemplos de divisibilidad

1) **124** es divisible por **4** , pues $124 = 100 + 20 + 4$
$\equiv 0 + 0 + 0$
$\equiv 0 \bmod (4)$

2) ¿Para qué valores de n el número $3^n + 1$ es divisible por **4**?

Si $n = 1$ --------- $3^n + 1 = 4$, que sí es divisible por **4**.
Si $n = 2$ --------- $3^n + 1 = 10$, que no es divisible por **4**.
Si $n = 3$ --------- $3^n + 1 = 28$, que sí es divisible por **4**.
Si $n = 4$ --------- $3^n + 1 = 82$, que no es divisible por **4**.
Si $n = 5$ --------- $3^n + 1 = 244$, que sí es divisible por **4**.
Si $n = 6$ --------- $3^n + 1 = 730$, que no es divisible por **4**.

Este experimento hace tentador arriesgar que $3^n + 1$ es divisible por **4** exactamente cuando n es impar. ¿Podremos probar esto para todo n? Sí, podemos.

Primer paso, observamos que $3 \equiv -1 \pmod 4$. Esta es la clave porque entonces $3^n \equiv (-1)^n 1$ o -1, según sea n par o impar. Finalmente, $3^n + 1 \equiv (-1)^n + 1 \equiv 2$ ó 0, según sea n par o impar, como queríamos.

□ 4.6. Las reglas de divisibilidad de los naturales

Las reglas de divisibilidad son reglas prácticas que permiten determinar si un número natural dado es divisible por **2**, **3**, **5**, etc. en términos de sus dígitos decimales. Por ejemplo, un número es divisible por **2**, es decir es par si su último dígito es par.

Estas reglas dependen de la escritura del número en base 10. Luego, no sirven para determinar si el número $124^2 - 11$ expresado así es divisible por **3** o no. Si quisiéramos aplicar la regla de divisibilidad por 3, primero debemos escribir $124^2 - 11$ como **15.365** para aplicarla luego.

Recordemos algunas de las reglas de divisibilidad más fáciles.

Divisibilidad por **2**: un número es divisible por **2,** si el dígito de las unidades es par, es decir si es **0**, **2**, **4**, **6** u **8**.

Divisibilidad por **5**: un número es divisible por **5,** si el dígito de las unidades es divisible por **5**, es decir es **0** ó **5**.

Divisibilidad por **3**: un número es divisible por **3,** si la suma de sus dígitos es divisible por **3**.

Divisibilidad por **9**: un número es divisible por **9,** si la suma de sus dígitos es divisible por **9**.

Las dos últimas reglas de divisibilidad, por **3** y por **9,** son distintas de las primeras, ya que incluyen determinar si otro número es divisible por **3** ó **9,** respectivamente. Sin embargo, estos números son mucho más chicos que los originales, así iterando esta regla llegaremos a un punto en el que podremos determinar si el número en cuestión es divisible por **3** o por **9** por simple inspección. A modo de ejemplo, determinemos si el número

$A = 123456789123456789123456789123456789123456789123456789123456789$

es divisible por **3** o no. La suma de sus dígitos es **315**, cuyos dígitos suman **9**. Como **9** es divisible por **3**, entonces **315** también es divisible por **3,** luego ***A*** es divisible por **3**.

A continuación, deducimos estas reglas y algunas más usando la aritmética modular. Una vez que las hayamos comprendido se podrá enunciar otras reglas de divisibilidad.

Divisibilidad por 2

Supongamos que queremos determinar si **3.257** es divisible por **2** o no. Esto es lo mismo que determinar si **3.257** es congruente a **0** módulo **2** o no. Por lo tanto, debemos calcular la clase de congruencia de **3.257** módulo **2.** Para esto resulta conveniente escribir **3.257** de la siguiente forma:

$$\mathbf{3.257 = 3 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 7.}$$

Esto no es más que nuestro sistema decimal.

Ahora, si planteamos lo que necesitamos saber: $\mathbf{3.257 \equiv X\ mod\ (2)}$, que es equivalente a plantear $\mathbf{3.257 = 3 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 7 \equiv X\ mod\ (2)}$, y dado que $\mathbf{10 \equiv 0\ mod\ (2)}$, resulta que :

$$\mathbf{3.257 = 3 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 7 \equiv 7\ mod\ (2).}$$

El que determinar si todo el número $\mathbf{3.257 = 3 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 7}$ es o no divisible por **2** es su último dígito, el **7.** En este caso, claro está, 7 no es par y **3.257** tampoco.

Repitamos esto en general. Si en vez de **3.257,** tenemos el número $a_r a_{r-1} \ldots a_3 a_2 a_1 a_0$, también escrito en sistema decimal, donde los ***a's*** son sus dígitos decimales, tenemos que:

$$a_r a_{r-1} \ldots a_3 a_2 a_1 a_0 = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

Nuevamente, como $\mathbf{10 \equiv 0\ mod\ (2)}$, resulta que:
$a_r a_{r-1} \ldots a_3 a_2 a_1 a_0 = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_0\ \mathbf{mod\ (2)}$.

Conclusión: $a_r a_{r-1} \ldots a_3 a_2 a_1 a_0$ es divisible por **2** si su último dígito, a_0, lo es.

Divisibilidad por 5

Sea $A = a_r a_{r-1} \ldots a_3 a_2 a_1 a_0$. Tomando congruencia módulo **5,** y dado que $\mathbf{10 \equiv 0\ mod\ (5)}$, tenemos que:
$a_r a_{r-1} \ldots a_3 a_2 a_1 a_0 = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \ldots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_0\ \mathbf{mod\ (5)}$.

Conclusión: $a_r a_{r-1} \ldots a_3 a_2 a_1 a_0$ es divisible por **5,** si su último dígito, a_0, lo es.

Divisibilidad por 3

Sea $A = a_r a_{r-1} \ldots a_3 a_2 a_1 a_0$. Tomando congruencia módulo **3,** y dado que $10 \equiv 1 \bmod (3)$, tenemos que:

$$a_r a_{r-1} \ldots a_2 a_1 a_0 = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$
$$\equiv a_r + a_{r-1} + \ldots + a_2 + a_1 + a_0 \bmod (3).$$

Conclusión: $a_r a_{r-1} \ldots a_3 a_2 a_1 a_0$ es divisible por **3,** si la suma de sus dígitos es divisible por **3.**

Divisibilidad por 9

Sea $A = a_r a_{r-1} \ldots a_3 a_2 a_1 a_0$. Tomando congruencia módulo **9,** y dado que $10 \equiv 1 \bmod (9)$, tenemos que:

$$a_r a_{r-1} \ldots a_2 a_1 a_0 = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$
$$\equiv a_r + a_{r-1} + \ldots + a_2 + a_1 + a_0 \bmod (9).$$

Conclusión: $a_r a_{r-1} \ldots a_3 a_2 a_1 a_0$ es divisible por **9,** si la suma de sus dígitos es divisible por **9.**

Divisibilidad por 11

Sea $A = a_r a_{r-1} \ldots a_3 a_2 a_1 a_0$. En este caso, tomando congruencia módulo **11,** tenemos una novedad.

Ahora $10 \equiv -1 \bmod (11)$, y luego $10^2 \equiv 1 \bmod (11)$.
En general, $10^k \equiv 1 \bmod (11)$ si k es par y $10^k \equiv -1 \bmod (11)$ si k es impar. Entonces, resulta que:

Si $A = a_r a_{r-1} \ldots a_3 a_2 a_1 a_0$, con r par, es decir A tiene un número impar de dígitos, entonces $a_r a_{r-1} \ldots a_2 a_1 a_0 = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$
$\equiv a_r - a_{r-1} + \ldots + a_2 - a_1 + a_0 \bmod (11)$.

Si $A = a_r a_{r-1} \ldots a_3 a_2 a_1 a_0$, con r impar, es decir A tiene un número par de dígitos, entonces $a_r a_{r-1} \ldots a_2 a_1 a_0 = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$
$\equiv -a_r + a_{r-1} - \ldots - a_2 + a_1 - a_0 \bmod (11)$.

Conclusión: $a_r a_{r-1} \ldots a_3 a_2 a_1 a_0$ es divisible por **11,** si la suma alternada de sus dígitos es divisible por **11.** No importa cómo se realice la suma alternada de los dígitos, es decir no importa empezar con **+** o con **–** ya que una suma alternada es la opuesta de la otra suma alternada, y así ambas son divisibles por **11,** o ambas no lo son.

□ 4.7. Ecuaciones lineales en la aritmética modular

Hasta aquí, hemos aprendido la aritmética elemental de los enteros modulares. Demos un paso hacia adelante y consideremos ecuaciones de grado 1 con una sola incógnita. Esto

resultará más complicado que el estudio de las mismas ecuaciones en los enteros o en los números reales. Sin embargo, daremos una respuesta completa y totalmente satisfactoria.

Recordemos cuál es la situación en el caso de los enteros o de los reales. La ecuación $3X + 1 = 0$ tiene siempre una solución real, que se obtiene despejando. Si $3X + 1 = 0$, entonces $3X = -1$ y $X = -1/3$. Más aún, esta es la única solución real. Si nos preguntamos si esta misma ecuación tiene o no soluciones enteras, basta mirar su única solución real y ver si es o no entera. En este caso como $-1/3$ no es entero, la ecuación no tiene solución entera.

La ecuación $AX + B = 0$, suponiendo A distinto de 0 tiene siempre una solución real, más precisamente $X = -B/A$. Más aun, esta solución es única.

¿Qué pasa con este mismo tipo de ecuaciones en el mundo modular?

Ejemplos

$2X + 2 \equiv 1 \mod (4)$ $\qquad$ $3X + 2 \equiv 1 \mod (4)$

Resolver una ecuación es encontrar al menos una solución, si la hay. Explicar claramente que no hay, si no las hay. Finalmente, en el caso de haber soluciones, darlas todas.

Al principio de esta sección consideramos una ecuación y buscábamos soluciones reales o enteras. Los conjuntos en los que buscábamos esas soluciones eran muy grandes, de hecho infinitos.

En cambio, en las ecuaciones del ejemplo buscamos soluciones en un conjunto finito y muy chico. Buscamos soluciones en Z_4 que tiene sólo 4 elementos, entonces podemos probar con todos ellos y ver qué resulta. Evaluamos, operando con la suma y la multiplicación de Z_4 los miembros de la izquierda de cada ecuación en todos los elementos de Z_4, el 0, el 1, el 2 y el 3.

	$2X+2$
0	2
1	0
2	2
3	0

	$3X+2$
0	2
1	1
2	0
3	3

Con esto es posible resolver estas dos ecuaciones completamente. En la primera tabla vemos que como resultado de la evaluación sólo obtuvimos los números 0 y 2. No obtuvimos el 1. Luego, la primera ecuación del ejemplo no tiene ninguna solución módulo 4. En cambio, en la segunda tabla obtuvimos todos los números posibles, luego la segunda ecuación del ejemplo tiene una solución: $X = 1$. Más aún, ésta es única.

Con estas tablas, que usamos para resolver las ecuaciones del ejemplo, también podemos decir algunas cosas más. Si en la primera ecuación en vez del 1 estuviera el 2, la primera tabla indica que la nueva ecuación tiene solución. Más aun, tiene exactamente dos soluciones: $X = 0$ y $X = 2$. En cambio, en la segunda la situación es más uniforme, ya que si cambiamos el 1 por cualquier otro número 0, 2, ó 3, la nueva ecuación también tiene una única solución.

Resumiendo: La ecuación $2X+2 \equiv C \mod (4)$ tiene solución sólo para $C=0$ y $C=2$. En estos casos tiene, exactamente, dos soluciones.

La ecuación $3X+2 \equiv C \mod (4)$ tiene solución para todo C, es decir $C=0, 1, 2$ ó 3. En todos los casos tiene una única solución.

¿Cuál es la razón de esta diferencia entre el comportamiento de una y otra ecuación?

Parte de la razón está en el coeficiente que acompaña a la incógnita X y en el 4. En la primera ecuación este coeficiente es 2 y en la segunda es 3. ¿Y la diferencia? Bueno, el máximo común divisor entre 2 y 4 es $(2, 4) = 2$ y el máximo común divisor de 3 y 4 es $(3, 4) = 1$. Éstas son, justamente, las cantidades de soluciones que hay en uno y otro caso, cuando hay solución.

Antes de seguir, observemos que la ecuación $2X + 2 \equiv 1 \mod (4)$ es equivalente a la ecuación $2X + 1 \equiv 0 \mod (4)$ porque para pasar de la primera a la segunda basta restar 1 a ambos miembros, y para volver de la segunda a la primera basta sumar 1 a ambos miembros. Así, ambas tienen las mismas soluciones.

Por lo tanto, basta estudiar las ecuaciones de la forma $AX + B \equiv 0 \mod (m)$. La verdad precisa y completa para estas ecuaciones es la siguiente:

Proposición: La ecuación $AX + B \equiv 0 \mod (m)$ tiene solución, si y sólo si (A, m) divide a B. Cuando hay solución, hay exactamente (A, m) soluciones distintas.

Ante una ecuación dada, esta verdad nos sirve para determinar si la misma tiene o no solución, y en caso de tener solución, para saber cuántas tiene. Sin embargo, no nos dice cómo encontrar las soluciones.

Veremos cómo encontrar, cuando existen, todas las soluciones. Si bien, esto no reemplaza a la demostración de la Proposición es una parte importante de la misma.

Analicemos un par de ejemplos:

Ejemplos

$$6X + 2 \equiv 0 \mod (15)$$
$$6X + 9 \equiv 0 \mod (15)$$

Ambas ecuaciones son muy parecidas $m = 15$ y $A = 6$ en ambas. Sólo cambia B, en un caso es $B = 2$ y en el otro $B = 9$.Tenemos que $(6, 15) = 3$. Según la proposición, debemos testear si 3 divide o no a B. Para la primera ecuación resulta que no, porque 3 no divide a 2. Para la segunda resulta que sí, porque 3 sí divide a 9. Conclusión: la primera ecuación no tiene solución, la segunda sí.

Aunque no es necesario, hagamos una tabla para cada ecuación

	$6X+2$
0	2
1	8
2	14
3	5
4	11
5	2
6	8
7	14
8	5
9	11
10	2
11	8
12	14
13	5
14	11

	$6X+9$
0	9
1	0
2	6
3	12
4	3
5	9
6	0
7	6
8	12
9	3
10	9
11	0
12	6
13	12
14	3

Como predijo la proposición, la primera no tiene solución y la segunda sí. Más aun, la segunda tiene **3** soluciones: $X = 1, X = 6, X = 11$. ¿Cómo encontrarlas?

A partir de la ecuación $6X + 9 \equiv 0 \bmod (15)$ consideramos otra que se obtiene dividiendo todo por el $(6, 15) = 3$, para obtener la ecuación $2X + 3 \equiv 0 \bmod (5)$. Esta última siempre tiene solución porque el coeficiente de X y m, en este caso **2** y **5,** son siempre coprimos, es decir con máximo común divisor igual a **1**. En este caso, esto quiere decir que el **2** es invertible en Z_5. En efecto, $2 \cdot 3 = 1$ en Z_5. Luego, la ecuación $2X + 3 \equiv 0 \bmod (5)$ se resuelve fácilmente. Sumamos -3 para obtener $2X \equiv -3$, y multiplicamos por **3**, el inverso de **2** y resulta $X \equiv -9 \equiv 1 \bmod (5)$. Esta solución es única módulo **5**. A partir de ésta, podemos encontrar otras módulo **15,** sumando **5** y luego **10**. Así, aparecen las soluciones **1, 6** y **11** que vimos en la tabla.

Hagamos un ejemplo más.

Ejemplo

Consideremos la ecuación $4X + 7 \equiv 17 \bmod (18)$. Procedamos paso a paso.

1. Reemplazamos la ecuación dada por esta otra equivalente $4X + 8 \equiv 0 \bmod (18)$. Esto se obtiene de la primera sumando **1** a ambos miembros.

2. Calculamos el máximo común divisor de **4** y **18**. Tenemos $(4,18) = 2$.

3. Observamos que **2** sí divide a **8** y concluimos que la segunda ecuación tiene solución. Como esta es equivalente a la primera, la primera también tiene solución. Más aún, ambas tienen las mismas soluciones.

4. A partir de la segunda ecuación consideramos otra, que se obtiene de ésta dividiendo todos los coeficientes y el **18** por **2**. Así, consideramos la ecuación $2X + 4 \equiv 0 \bmod (9)$ que es equivalente a la ecuación $2X \equiv 5 \bmod (9)$.

5. En ésta última, como **2** es inversible y su inverso es **5**, multiplicamos ambos miembros por **5** para obtener la ecuación equivalente $X \equiv 7 \bmod (9)$.

6. Ahora **7** es la única solución de esta última ecuación y **7** es solución de la primera pero no la única.

7. Para obtener las restantes, que sabemos son **2**, sumamos a esta solución **9**. Obtenemos así las dos soluciones de la ecuación original: **7** y **16**.

Para resolver

Resolver completamente las siguientes ecuaciones.

4.16. **$6X + 5 \equiv 14 \bmod (21)$**

4.17. **$6X + 5 \equiv 13 \bmod (21)$**

4.8. Residuos cuadráticos

Esta sección es más difícil que las anteriores. Su contenido es elemental, pero profundo. Se incluyó porque es considerado como el inicio de la teoría de números moderna.

Sea p un primo impar. Un entero a, coprimo con p, es un *residuo cuadrático* módulo p, si existe un x tal que $x^2 \equiv a \bmod (p)$. En caso contrario, a es un *no–residuo cuadrático* módulo p.

Dados un primo p, y un entero cualquiera a, el símbolo de Legendre está definido como sigue:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & (\text{si } p,a)=1, \text{ y } a \text{ es residuo cuadrático módulo } p \\ 0, & \text{si } p \mid a \\ -1, & (\text{si } p,a)=1, \text{ y } a \text{ es no - residuo cuadrático módulo } p \end{cases}$$

Calculemos los cuadrados en Z_p, para $p = 5, 7, 11$.

	1	2	3	4	5	6	7	8	9	10
k^2 módulo 5	1	4	4	1						
k^2 módulo 7	1	4	2	2	4	1				
k^2 módulo 11	1	4	9	5	3	3	5	9	4	1

Ahora listemos los residuos cuadráticos y los no–residuos cuadráticos para $p = 5, 7, 11$, menores que p.

	Residuos cuadráticos	Residuos no-cuadráticos
$p = 5$	{1,4}	{2,3}
$p = 7$	{1,2,4}	{3,5,6}
$p = 11$	{1,3,4,5,9}	{2,6,7,8,10}

Es notable que para cada uno de estos primos, la cantidad de residuos cuadráticos y la cantidad de no–residuos cuadráticos sea la misma. Si hiciéramos más experimentos, encontraríamos que este fenómeno se repite.

Proposición: Exactamente la mitad de los enteros a, con $0 < a < p - 1$, son residuos cuadráticos módulo p.

Este resultado dice cuántos residuos hay, pero no cómo encontrarlos, ni determinar si un número dado es residuo cuadrático o no. El siguiente criterio es una herramienta eficiente, justamente para determinar si un a dado es residuo cuadrático o no.

Criterio de Euler

Sea p un número primo impar, es decir distinto de **2**, y a un entero cualquiera coprimo con p, entonces:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$$

Ejemplos

¿Es **2** residuo cuadrático módulo **13**?

Usemos el criterio de Euler para contestar esta pregunta.

Como $2^6 = 64 = 13 \cdot 5 - 1$, entonces $2^6 \equiv -1 \mod (13)$, por lo tanto **2** no es residuo cuadrático módulo **13** y la ecuación $x^2 \equiv 2 \mod (13)$ no tiene solución.

Residuos cuadráticos módulo **11**.

Para determinar todos los residuos cuadráticos módulo **11** usamos nuevamente el criterio de Euler. Entonces, calculemos $a^{(11-1)/2} = a^5$ para toda unidad a de Z_{11}.

Tenemos: $1^5 \equiv 1, 2^5 \equiv -1, 3^5 \equiv 1, 4^5 \equiv 1, 5^5 \equiv 1, 6^5 \equiv -1, 7^5 \equiv -1, 8^5 \equiv -1, 9^5 \equiv 1$ y $10^5 \equiv -1$. Los residuos cuadráticos módulo **11** son entonces $\{1, 3, 4, 5, 9\}$.

El papel de los números primos toma enorme relevancia en este tema debido al próximo resultado. El mismo reduce el problema de decidir qué enteros m son residuos cuadráticos módulo un primo p, al problema de decidir que primos q son residuos cuadráticos módulo p.

Teorema: Sea p un primo impar y sean a y b enteros coprimos con p. Entonces

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

La prueba de este teorema es inmediata a partir del criterio de Euler.

Como dijimos, este teorema permite reducir el cálculo de $\left(\frac{m}{p}\right)$ para un m dado, al cálculo de $\left(\frac{q}{p}\right)$ para los primos q que dividen a m.

En efecto si $m = q_1 \cdot \ldots \cdot q_r$ es la factorización prima de m, entonces, el teorema aplicado repetidas veces dice que $\left(\frac{m}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\ldots\ldots\left(\frac{q_r}{p}\right)$.

Luego, para conocer $\left(\frac{m}{p}\right)$ para cualquier entero m y cualquier primo impar p, basta conocer $\left(\frac{q}{p}\right)$ para todos los primos q y conocer $\left(\frac{\pm 1}{p}\right)$. Comenzamos con lo más fácil.

Teorema: Para todo primo p impar, es decir distinto de **2**, valen:

a. $\left(\frac{1}{p}\right) = 1$

b. $\left(\frac{-1}{p}\right) = 1$, si $p \equiv 1 \bmod (4)$ y $\left(\frac{-1}{p}\right) = -1$, si $p \equiv 3 \bmod (4)$

c. $\left(\frac{2}{p}\right) = 1$, si $p \equiv 1$ o $p \equiv 7 \bmod (8)$ y $\left(\frac{2}{p}\right) = -1$, si $p \equiv 3$ o $p \equiv 5 \bmod (8)$.

La Ley de Reciprocidad Cuadrática

Cada uno de los matemáticos que se ocuparon de este fenómeno formuló el resultado a su manera. Quizá hoy, la versión más difundida sea la de Legendre. Sin embargo, en ciertos contextos, otras pueden resultar más útiles.

Versión de Legendre.

Sean p y q primos impares. Entonces $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(p\frac{1}{2}\right)\cdot\left(q\frac{1}{2}\right)}$

Este teorema nos da un método muy eficiente para calcular recursivamente $\left(\frac{p}{q}\right)$. Veamos cómo funciona.

Ejemplo. Tomemos $p = 11$ y $q = 43$ y calculemos $\left(\frac{11}{43}\right)$. Por la reciprocidad cuadrática: $\left(\frac{11}{43}\right)\left(\frac{43}{11}\right) = (-1)^{\left(11\frac{-1}{2}\right)\cdot\left(43\frac{-1}{2}\right)} = (-1)^{5.21} = -1$. Además $\left(\frac{43}{11}\right) = \left(\frac{-1}{11}\right) = -1$, pues 43 es congruente a –1 módulo 11. Luego, $\left(\frac{11}{43}\right) = 1$.

Es decir, existe al menos un entero m, tal que m al cuadrado es congruente a **11** módulo **43**.

Ejemplo

Calculemos $\left(\frac{17}{97}\right)$. Tenemos $\left(\frac{17}{97}\right) = \left(\frac{97}{17}\right)(-1)^{8.48} = \left(\frac{12}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{2}{17}\right)\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right)(-1)^{8} = \left(\frac{2}{3}\right) = -1$

En este ejemplo, hemos usado varias manipulaciones aritméticas sin mencionarlas explícitamente. Por ejemplo, que $\left(\frac{2}{17}\right)\left(\frac{2}{17}\right) = 1$, esto es así porque el símbolo de Legendre vale **1** ó **–1** y, por lo tanto, su cuadrado siempre es **1.**

Como conclusión de este cálculo podemos asegurar que no existe ningún entero m, que al cuadrado sea congruente a **17** módulo **97.**

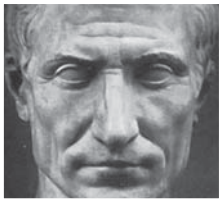
Para resolver

4.18 Listar todos los residuos cuadráticos y los no–residuos cuadráticos módulo p, para p = **13, 17**.

4.19 Decir si las siguientes ecuaciones tienen o no solución.

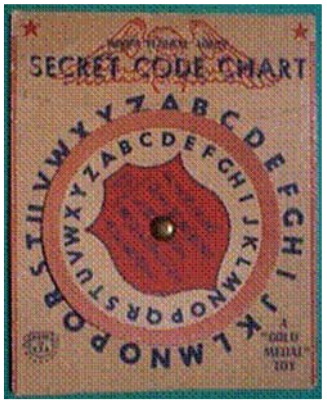
$x^2 \equiv -7 \bmod (13)$ **$5x^2 \equiv 2 \bmod (13)$** **$x^2 \equiv 9 \bmod (23)$**

4.20 Evaluar los siguientes símbolos de Legendre. $\left(\frac{11}{29}\right)$ $\left(\frac{23}{61}\right)$



□ 4.9. Los códigos secretos de Julio César

Ya en la época del Imperio Romano, el envío de mensajes a los ejércitos propios, o a los aliados, sin que fueran interceptados por los enemigos era un problema que desvelaba al emperador. La historia le reconoce a Julio César, entre otros méritos, el de haber inventado un sistema para enviar mensajes que de ser interceptados no podían ser interpretados y sólo podían ser descifrados por sus aliados.



Estos códigos se basan en la aritmética modular con m = 26, el 26 no es casual, es la cantidad de letras del alfabeto (el 26 corresponde a nuestro alfabeto sin dobles ni ñ, cada uno debe usar la cantidad de letras de su propio alfabeto).

En esta sección describiremos la primera versión de estos códigos y otras modificadas, y aún más sofisticadas.

Una idea elemental para codificar mensajes es la de reemplazar cada letra del mensaje original por otra, según un diccionario dado. Tanto el que envía un mensaje, como el que lo recibe, debe conocer el diccionario. Para mantener los mensajes secretos hay que asegurarse que el enemigo no encuentre el diccionario. Hasta aquí, nada de aritmética modular.

Ejemplo

Supongamos que en nuestro diccionario secreto para codificar mensajes tenemos los siguientes reemplazos.

$$a \to g, \qquad e \to j,$$
$$i \to o, \qquad m \to r$$

Supongamos que recibimos el mensaje secreto Ro rgrg rj rorg
Para decodificarlo tenemos que usar los reemplazos inversos

$$g \to a, \qquad j \to e,$$
$$o \to i, \qquad r \to m.$$

Resultado … “mi mamá me mima”.

En este juego de enviar mensajes secretos el tiempo es un factor relevante. El enemigo intentará quebrar nuestro código, y es posible que lo logre después de algún tiempo. Es así que el mantener por mucho tiempo un diccionario fijo puede resultar peligroso. A pesar de que hay muchos diccionarios posibles, tantos como permutaciones de las 26 letras del alfabeto (esto es 26!= 403.291.461.126.605.635.584.000.000) quien intente descubrir uno de estos diccionarios puede ayudarse con algunas verdades del idioma. Por ejemplo, la forma en que se combinan las vocales y las consonantes, de combinaciones prohibidas, de saber qué letras son más frecuentes, etc. Así, con tiempo y luego de interceptar suficiente cantidad de mensajes es posible descubrir el diccionario secreto.

Julio César tuvo la siguiente idea. Propuso considerar el diccionario cíclico que reemplaza a una letra dada por la que está 3 posiciones más adelante, considerando que luego de la z sigue la a. En definitiva propuso considerar un alfabeto cíclico.

Julio César, por alguna razón, eligió el 3. Pero nosotros podríamos, sin más complicaciones, elegir un **m** entre 1 y 25 y reemplazar a cada letra por la que está **m** lugares más adelante en el alfabeto cíclico.

Para ayudar a codificar y decodificar anotamos

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Ejemplo

Tomemos **m = 5** y supongamos que el mensaje a codificar es

TU MAMA TE MIMA

T = 20, luego su reemplazo es 20 + 5 = 25 = Y
U = 21, luego su reemplazo es 21 + 5 = 26 = Z
M = 13, luego su reemplazo es 13 + 5 = 18 = R
….

Así el mensaje codificado es

YZ RFRF YJ RNRF

El mensaje codificado cambia si cambiamos **m** porque estamos cambiando el diccionario.

Veamos que resulta para diversos valores de **m**.

m	TU	MAMA	TE	MIMA
1	UV	NBNB	UF	NJNB
7	AB	THTH	AL	TPTH
15	IJ	BPBP	IT	BXBP
21	OP	HVHV	OZ	HDHV
25	ST	LZLZ	SD	LHLZ

Entonces, Julio César podía elegir un **m** distinto cada vez que había que codificar un mensaje y enviar junto con el mensaje cifrado la llave, es decir el valor de **m**. Quien recibía el mensaje conocía el sistema y, con el valor de **m,** podía decodificar el mensaje recibido.

Ejemplo

El mensajero murió.
El mensaje codificado usando **m = 7** se lee: LS TLUZHQLYV TBYPV

Supongamos que recibimos este mensaje que incluye la llave, en este caso **m = 13**.

NGNPNE RFGN ABPUR AB ABF RFCRENA 13

No debemos olvidar que estamos con la aritmética módulo 26.
N = 14, luego 14 – 13 = 1 = A, es decir N → A
G = 7, luego 7 – 13 = – 6 = 20 = T, es decir G → T
….

Hagamos algo más sistemático. Recordemos el orden de cada letra en el alfabeto.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Ahora hacemos

Codificado	N	G	N	P	N	E		R	F	G	N		A	B	P	U	R
Orden	14	7	14	16	14	5		18	6	7	14		1	2	16	21	18
-13	1	20	1	3	1	18		5	19	20	1		14	15	3	8	5
decodificado	A	T	A	C	A	R		E	S	T	A		N	O	C	H	E

Codificado	A	B		A	B	F		R	F	C	R	E	N	A
Orden	1	2		1	2	6		18	6	3	18	5	14	1
-13	14	15		14	15	19		5	19	16	5	18	1	14
decodificado	N	O		N	O	S		E	S	P	E	R	A	N

¡ATACAR ESTA NOCHE NO NOS ESPERAN!

En algún momento, quizá los mismos romanos, construyeron un aparato para codificar y decodificar mensajes usando estos sistemas. Este consistía de dos platos redondos montados sobre un eje, ambos con las 26 letras del alfabeto ordenadas en sentido horario. Se acomodan los discos de manera tal que las letras A de ambos coincidan. Luego, haciendo girar uno sobre el otro **m** lugares en sentido horario, se lee el diccionario para codificar, mientras que girándolo en sentido antihorario se lee el diccionario para decodificar.

4.21 Codificar el mensaje "Traigan agua y pan", usando **m = 6, 11, y 19**.

4.22 Decodificar el mensaje "HGNKEKVCEKQPGU NQ NQITCUVG", sabiendo que la llave es **m = 2**.

Criptografía

5.

Por Daniel Penazzi

5.1. Introducción

Alicia (en el teléfono): Tengo algo para decirte, Berto.

Berto: Bueno, y ¿por qué no me lo decís?

Alicia: Tengo miedo de que Eva esté escuchando.

Berto: ¡Ah! Bueno, mandámelo por e-mail.

Alicia: ¿Y si también tiene interceptada la línea de Internet?

Berto: Mandámelo encriptado.

Alicia: ¿Y qué uso? ¿El César?

Berto: ¡Ah, Ja Ja! ¡Qué buen chiste! No, escucha, te voy a mandar por e-mail un sistema seguro para que lo uses.

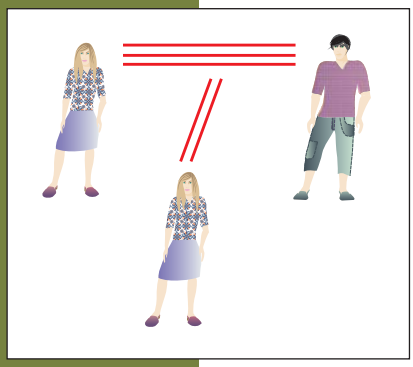
Alicia: Pero Eva puede interceptar todo lo que me mandes.

Berto: No importa que Eva intercepte todo, si seguís mis instrucciones Eva no va a poder saber cuál es el mensaje original que quieres mandarme.

En el capítulo anterior se presentó un esquema para mandar mensajes secretos, basado en las propiedades de la aritmética modular. En este capítulo exploraremos este tópico con más detalle. Analizaremos algunos de los esquemas históricos más conocidos y sus debilidades, y presentaremos una idea, en versión reducida, de cómo son los esquemas actuales que se usan en las transacciones electrónicas para garantizar que los mensajes sólo sean leídos por las personas indicadas y no por otras.

Los personajes principales en esta presentación serán Alicia, Berto y Eva [1].

[1] Se suele utilizar por convención Alicia, Bob y Eva; pero por ser ésta una publicación del Ministerio de Educación de la Nación se adoptó Berto en lugar de Bob.



Alicia desea mandarle un mensaje a Berto. Eva puede estar espiando (por eso se llama Eva. También porque es el Enemigo). Es decir, Alicia puede estar hablando con Berto por teléfono y Eva lo tiene "pinchado" y puede escuchar todo lo que Alicia le dice a Berto. O Alicia le puede estar mandando algo a Berto por correo electrónico; pero la línea por la cual lo manda también puede estar bajo escucha de Eva, grabando todo lo que se manda por ella. O bien Alicia le manda una carta a Berto, pero no puede estar segura de que no será interceptada y leída por Eva.

De cualquier forma, Alicia no puede confiar en que Berto será el único que lea su mensaje. Ahora bien, Alicia y Berto comparten algún secreto. Lo que desean hacer es transformar ese secreto, que en general será un secreto no muy largo, en un secreto más largo (el mensaje que Alicia desea mandarle a Berto). El objetivo de Eva es: o bien saber cuál es el mensaje, o mejor aún, aprender el secreto así podrá leer todos los mensajes entre Alicia y Berto.

Para empezar, es importante definir el vocabulario que usaremos.
El mensaje que Alicia desea mandar suele llamarse el texto plano.
El mensaje que Alicia realmente manda se llama texto cifrado.
El método que Alicia usa para transformar el texto plano en texto cifrado se llama algoritmo, sistema de encriptación o cifrado, o simplemente cifer (a veces también se le llama código, pero la palabra código se usa en general para otras cosas).

□ 5.2. Primera ley de la criptografía

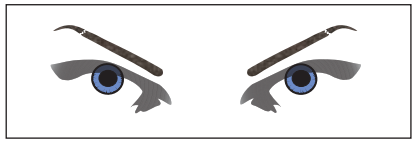
En el capítulo de la aritmética del reloj vimos que César había ideado un esquema para mandar mensajes secretos que consistía en reemplazar cada letra por la letra que estaba a tres lugares de ella en el abecedario.

Si bien para la época parecía espectacular ese esquema, en realidad es muy débil. Las debilidades son varias; pero la principal es que es un sistema cuya seguridad depende de que no se conozca el sistema.

Esto viola una de las reglas cardinales de la criptografía. Mucha gente cree que la seguridad de un sistema radica en que no se conozca el sistema; pero eso es un error.

La primera regla de la criptografía es la siguiente:

Se debe suponer que el adversario tendrá conocimiento del sistema.



En la práctica, ya sea por soborno, ingeniería reversa, o lo que sea, un adversario suele ser capaz de conocer los detalles del sistema si está realmente interesado.

Por lo tanto, un sistema que se base en "seguridad por obscuridad" (es decir que se base en que el

adversario no conoce el sistema) no es seguro. Por ejemplo, si César usaba su sistema para hablar con Pompeyo y con Marco Antonio, y luego Pompeyo se volvía su enemigo, César ya no podía hablar con Marco Antonio sin que se enterara Pompeyo.

Entonces ¿de qué sirve un sistema criptográfico si no se puede mantener en secreto?

Pensemos en el sistema de César. En el capítulo de la aritmética del reloj vimos que el sistema de César es simplemente sumarle 3 a cada letra, módulo 26. También vimos una generalización del sistema de César donde, en vez de sumarle 3 módulo 26, podían sumarle algún otro número módulo 26. Si César hubiera usado ese sistema, podría haber usado, por ejemplo, suma de tres con Pompeyo pero suma con 8 (o cualquier otro número) con Marco Antonio.

En resumen, el sistema "César generalizado" tiene una CLAVE (¿qué número sumar?). Para desencriptarlo no sólo se necesita un conocimiento del sistema en sí, sino también saber cuál es, exactamente, la suma usada.

En general, los sistemas criptográficos deben depender, además del sistema en sí, de una clave relativamente corta y fácil de cambiar (esa clave es el secreto que comparten Alicia y Berto). Esta clave puede variar entre individuos distintos (así, aunque uno sea capturado no compromete la seguridad de los demás) o también variada periódicamente (así, si el enemigo averigua una clave en particular, sólo podrá leer una cantidad limitada en el tiempo de mensajes). Por ejemplo, durante las guerras mundiales se acostumbraba cambiar las claves todos los días (o en vísperas de alguna batalla importante) así, si alguien averiguaba una clave en particular sólo podía leer los mensajes de ese día.

La clave provee una doble medida de seguridad: Eva debe saber no sólo cuál es el sistema usado, sino que aún si lo puede averiguar por algún motivo, debe todavía atravesar la "pared" que significa que el sistema tenga una clave. Por lo tanto, el diseñador de un sistema criptográfico lo debe diseñar **asumiendo** que Eva conocerá todo el diseño, y el diseño debe ser lo suficientemente robusto para que **aún así** Eva no pueda atacarlo si no conoce la clave. Esto no significa que las grandes agencias de seguridad del mundo se apresuren a publicar sus algoritmos en el diario; pero los algoritmos que diseñan son hechos de tal forma que **aún** si fueran publicados en el diario serían seguros.

Este principio fue enunciado por primera vez por Auguste Kherckhoff en 1883. Básicamente, su argumento fue que los sistemas criptográficos deben, en general, ser ampliamente distribuidos (por ejemplo, en una guerra) y engorrosos de cambiar. Si se tuviera que cambiar el sistema cada vez que el enemigo toma conocimiento del mismo (por ejemplo al tomar prisioneros) el costo sería muy alto. Por otro lado, si lo único que hay que cambiar es una clave, (que además puede ser cambiada por ejemplo todos los días) entonces el sistema es, inherentemente, más seguro y robusto. Así, aún si el sistema cae en las manos de los enemigos y está bien construido, el enemigo no debería poder atacarlo. Un buen sistema criptográfico debe ser indescifrable incluso para el diseñador si éste no posee la clave. En cambio, un sistema cuya seguridad dependa sólo de que el enemigo no lo conozca es inherentemente frágil.

Repetimos el principio de Kherckhoff: Se debe suponer que el adversario conoce todo el sistema, y que lo único que ignora es la clave.

En el mundo moderno no militar este principio es todavía más importante. Por ejemplo, para realizar transacciones comerciales entre distintos bancos es necesario que todos tengan el **mismo** sistema, y además, que todo el mundo lo conozca, así cualquiera puede programarlo o construir un dispositivo electrónico que se encargue de realizar las encripciones. Por supuesto, que si el sistema fuese frágil y dependiera de que nadie lo conozca no serviría de nada porque es mucha la gente que **debe** conocerlo. Así, los bancos usan un sistema conocido por todos, pero diseñado con robustez, además no es necesario controlar a todos los programadores, sólo a los pocos que conocen las claves.

Volvamos al sistema de César y recordemos que la modificación vista en el capítulo de la aritmética del reloj tiene una clave. Aún así, este sistema "César modificado" es ridículamente débil.

Para empezar, sólo hay 26 (o 27, si usamos un alfabeto con la Ñ) claves posibles. Esto significa que si alguien sabe que se está encriptando con este método todo lo que tiene que hacer es probar con las 26 ó 27 claves posibles hasta obtener algo que tenga sentido.

Entonces, no sólo debemos tener una clave, sino que el espacio de claves posibles debe ser lo suficientemente grande como para que no sea factible efectuar un ataque testeando todas las claves posibles en un tiempo razonable.

Enunciemos este otro principio básico: El número de claves posibles debe ser lo suficientemente alto como para que no sea práctico testear todas las claves una por una.

¿Qué otras debilidades tiene el sistema de "César extendido"? Aún si no tuviese un espacio de claves chico (podríamos imaginar que tenemos un lenguaje con un alfabeto sumamente grande con muchas letras), tiene otro gran defecto: **si se averigua como se encripta una letra, se averigua como se encriptan todas las letras.**

Es decir, si Eva sabe que por ejemplo N se encripta con X entonces sólo debe hacer X-N=25-14=11 y sabe que la clave usada fue 11, y así puede leer todo el mensaje.

Pero se puede preguntar ¿cómo puede Eva saber que N se encripta con X?

Puede pasar que Eva intercepte parte del mensaje, o lo sepa por ciertas estructuras. Por ejemplo, si sabe que Alicia siempre empieza sus mensajes con la fecha del día, puede saber cómo se encripta parte del mensaje. En noviembre, sabremos que Alicia empezará el mensaje con **NOVIEMBRE**..... de 2...; si Eva intercepta el mensaje cifrado, sabrá que, si empieza con X....., N fue encriptada con X, y podrá leer el resto del mensaje.

En general, hay varios tipos de ataque que Eva puede tratar. El más básico se llama ataque de **texto cifrado conocido.** Se corresponde con el ataque que enunciamos al principio del capítulo: Eva puede interceptar las comunicaciones entre Alicia y Berto, y al poder hacer esto es capaz de leer todo el texto cifrado entre ellos.

Posiblemente sea todo lo que esté al alcance de Eva, pero **no puede suponerse eso.**

Hay situaciones en las que Eva podría hacer más. En general, como en criptografía un exceso de paranoia no le viene mal a nadie, los sistemas se tratan de diseñar asumiendo que el adversario es capaz de hacer más. Una de las cosas que se suele suponer es que Eva podría averiguar, por medios independientes, **parte** del texto plano.

Definición: Un ataque donde Eva conoce todo el texto cifrado y **parte** del texto plano, y en el cuál la tarea de Eva es recobrar el resto del texto plano, o la clave, se llama ataque de **texto plano conocido**.

Eva puede montar un ataque de texto plano conocido por diversos motivos, por ejemplo, podría saber que el comienzo de los mensajes es de una cierta forma.

Otra posibilidad, es que Alicia mande diversos mensajes a Berto y que Eva, por algún motivo, averigüe lo que dice uno de ellos, esto sucedió muchas veces en las guerras. Entonces, Eva tendrá tanto el mensaje cifrado como el mensaje original. El sistema debería ser lo suficientemente robusto como para que aún así, Eva no pueda leer **los otros** mensajes, ni averiguar la clave.

No siempre se pidió este requerimiento a los sistemas criptográficos, pero en la actualidad se da por supuesto.

Un sistema debería ser lo suficientemente robusto para resistir no sólo ataques de texto cifrado conocido, sino también ataques de texto plano conocido.

Volvamos otra vez al sistema de César extendido. Aunque Eva no pueda montar un ataque de texto plano conocido, otra gran debilidad del sistema es que las **distancias** entre las letras no varían.

En el alfabeto, entre la letra A y la letra E hay otras 3 letras (B, C y D). Supongamos que usamos la clave F. Entonces A será encriptada como G, y E será encriptada como K. Entre la letra G y la letra K hay también 3 letras (H, I y J).

¿Por qué esto tiene importancia?

Porque en el idioma castellano, las letras no aparecen con la misma frecuencia. Si uno toma una página de un libro, algunas letras aparecen más que otras. Es menos frecuente que aparezca la letra W o la Z, pero muy común que aparezcan las vocales, o la R, la S, etc.

Las dos letras que aparecen más frecuentemente que las otras son la A y la E. Si se hace un gráfico con la frecuencia de las letras, "salta" a la vista la cantidad de veces que aparecen A y E respecto de las otras. Si encriptamos todo el texto con F, y realizamos un conteo de frecuencia del texto encriptado, se notará un salto importante tanto en la G

como en la K, las cuales están entre sí a la misma distancia que A y E, por lo tanto es fácil deducir que A debe haber sido encriptada con la G y, por lo tanto, la clave es la F.

Supongamos el siguiente texto:

YZDUFYELCPXZDPDELELCOPLWLDECPDJXPOTLPYWLNLDLOPRFTWWP
CXZDTYZGTPYPYALCLWLDNFLECZWZDALDLXZDLMFDNLCCPNTPYPW
DLMLOZ

Si hacemos un conteo de las letras, obtenemos:

A:2 B:0 C:8 D:13 E:5 F:4 G:1 H:0 I:0 J:1 K:0 L:19 M:2
N:4 O:4 P:13 Q:0 R:1 S:0 T:5 U:1 V:0 W:7 X:4 Y:7 Z:8

Las letras más frecuentes son L, P y D, con C y Z bastante menos. De ellas, entre la L y la P hay otras tres letras, por lo tanto es muy probable que L sea la encriptación de A y P la encriptación de E. Entonces, la clave es L-A=K. Si al texto encriptado le restamos K módulo 26 letra a letra, obtenemos:

NOSJUNTAREMOSESTATARDEALASTRESYMEDIAENLACASADEGUILLERMO
SINOVIENENPARALASCUATROLOSPASAMOSABUSCARRECIENELSABADO

y, colocando los espacios:

NOS JUNTAREMOS ESTA TARDE A LAS TRES Y MEDIA EN LA CASA DE
GUILLERMO SI NO VIENEN PARA LAS CUATRO LOS PASAMOS A BUSCAR
RECIEN EL SABADO

Complicando las cosas.

Para resolver los problemas del método de César, se inventaron sistemas más complicados. En ellos cada letra va a otra letra por medio de alguna regla más complicada que sólo sumarle módulo 26, o incluso sin ninguna regla, es decir, seleccionando al azar con qué letra se encripta A, luego seleccionando al azar con qué letra se encripta B, etc.

Por ejemplo, podría decir, A se encripta con D, B se encripta con X, C se encripta con H, D se encripta con Z, E se encripta con G, etc.

La clave sería el mapa completo de dónde va cada letra. Por ejemplo, una clave podría ser:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	X	H	Z	G	Ñ	P	W	E	R	Y	F	T	A	V	Q	B	S	C	I	N	L	J	M	O	U	K

VAMOS A INVADIR sería encriptado como: JDTQI D EAJDZEC

o bien, se podría agrupar de a cuatro para ocultar las estructuras gramaticales:

JDTQ IDEA JDZE C

Podemos preguntarnos ¿Cuántas claves posibles hay? Y podemos contestar, en función de lo visto en el capítulo de combinatoria, lo siguiente:

La letra A puede ir a cualquiera de las 27 letras, por lo tanto tiene 27 posibilidades.

La letra B puede ir a cualquiera de las 27 letras, excepto a la letra que se eligió para A, entonces, tiene 26 posibilidades. La letra C puede ir a cualquiera de las 27 letras, excepto las letras elegidas para A y para B, así tiene 25 posibilidades, etc.

El total de posibilidades es 27.26.25...3.2.1=27!

El resultado es mayor a 10.888.869.450.418.352 billones de posibilidades.

¿Cuánto demoraríamos en testear todas las claves posibles?

Supongamos que tardáramos un segundo por clave sin ninguna interrupción, demoraríamos más de tres trillones de siglos. Aún usando una computadora que permitiera testear mil millones de claves por segundo, demoraríamos más de 345.283.785.211 años. Ciertamente, el espacio de claves es lo suficientemente grande para que no se pueda deducir la clave por fuerza bruta.

Además, como el encriptamiento de la letra A es independiente del de la letra B, y éste independiente de la letra C, etc., aunque el adversario averiguara algunas letras no podría deducir todas. Tampoco es probable que se mantenga la distancia entre letras, así que el conteo no revelaría inmediatamente la clave. Parece que este sistema es entonces muy seguro, pero **no** lo es.

Para empezar, no resiste un ataque de texto plano conocido, porque si Eva logra averiguar suficiente texto plano como para que cada letra, o al menos la mayoría, aparezcan entonces averiguará la clave.

Tampoco resiste un ataque de texto cifrado conocido porque el conteo de frecuencias también se puede aplicar a este sistema y, aunque es engorroso, si hay suficiente texto se puede hacer.

Ejemplo

Supongamos que interceptamos el siguiente mensaje del que sólo sabemos que ha sido encriptado con alguna tabla similar a la anterior, pero no sabemos cuál es entre las 27! Posibilidades:

BIEX HKIE HBHS ŃIIS IWAY IHBS GMGD SGNH SIEZ AWQH EHEZ GZGQ NHGS GEPD ABYH GYIQ NGZH NHSS HXGQ SIES ALQI ECHS URAE VC

Contemos cuántas veces aparece cada letra en ese mensaje. Obtenemos:

A:5 B:4 C:2 D:2 E:9 F:0 G:10 H:13 I:10 J:0 K:1 L:1 M:1
N:4 Ñ:1 O:0 P:1 Q:5 R:1 S:11 T:0 U:1 V:1 W:2 X:2 Y:3 Z:4

Las letras más frecuentes en español son la E y la A. Por lo tanto, es probable que la E haya sido encriptada, de acuerdo con la tabla anterior, como G,H,I o S y lo mismo con A. Podemos tratar primero suponiendo que E fue encriptado como H, que es la más frecuente. Escribamos debajo de cada H del mensaje cifrado una E, para ver que obtenemos:

BIEX HKIE HBHS ÑIIS IWAY IHBS GMGD SGNH SIEZ AWQH EHEZ GZGQ
E E E E E E E

NHGS GEPD ABYH GYIQ NGZH NHSS HXGQ SIES ALQI ECHS URAE VC
E E E E E E

La siguiente letra más frecuente es la S, así que podríamos suponer que la A fue encriptada como S. Si hacemos esa suposición tenemos:

BIEX HKIE HBHS ÑIIS IWAY IHBS GMGD SGNH SIEZ AWQH EHEZ GZGQ
E E EA A E A A EA E E

NHGS GEPD ABYH GYIQ NGZH NHSS HXGQ SIES ALQI ECHS URAE VC
E A E E EAA E A A EA

Tenemos un problema porque hay una secuencia de cuatro letras consecutivas EAAE. Aunque supongamos un corte de palabra entre las dos A, tendríamos una palabra que termine en EA seguida de otra que empieza con AE. Podría ser algo como...VEA AERO.... pero vemos que hay otros dos lugares con la combinación EA. Sabemos que el artículo EL es muy común en español, así que es más probable que sea la L haya sido con S y no con la A.

Ahora asumiremos que L fue a S. La G y la I, que son letras con altas frecuencias, deben ser las encriptaciones de A y O, o al revés. Supongamos primero que A fue a G y O a I. Con estas suposiciones tenemos:

BIEX HKIE HBHS ÑIIS IWAY IHBS GMGD SGNH SIEZ AWQH EHEZ GZGQ
O E O E EL OOL O OE L A A LA E LO E E A A

NHGS GEPD ABYH GYIQ NGZH NHSS HXGQ SIES ALQI ECHS URAE VC
EAL A E A O A E ELL E A LO L O EL

Vemos el segmento EL ?OOLO que trae a la mente la frase EL ZOOLOGICO, además hay otra O tres letras después de la secuencia OOLO. Si estamos en lo correcto, entonces WAY debe ser el encriptamiento de GIC y Ñ debe ser el encriptamiento de Z. Reemplazando entonces tenemos:

BIEX HKIE HBHS ÑIIS IWAY IHBS GMGD SGNH SIEZ AWQH EHEZ GZGQ
O E O E EL ZOOL OGIC OE L A A LA E LO IG E E A A

NHGS GEPD ABYH GYIQ NGZH NHSS HXGQ SIES ALQI ECHS URAE VC
EAL A I CE ACO A E ELL E A LO L I O EL I

Observemos que tenemos que HBHS ŃIIS IWAY I es el encriptamiento de E? EL ZOOLOGICO, y que luego sigue otra vez el par HB que se traduce como E? Y luego tenemos SG que se traduce como LA. Pareciera que HB es EN lo que quedaría EN EL ZOOLOGICO EN LA así que asumamos que B es el encriptamiento de N y tenemos:

BIEX HKIE HBHS ŃIIS IWAY IHBS GMGD SGNH SIEZ AWQH EHEZ GZGQ
NO E O ENEL ZOOL OGIC OENL A A LA E LO IG E E A A

NHGS GEPD ABYH GYIQ NGZH NHSS HXGQ SIES ALQI ECHS URAE VC
EAL A INCE ACO A E ELL E A LO L I O EL I

La frase EN EL ZOOLOGICO EN LA ?A?LA, sugiere que es

EN EL ZOOLOGICO EN LA JAULA, se podría decir que la M es el encriptamiento de la J y la D el encriptamiento de la U. Además, observemos que la letra E tiene una frecuencia de 9, que es bastante alta, y otra de las letras frecuentes del castellano es la S, así que reemplacemos las E por S:

BIEX HKIE HBHS ŃIIS IWAY IHBS GMGD SGNH SIEZ AWQH EHEZ GZGQ
NOS E OS ENEL ZOOL OGIC OENL AJAU LA E LOS IG E SES A A

NHGS GEPD ABYH GYIQ NGZH NHSS HXGQ SIES ALQI ECHS URAE VC
EAL AS U INCE ACO A E ELL E A LOSL I O S EL IS

La oración NOS E OS ENEL ZOOL OGIC OENL AJAU LA E LOS IG E S debe ser NOS VEMOS EN EL ZOOLOGICO EN LA JAULA DE LOS TIGRES.

Así, podemos completar:

BIEX HKIE HBHS ŃIIS IWAY IHBS GMGD SGNH SIEZ AWQH EHEZ GZGQ
NOSV EMOS ENEL ZOOL OGIC OENL AJAU LADE LOST IGRE SEST ATA

NHGS GEPD ABYH GYIQ NGZH NHSS HXGQ SIES ALQI ECHS URAE VC
DEAL AS U INCE ACO DATE DELL EVA LOSL I O S EL IS

Y, podemos deducir que el mensaje es:

NOS VEMOS EN EL ZOOLOGICO EN LA JAULA DE LOS TIGRES ESTA TARDE A LAS QUINCE ACORDATE DE LLEVAR LOS LIBROS ? EL ??IS??

El primer ? (que corresponde con la C) parecería ser la Y, con lo que tendríamos

NOS VEMOS EN EL ZOOLOGICO EN LA JAULA DE LOS TIGRES ESTA TARDE A LAS QUINCE ACORDATE DE LLEVAR LOS LIBROS Y EL ??IS?Y

Si vemos las letras que faltan asignar, terminamos de completar:

NOS VEMOS EN EL ZOOLOGICO EN LA JAULA DE LOS TIGRES ESTA TARDE A LAS QUINCE ACORDATE DE LLEVAR LOS LIBROS Y EL WHISKY

Este fue un ejemplo de un mensaje muy corto. Cuando el mensaje es muy largo, las frecuencias de las letras dirán con mucha seguridad donde se encriptaron la A, la E y las letras más comunes. A partir de allí, con un buen conocimiento del idioma es fácil quebrarlo.

En resumen, no importa que tan compleja sea la substitución, el hecho de que el idioma castellano tiene ciertas regularidades en su estructura y que la frecuencia de las letras no es uniforme, permite descifrar el mensaje si este es lo suficientemente largo. Además, está el problema de que si por algún motivo Eva averigua de alguna forma parte del texto plano, ya averiguó bastante de la clave y es probable que pueda descifrar el texto cifrado.

¿Cómo resolver este problema? La solución consiste en usar bloques más grandes que una letra. El problema en el esquema anterior es que la A siempre se encripta como una G, la E siempre como una H, etc. Pero si tomáramos bloques de dos letras, entonces la A no siempre se encriptaría de la misma forma porque dependería de la que tenga al lado.

Aclaración

Esta es otra lección aprendida a lo largo de la historia de la criptografía:

El tamaño del bloque debe ser lo suficientemente grande como para que un análisis de frecuencia no sea útil, y también lo suficientemente grande como para que sea improbable que una revelación de parte del texto plano revele todos los posibles bloques.

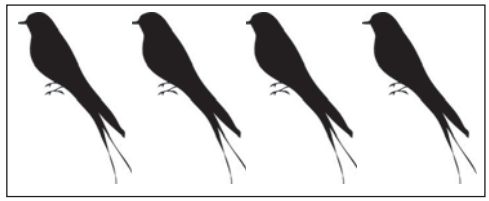
El problema con un bloque de dos letras es que, en vez de guardar una tabla con 27 elementos, debemos guardar una con 27.26/2=351 elementos. Una alternativa sería usar algún sistema que permitiera deducir cuál es el encriptamiento de un par de letras. Como ejemplo daremos el **cifer Playfair** que se usó en Inglaterra a fines del siglo XIX, en realidad hay varias versiones; pero ejemplificaremos sólo con una.

□ 5.3. Sistema Playfair

En este **cifer** basta recordar una palabra o frase clave. Por ejemplo, usaremos como frase clave:

VOLVERAN LAS OSCURAS GOLONDRINAS EN TU BALCON SUS NIDOS A COLGAR.

Tomamos esa frase y la escribimos en un cuadrado con cinco filas de cinco casillas cada una, no volvemos a escribir las letras repetidas.



Al terminar con toda la frase, escribimos las letras que no se usaron en orden alfabético. Consideraremos la I y la J como una sola letra y, como esto fue inventado en Inglaterra, no se toma la Ñ.

V	O	L	E	R
A	N	S	C	U
G	D	I/J	T	B
F	H	K	M	P
Q	W	X	Y	Z

Para encriptarlo se toman pares de letras. Puede suceder que cada par de letras esté en la misma fila, en la misma columna, o en columnas y filas distintas. Veamos cada caso por separado:

En la misma fila: Por ejemplo el par OE.

Se toman las letras a la derecha de cada una de ellas, en este caso LR. También podríamos haber acordado tomar las letras a la izquierda. En ese caso OE se encriptaría con VL. Pero para ejemplificar el cifer fijemos las letras a la derecha.

¿Qué pasa si tenemos por ejemplo el par SU? ¿Cuál es la letra a la derecha de U? Las filas se leen dando la vuelta, es decir, que la letra a la derecha de la U sería la A. Así el par SU se encripta como CA. Otro ejemplo: el par PH se encripta como FK.

En la misma columna: Por ejemplo el par DO.

Se reemplazan por las letras que están debajo de ellas, entendiendo que si estamos en la última fila la letra debajo de ella es la que está en la primera fila. Así, DO se encripta como HN y AQ se encripta como GV.

Ni en la misma ni en la misma columna: Por ejemplo el par AM.

En este caso las letras son dos de los vértices de un rectángulo. Para encriptarlas se toman los otros dos vértices. Si las letras son A y M, la A está en la segunda fila y la primera columna y la M está en la cuarta fila y cuarta columna. Entonces, reemplazamos la A por la letra de la segunda fila pero cuarta columna, es decir la C, y la M por la letra de la cuarta fila pero primera columna, es decir la F.

V	O	L	E	R
A	N	S	**C**	U
G	D	I/J	T	B
F	H	K	**M**	P
Q	W	X	Y	Z

AM → CF

Similarmente, ED se reemplaza con OT:

V	**O**	L	**E**	R
A	N	S	C	U
G	**D**	I/J	**T**	B
F	H	K	M	P
Q	W	X	Y	Z

ED → OT

Para desencriptar hay que hacer las operaciones inversas, es decir, rotar a la derecha si están en la misma fila, o hacia arriba si están en la misma columna, o hacer el cambio mencionado antes si están en distintas filas o columnas.

El único problema es el caso de letras repetidas. Para evitarlo, antes de encriptar hay que agregar una letra muda (por ejemplo la X) entre dos letras iguales, si las letras iguales fueran X, hay que agregar una segunda letra muda, por ejemplo Q. Otro problema, que también se resuelve agre-

gando una letra extra, es que la longitud del mensaje sea impar.

Ejemplos

Encriptemos ATACAREMOS ALABAMA Y MISSISSIPPI.

Si usáramos un cifer de substitución de una letra, se notaría la repetición de las As, Ss e Is. En cambio, con Playfair, se encripta de la siguiente manera:

Se agrupan las letras en grupos de a dos, en el caso de grupos con dos letras iguales, agregamos una X. Obtenemos:

AT AC AR EM OS AL AB AM AY MI SX SI SX SI PX PI

que se encripta:

CG NU UV CY LN SV UG CF CQ KT IL IK IL IK KZ KB

Observar que la A se ha encriptado como C, N, U y S, y se ha encriptado la I como T, K y B, lo que borra bastante un posible análisis de frecuencia de letras. Por otro lado, podemos ver que la S siempre se ha encriptado como I, esto es porque para este caso siempre aparece en combinación con letras de su misma columna; éste es uno de los defectos de Playfair.

Si bien Playfair oculta un poco las frecuencias de las letras, se puede hacer un análisis de frecuencia de **pares** de letras, y aunque se necesita más texto y un análisis más complicado, los criptógrafos pueden quebrar fácilmente un cifer como Playfair. Se necesita un cifer con bloque más grande.

Para resolver

Ejercicios 5.1:

1) Usando Playfair con clave DEJE EL XILOFON EN EL ZOOLOGICO, encriptar MARIA FUE A BUSCAR LA GUITARRA.

2) Usando Playfair con clave ATAHUALPA YUPANQUI, encriptar NOS JUNTAMOS EN LA CASA DE MIGUEL A LAS NUEVE.

□ 5.4. El cifer (supuestamente) indescifrable

Durante algunos siglos hubo un cifer que se consideraba indescifrable, en realidad no lo es, aunque hasta hoy hay quienes siguen sosteniendo esa idea. Es el cifer Vigenere, llamado así por **Blaise de Vigenère** (1523-1596).

Vigenere inventó un cifer que es básicamente el de César con clave variable; **pero** le agregó la idea de **cambiar** la clave de letra a letra.

Por ejemplo, tomando como palabra clave CAMION la primera letra del texto se encripta sumando C, la segunda sumando A, la tercera sumando M, la cuarta sumando I, la quinta sumando O, la sexta sumando N, y se vuelve a empezar: la séptima se encripta usando C, la octava con A, etc. Por ejemplo, para encriptar ATACAREMOS ALABAMA Y MISSISSIPPI con la palabra clave CAMION, si ignoramos la Ñ, es decir módulo 26 tenemos:

A	T	A	C	A	R	E	M	O	S	A	L	A	B	A	M	A	Y	M	I	S	S	I	S	S	I	P	P	I
C	A	M	I	O	N	C	A	M	I	O	N	C	A	M	I	O	N	C	A	M	I	O	N	C	A	M	I	O
D	U	N	L	P	F	H	N	B	B	P	Z	D	C	N	V	P	M	P	J	F	B	X	G	V	J	C	Y	X

Si escribimos el mensaje cifrado en grupos de cinco letras para mejor lectura tenemos:
DUNLP FHNBB PZDCN VPMPJ FBXGV JCYX

Vemos que la misma letra se encripta de diversas formas. Es necesario hacer un análisis de frecuencia de bloques de 6 letras, o más si la palabra clave es más larga, lo que era completamente impracticable, por eso se lo consideraba el cifer indescifrable.

Pero no lo es, aunque sí es cierto que se necesita interceptar más texto para quebrarlo.

Por ejemplo, observemos que la A se encripta como D, N, P, P otra vez y N otra vez. Las dos veces que se encripta como P es porque en dos lugares distintos coincide una A con la O de camión. Si se tiene suficiente texto, estas coincidencias van a aparecer. Básicamente, lo que sucede es que se está encriptando las letras 1, 7, 13, 19, etc, todas con la misma clave (C en nuestro caso). Si tenemos un número suficiente de texto, y sabemos la longitud de la clave, podemos simplemente tomar todas esas letras (las que están en posición congruente a 1 módulo 6) y aplicarles un análisis de frecuencia a **ese** texto. Como se trata de un cifrado tipo César, ni siquiera hace falta mucho trabajo porque, como vimos antes, una vez que se sabe dónde va una letra se sabe el lugar de todas. Aunque queda el problema de saber la longitud de la clave, también hay técnicas para deducirla.

Ejemplo

Las operaciones serán todas módulo 26, es decir, sin la Ñ.

Supongamos que se encuentra el siguiente mensaje y que, además, se supone que fue encriptado con Vigenere y se quiere desencriptar:

AXLEBOTFPJOIAVNYHASWAXHEAWJFGXJYJEAAQLIBKWGIUYFBSWYTFIBPJLI-
BKWGIBPFWRCAWJEMKJFIULFJUDASSGRKSSPMAQSWLWYSVJPFKHNHNYYJVZHEA
WUGHNNJFGXJYJEAAXWKAWSLIBKWGHNXJTYBYFJYWWWTSUYJJGJZJDEPWWYE
WPFVIUZNSFUKVMICASYEDJIAFDFTHEAAHAHXWZFEBPWGRJQYSFJFFFHXOJVIDJF
ESCKHAGUAYSNDOYGEKWOGHNHFJYNZFLVJOJJEMAQSQXPTUMLHJLEQWDMRQQ
JUSNJJKIQQJUSNJHGRCNFJEDJRSTJONYEUWXARBPWMGLETFIBZJDQJLFWWJOQSW
UHJNEAWSSPVAIASMAQTSBMZWGXHNFHJJYWGXJQSWLWYSVJPFKLJOYSYWHZYE
AIFJGJZTUSWQSSBYAWGIBASGIBAQDYPWWVSWZJKINJHMIWPWSIUYFBSWYTFIUP
JKSAKIWWMAJKIUQLSVMAGWGJINFEAACSGCWRWRCAUSWXOMSGRWJDRXNYWP
DALGHXXQSVHYFEMWWWHEBKXZELEFWPNOYWEUHNVIKAWAENJHGRCNFJWNB
WWRCAFGXAKFJFXHHSZNWQHMNZJDQRORGEUHNWRLKSLVJNFGXAKRSTJMZWG
XINWRIWJFYWWCQXNNRARJASMRJVQSBMKSVILKRAIWVFWWUWRAWVWCVSWZ
JLIAINFEKWJDSCNTEEYWFKMZQJNYNHASENOJDYPWWQWRCFWWCASMIEKRSTJH

ZWKXZJIYNHQWKDAFDEIZJTIAWHSQRJFJTJOTKLJYNSIUOZJCUQJYSYWXGWQWH
AENHTWWCAFZSAWXAIBPFSVAEGSHNHHSNXJIWPCAXGVXZJTILWASVJLWGBRIFV
EVASLIVAYJSBASHVXBZFHRZFVTJNFDYNCTHSMAWWBCNFWVNHHSNXJUWVXAX
LINOYSGNNWSHXYTFYWYFFHJZTUSWYTEFRJFUMXJQSGUWAWHNHFUSVXNFELE
TFWNZJVYLAZKEWZTVSBLFDEKNFKGUWAWWUWUJMVAWSGUWAWIBHFEMBIFUP
JRJIYNJJUIBEYSTJNFDINNJKXNIJFWJFJSWRMZWWRQXLIMAXLEUADWRMKJKXNIJ
FWJFJQEUWXSFNHFKIPQSVEYWQSFAWHDEEAJKHNOTPMANNTSWQHDIRYTMWJN
QSGUWAWHNOTPMANNTSWQHDIRYTUSVKHDEEAIWYWIJLSMKUDEHBFAVYWWSI
WYWATCWWDEXPWSTJHFTVJYQSZNAQJIBQQLEMKJKPJYQSZNMZWPNLJJQRPNJEJ
XWAVNHHSNXJIWPCAXGVXXZWRJOZWVCA

Lo primero que debemos hacer es tratar de encontrar la longitud de la clave. Hay varios métodos para ello, pero usaremos uno de los más simples: busquemos coincidencias, es decir, cadenas de letras iguales. En general, si la cadena es muy larga, es improbable que se haya producido meramente por azar y estará apuntando a que un segmento idéntico del texto fue encriptado con el mismo segmento de la clave, lo que nos permitirá encontrar la longitud. Después de mirar un rato... Vemos: que la cadena LIBKWG se repite dos veces, la cadena QQJUSNJ se repite una vez, la cadena NHHSNXJ se repite dos veces, y también que la cadena más larga HNOTPMANNTSWQHDIRYT se repite una vez. También se observa que se repiten cadenas más cortas, pero es mejor tener en cuenta las cadenas más largas.

AXLEBOTFPJOIAVNYHASWAXHEAWJFGXJYJEAAQLIBKWGIUYFBSWYTFIBPJLI-
BKWGIBPFWRCAWJEMKJFIULFJUDASSGRKSSPMAQSWLWYSVJPFKHNHNYYJVZHEA
WUGHNNJFGXJYJEAAXWKAWSLIBKWGHNXJTYBYFJYWWWTSUYJJGJZJDEPWWYE
WPFVIUZNSFUKVMICASYEDJIAFDFTHEAAHAHXWZFEBPWGRJQYSFJFFFHXOJVIDJF
ESCKHAGUAYSNDOYGEKWOGHNHFJYNZFLVJOJJEMAQSQXPTUMLHJLEQWDMRQQ
JUSNJJKIQQJUSNJHGRCNFJEDJRSTJONYEUWXARBPWMGLETFIBZJDQJLFWWJOQSW
UHJNEAWSSPVAIASMAQTSBMZWGXHNFHJJYWGXJQSWLWYSVJPFKLJOYSYWHZYE
AIFJGJZTUSWQSSBYAWGIBASGIBAQDYPWWVSWZJKINJHMIWPWSIUYFBSWYTFIUP
JKSAKIWWMAJKIUQLSVMAGWGJINFEAACSGCWRWRCAUSWXOMSGRWJDRXNYWP
DALGHXXQSVHYFEMWWWHEBKXZELEFWPNOYWEUHNVIKAWAENJHGRCNFJWNB
WWRCAFGXAKFJFXHHSZNWQHMNZJDQRORGEUHNWRLKSLVJNFGXAKRSTJMZWG
XINWRIWJFYWWCQXNNRARJASMRJVQSBMKSVILKRAIWVFWWUWRAWVWCVSWZ
JLIAINFEKWJDSCNTEEYWFKMZQJNYNHASENOJDYPWWQWRCFWWCASMIEKRSTJH
ZWKXZJIYNHQWKDAFDEIZJTIAWHSQRJFJTJOTKLJYNSIUOZJCUQJYSYWXGWQWH
AENHTWWCAFZSAWXAIBPFSVAEGSHNHHSNXJIWPCAXGVXZJTILWASVJLWGBRIFV
EVASLIVAYJSBASHVXBZFHRZFVTJNFDYNCTHSMAWWBCNFWVNHHSNXJUWVXAX
LINOYSGNNWSHXYTFYWYFFHJZTUSWYTEFRJFUMXJQSGUWAWHNHFUSVXNFELE
TFWNZJVYLAZKEWZTVSBLFDEKNFKGUWAWWUWUJMVAWSGUWAWIBHFEMBIFUP
JRJIYNJJUIBEYSTJNFDINNJKXNIJFWJFJSWRMZWWRQXLIMAXLEUADWRMKJKXNIJ
FWJFJQEUWXSFNHFKIPQSVEYWQSFAWHDEEAJKHNOTPMANNTSWQHDIRYTMWJN
QSGUWAWHNOTPMANNTSWQHDIRYTUSVKHDEEAIWYWIJLSMKUDEHBFAVYWWSI
WYWATCWWDEXPWSTJHFTVJYQSZNAQJIBQQLEMKJKPJYQSZNMZWPNLJJQRPNJEJ
XWAVNHHSNXJIWPCAXGVXXZWRJOZWVCA

Vemos que hay una diferencia de 20 letras entre el comienzo del primer LIBKWG y el comienzo del segundo, y una diferencia de 85 letras entre el segundo y el tercero. Hay una

diferencia de 10 entre el principio del primer QQJUSNJ y el segundo. Entre el primer NHHSNXJ y el segundo hay una diferencia de 80 y, entre éste y el tercero, hay 375 letras. Entre el primer HNOTPMANNTSWQHDIRYT y el segundo hay una diferencia de 30.

El máximo común divisor entre 20, 85, 10, 80, 375 y 30 es 5. Entonces, dividimos el mensaje tomando las letras que están en posiciones congruentes a 1 módulo 5, luego las congruentes a 2 módulo 5, etc. Con las letras que están en posiciones congruentes a 1 módulo 5 hacemos un conteo y obtenemos:

A:42 B:3 C:2 D:0 E:5 F:4 G:0 H:20 I:9 J:18 K:19 L:5 M:4
N:16 O:18 P:13 Q:12 R:1 S:0 T:0 U:0 V:3 W:39 X:5 Y:17 Z:15

Las letras más frecuentes son A y W, que aparecen casi el doble de veces que la que les sigue en tercer lugar. Además, entre la W y la A hay tres letras (X,Y y Z) contando en forma circular. Esto es un fuerte indicio que la letra W del texto cifrado es en realidad el encriptamiento de la letra A del texto original, y que la letra A del texto cifrado es el encriptamiento de la letra E del texto original. Para que A se encripte como W la clave de las letras congruentes a 1 módulo 5 debe ser V.

Hacemos el mismo conteo, con las letras que son congruentes a 2 módulo 5, obtenemos:

A:6 B:0 C:3 D:2 E:0 F:43 G:2 H:16 I:7 J:42 K:0 L:2 M:1
N:14 O:1 P:0 Q:18 R:8 S:14 T:20 U:5 V:1 W:24 X:13 Y:14 Z:13

Vemos que las letras más frecuentes, y separadas por tres letras en el medio, son F y J. Así que la A debe haber sido encriptada como F, con lo cual la clave de las letras congruentes a 2 módulo 5 es E.

Veamos ahora las congruentes a 3 módulo 5. Contando:

A:16 B:2 C:0 D:17 E:5 F:20 G:19 H:7 I:2 J:19 K:15 L:14 M:7
N:2 O:0 P:2 Q:3 R:0 S:47 T:8 U:10 V:11 W:35 X:0 Y:6 Z:2

y ahí vemos un salto grande en S y W, también separadas por tres letras. Así que, A debe haber sido encriptada como S, la clave es R.

Para las congruentes a 4 módulo 5 tenemos:

A:0 B:4 C:1 D:0 E:42 F:7 G:18 H:15 I:39 J:0 K:3 L:2 M:9
N:4 O:0 P:10 Q:5 R:15 S:25 T:8 U:1 V:18 W:20 X:5 Y:15 Z:3

y ahí el salto se ve en E y en I, con tres letras en el medio. Para que A se encripte como E la clave debe haber sido D.

Finalmente, para las congruentes a 5 módulo 5:

A:19 B:21 C:16 D:8 E:3 F:0 G:0 H:2 I:2 J:35 K:4 L:10 M:12
N:37 O:0 P:4 Q:4 R:13 S:0 T:0 U:23 V:7 W:20 X:23 Y:5 Z:1

Vemos un salto de las frecuencias en J y N, separadas por tres letras, lo que indica que A fue encriptada como J, es decir, la clave es I.

Vemos que la clave completa es VERDI.

Si hacemos Vigenere restando esa palabra del texto cifrado obtenemos:

ESTASSONLASDIRECCIONESPARAENCONTRARELTESOROELCAJONCONESTETESO-
ROESTAENTERRADOENELPARQUENACIONALDELASCATARATASDELIGUAZUPARAP
ODERENCONTRARESEGRANTESORODEBEBUSCARUNARBOLCERCADELAGARGANT
ADELDIABLOQUETENGAUNDIBUJOPARECIDOAUNASTRONAUTABAJANDOSEDEUN
AMOTOCICLETAJUSTOABAJODELARUEDATRASERADELAMOTOCICLETAHAYUNHU
ECOENESEHUECOENCONTRARAUNMAPASIGALASINSTRUCCIONESDELMAPAESASL
ASLLEVARANALMEDIODELBOSQUECOLINDANTECONLASCATARATASHASTAUNLU
GARMARCADOCONUNAXPEROESENOESELLUGARDONDESEENCUENTRAELCAJONC
ONELTESORODESDEESELUGARDEBECAMINAREXACTAMENTEPASOSHACIAELNORT
ELUEGODOBLARYCAMINARPASOSHACIAELESTEALLIDEBERIAENCONTRARSEFREN
TEAOTROARBOLCAVEALPIEDELMISMOALLIENCONTRARAOTROMAPAQUECOMIEN
ZAENUNAXYTERMINAENUNAZLAXDONDECOMIENZAESLAMISMAXDONDETERMIN
ABAELOTROMAPAASIQUEVUELVAAESELUGARYSIGAESTENUEVOMAPALUEGODEQ
UELLEGUEALAZDEBERACAMINARPASOSHACIAELSURYLUEGOPASOSHACIAELOES
TEAHORASIESTAARRIBADELCAJONDELTESORODEBECAVARAPROXIMADAMENTEM
ETROSENPROFUNDIDADPARALUEGOPODEREXTRAERELCAJONPEROESTEESTACER
RADOCONUNCANDADOCONCOMBINACIONLACLAVEDELACOMBINACIONSEDEDUC
EUSANDODOSPALABRASCLAVESLAPRIMERACLAVEESLAMISMACLAVEQUENECESIT
APARALEERESTEMENSAJEASIQUESIUSTEDESTALEYENDOESTEMENSAJEYALASABE
LASEGUNDAPALABRACLAVEESDESOXIRRIBONUCLEICOUSARLACLAVEDESOXIRRI
BONUCLEICOCOMOCLAVEDEUNMETODOPLAYFAIRPARAENCRIPTARLAOTRAPALAB
RACLAVEELRESULTADOESLACLAVEQUELEPERMITIRAABRIRELCAJONDELTESORO
BUENASUERTE

o bien, más legible:

ESTAS SON LAS DIRECCIONES PARA ENCONTRAR EL TESORO EL CAJON CON ESTE TESORO ESTA ENTERRADO EN EL PARQUE NACIONAL DE LAS CATARATAS DEL IGUAZU PARA PODER ENCONTRAR ESE GRAN TESORO DEBE BUSCAR UN ARBOL CERCA DE LA GARGANTA DEL DIABLO QUE TENGA UN DIBUJO PARECIDO A UN ASTRONAUTA BAJANDOSE DE UNA MOTOCICLETA JUSTO ABAJO DE LA RUEDA TRASERA DE LA MOTOCICLETA HAY UN HUECO EN ESE HUECO ENCONTRARA UN MAPA SIGA LAS INSTRUCCIONES DEL MAPA ESAS LAS LLEVARAN AL MEDIO DEL BOSQUE COLINDANTE CON LAS CATARATAS HASTA UN LUGAR MARCADO CON UNA X PERO ESE NO ES EL LUGAR DONDE SE ENCUENTRA EL CAJON CON EL TESORO DESDE ESE LUGAR DEBE CAMINAR EXACTAMENTE PASOS HACIA EL NORTE LUEGO DOBLAR Y CAMINAR PASOS HACIA EL ESTE ALLI DEBERIA ENCONTRARSE FRENTE A OTRO ARBOL CAVE AL PIE DEL MISMO ALLI ENCONTRARA OTRO MAPA QUE COMIENZA EN UNA X Y TERMINA EN UNA Z LA X DONDE COMIENZA ES LA MISMA X DONDE TERMI-

NABA EL OTRO MAPA ASI QUE VUELVA A ESE LUGAR Y SIGA ESTE NUEVO MAPA LUEGO DE QUE LLEGUE A LA Z DEBERA CAMINAR PASOS HACIA EL SUR Y LUEGO PASOS HACIA EL OESTE AHORA SI ESTA ARRIBA DEL CAJON DEL TESORO DEBE CAVAR APROXIMADAMENTE METROS EN PROFUNDIDAD PARA LUEGO PODER EXTRAER EL CAJON PERO ESTE ESTA CERRADO CON UN CANDADO CON COMBINACION LA CLAVE DE LA COMBINACION SE DEDUCE USANDO DOS PALABRAS CLAVES LA PRIMERA CLAVE ES LA MISMA CLAVE QUE NECESITA PARA LEER ESTE MENSAJE ASI QUE SI USTED ESTA LEYENDO ESTE MENSAJE YA LA SABE LA SEGUNDA PALABRA CLAVE ES DESOXIRRIBONUCLEICO USAR LA CLAVE DESOXIRRIBONUCLEICO COMO CLAVE DE UN METODO PLAYFAIR PARA ENCRIPTAR LA OTRA PALABRA CLAVE EL RESULTADO ES LA CLAVE QUE LE PERMITIRA ABRIR EL CAJON DEL TESORO BUENA SUERTE

Obviamente, debe haber otro mensaje diciendo exactamente cuántos pasos caminar y cuántos metros cavar.

En el ejemplo anterior dedujimos la longitud de la clave buscando coincidencias, que no suelen ser tan fáciles de encontrar. Luego, dedujimos la clave simplemente haciendo el conteo de frecuencias y reconociendo el doble salto de la A y la E.

Pero en realidad, si uno sospecha que la clave tiene una longitud más o menos razonable (digamos menos de 10 -12 caracteres), ese segundo método basta. Simplemente, vamos asumiendo que la longitud de la clave es 2, 3, 4 etc. y haciendo un conteo módulo esos números. En cuanto encontremos la longitud correcta aparecerá el doble salto en la frecuencia de las letras.

El problema con Vigenere es que básicamente está encriptando en bloques de, por ejemplo cinco letras, pero no trata al bloque como un bloque compacto, sino que lo que le pasa a la primera letra es independiente de lo que le pasa a la segunda letra, e independiente de lo que le pasa a la tercera letra, etc. Comparemos esto con el cifer Playfair, en el que el bloque se comporta como tal y no se puede partir en sub-bloques de a uno. Una lección aprendida de Vigenere, es que todas las componentes del bloque deben interactuar unas con otras.

AGRANDANDO EL BLOQUE

Vimos que Playfair realmente trata a su bloque de dos letras como un bloque, mientras que Vigenere no. Pero un bloque de dos letras es un tanto chico.

A un norteamericano llamado Lester S. Hill se le ocurrió en 1929 un método ingenioso para conseguir un bloque grande sin mucho esfuerzo. En vez de usar sólo sumas modulares, también utiliza productos modulares.

Ejemplo con un bloque de 4 letras:

Supongamos que queremos encriptar ABCD. Para eso se necesita una palabra clave de 4 letras, por ejemplo NEMO. Entonces, se multiplica (módulo 27 o módulo 26, dependiendo si se usa o no la Ñ) A por N, B por E, C por M y D por O y se suman esos resultados. Supongamos que usamos el alfabeto con la Ñ, las operaciones son módulo 27. La numeración que será: A=1, B=2, ..., X=25, Y=26, Z=0. Entonces:

A por N= 1x14=14.
B por E= 2x5=10.
C por M=3x13=39 pero módulo 27 tengo 39=12.
D por O=4x16=64, pero módulo 27 tengo 64=10.

Luego, sumamos esos resultados parciales:
14+10+12+10=46, y módulo 27 tenemos 46=19=R.

Así, el encriptamiento de ABCD con NEMO da la letra R.

Pero el texto cifrado debería dar un bloque de 4 letras, no una sola. Esta es sólo la primera letra del bloque cifrado. Para obtener las otras tres, se necesitan tres palabras claves más. Es decir, para poder encriptar un bloque de 4 letras, se necesita un total de 4 palabras claves de 4 letras cada una o, también es válido, una palabra clave de 16 letras.

Por ejemplo, supongamos que uso la clave NEMOCAMINOSEGURO.

Las ordeno tomando de a cuatro letras:

N	E	M	O
C	A	M	I
N	O	S	E
G	U	R	O

Esta disposición de las letras (en realidad, de los números que representan las letras) se llama una matriz.

La primera fila de la matriz dará la primera letra del encriptamiento, la segunda fila la segunda letra, etc. Ya vimos que encriptar ABCD con NEMO da la letra R.

De la misma forma, tenemos que usar la palabra CAMI para obtener la segunda letra:

A por C= 1x3=3.
B por A= 2x1=2.
C por M=3x13=39 módulo 27 =12.
D por I=4x9=36 módulo 27 =9.

Sumamos esos resultados parciales: 3+2+12+9=26, y que la segunda letra es Y.

Para la tercera letra hacemos lo mismo con NOSE y para la cuarta con GURO, y obtenemos que ABCD se encripta con RYQJ.

Veamos un ejemplo más extenso:

Supongamos que queremos encriptar ANDA HACIA ESE ANDEN.

Si dividimos en grupos de 4, tenemos los grupos ANDA HACI AESE ANDE N
Para que queden 4, agregamos tres X al final de todo:

ANDA HACI AESE ANDE NXXX

Observar que tenemos varias A, E, e incluso tenemos dos veces el grupo de tres letras AND. Si hacemos todas las operaciones, esto queda encriptado como:

PWYB CJPI AOFJ ZFRL SVFK

Las letras A se encriptaron como P, B, J, A y Z. Las letras E como O, J y L. Las letras N como W, F y S. Es más, ANDA y ANDE tan parecidas, se encriptaron como PWYB en un caso y ZFRL en el otro.

Ahora, ¿cómo desencriptamos?

Si bien no se desarrollarán todos los detalles, aclaramos que mediante operaciones matemáticas a partir de la matriz, se obtiene la matriz inversa. Mediante operaciones de suma y multiplicación aplicadas al texto cifrado, obtendremos el texto original.

En nuestro ejemplo, la inversa (módulo 27) es:

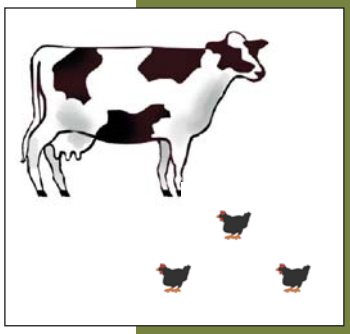
MWRC
Z I HK
FGDD
YKHQ

Aclaración: no todas las matrices tienen inversa. Como no se desarrolla en el texto cómo obtener la inversa de la matriz, anticipamos que la que se plantea aquí, sí la tiene.

Justamente, un problema del método de Hill, es que depende de que la clave tenga inversa. Si no la tiene, el sistema no sirve para encriptar.

Salvo por este problema, el cifer de Hill mezcla bien las palabras, la clave es lo suficientemente grande y el bloque también, al menos para la época en que lo inventó. Sin embargo, Hill tiene una falla fatal.

Explicar en detalle la falta, excede las posibilidades de este libro, pero sí se expondrá el concepto de esa falta.



Para explicarlo, nos situaremos en una granja. Estando allí, vemos que sólo hay vacas y gallinas. Supongamos que le preguntamos al dueño cuántas gallinas y cuántas vacas tiene.

Responde que tiene 22 animales, que todos están sanos y enteros, y que entre todos ellos hay 48 patas. ¿Cómo averiguar lo que preguntamos?

Si llamamos G al número de gallinas y V al número de vacas, entonces G+V=22. Por otro lado, como las gallinas tienen 2 patas y las vacas 4, y todos los animales están sanos y enteros, 2G+4V=48. Esto se puede expresar como un **sistema** de dos ecuaciones con dos incógnitas:

$$G+V=22$$
$$2G+4V=48$$

Dividimos la segunda ecuación por 2, obteniendo:

$$G+V=22$$
$$G+2V=24$$

Restamos a la segunda ecuación la primera:

$$G+2V-(G+V)=24-22, \text{ es decir, } V=2$$

Sabemos que el dueño tiene 2 vacas. Entonces, de la ecuación G+V=22 debe tener 20 gallinas.

¿Qué tiene que ver todo esto con el sistema Hill?

Utilizamos ese ejemplo, para ver que era un caso de resolución de ecuaciones lineales. El caso es que todo el sistema de Hill es lineal. En el caso de un bloque de, digamos, 4 letras todo lo que el atacante necesita son 4 textos cifrados, más sus 4 correspondientes textos originales. Si esos textos satisfacen la condición de independencia lineal (que no desarrollaremos en este texto), entonces el atacante puede escribir un sistema de ecuaciones que le permite calcular todas las palabras claves.

La lección que aprendieron los criptógrafos del sistema de Hill es que: Todo buen sistema necesita alguna no linealidad.

JUNTANDO LAS LECCIONES

Veremos un sistema que aplica todas las lecciones aprendidas. Es un sistema con un bloque no muy grande, para que podamos seguir las ideas, así que es probablemente más o menos fácilmente rompible con computadoras. Sin embargo, nos sentará las bases para entender otro sistema muy bueno.

La idea básica es: **Hill es muy bueno en mezclar las letras, pero es lineal.**

Una substitución letra a letra puede hacerse no lineal, pero al ser letra a letra permite un análisis de frecuencia.

Entonces, podemos preguntarnos ¿Qué tal combinar los dos sistemas?

Es decir, hacer una substitución letra a letra, y luego combinarlas con Hill. Hill se encargará de que no se pueda hacer el análisis de frecuencia y la substitución, si está bien elegida, prevendrá el ataque mediante ecuaciones lineales.

Esta idea es muy buena, tanto que se utiliza en casi todos los cifers modernos.

¿Cuál será la clave?
Un sistema bastante seguro tendría la clave involucrada tanto en la substitución letra a le-

tra, como en la matriz de Hill. Ahora bien, queremos estar seguros de que la substitución tenga suficiente no linealidad, entonces (con mayor razón si vamos a dejar que el usuario del sistema elija sus claves) debemos descomponer la substitución en dos partes: una no secreta pero que asegure no linealidad, y otra secreta. Combinaremos un cifer Vigenere con clave secreta, con un cifer no lineal sin clave. La clave será simplemente la clave de Vigenere.

En cuanto a la matriz de Hill, recordemos que debe ser invertible.
Si la dejamos a merced de una clave, ésta debería ser muy bien elegida. Pero si queremos que lo utilice cualquiera, podríamos usar una matriz fija y luego una mezcla tipo Vigenere al final.

Para ejemplificar, tomaremos un bloque de 4 letras.
Nuestra clave será de 8 letras (incluyendo la Ñ, el espacio y el punto), para un total de 29 letras. Éste es un sistema que una computadora podría quebrar en un par de horas o menos por fuerza bruta, porque 8 letras de este tipo son un poco menos de 39 bits. Así que, para evitar el quiebre, lo complicaremos un poco más.

Asignamos A=1, B=2, ..., Z=27, espacio =28, punto =0. Lo primero que haremos será pasar por un Vigenere con nuestro bloque de 4 letras, más las primeras 4 letras de la clave. Luego, por la substitución no lineal fija, a continuación por el cifer Hill, y finalmente una última encriptación Vigenere para ocultar el paso por Hill.

Texto original
Vigenere
Substitución no lineal
Hill
Vigenere

Tomamos la misma matriz de Hill que antes, pero las operaciones serán módulo 29. La substitución no lineal será la siguiente: (el espacio en blanco está expresado con _).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	_	.
C	P	L	W	H	G	Z	M	Ñ	E	J	R	K	.	D	U	N	V	_	Q	S	F	Y	X	I	T	O	A	B

Ésta es una substitución no lineal más o menos arbitraria, podría ser otra mientras sea no lineal. Más abajo, se mostrará por qué ésta sería una buena elección, pero en realidad no importa mucho para el propósito de ilustrar el sistema.

Veamos un **ejemplo.** Supongamos que queremos volver a encriptar:
ATACAREMOS ALABAMA Y MISSISSIPPI.

Usaremos como claves AZUL y REMO.

Primero debemos dividir el mensaje en bloques de cuatro, ahora podemos usar los espacios:

ATAC AREM OS_A LABA MA_Y _MIS SISS IPPI.

Veamos paso a paso el primer bloque:

Texto	A	T	A	C
Clave Vigenere	A	Z	U	L
Resultado intermedio	B	R	V	Ñ
Substitución no lineal	P	_	Y	D
Hill	Y	Q	H	P
Clave Vigenere	R	E	M	O
Resultado final	O	V	T	D

Veamos de la misma forma los otros:

(1)

Texto	A	R	E	M
Clave Vigenere	A	Z	U	L
Resultado intermedio	B	P	Z	X
Substitución no lineal	P	N	O	I
Hill	U	F	Ñ	E
Clave Vigenere	R	E	M	O
Resultado final	L	K	_	T

(3)

Texto	L	A	B	A
Clave Vigenere	A	Z	U	L
Resultado intermedio	M	_	W	M
Substitución no lineal	K	A	X	K
Hill	U	V	.	X
Clave Vigenere	R	E	M	O
Resultado final	L	_	M	L

(5)

Texto	_	M	I	S
Clave Vigenere	A	Z	U	L
Resultado intermedio	.	K	B	C
Substitución no lineal	B	J	P	L
Hill	Z	Y	H	W
Clave Vigenere	R	E	M	O
Resultado final	P	B	T	K

Por lo tanto, el mensaje cifrado es:

VTDLKTLVPOLMLBWKSPBTKÑW
RSKJMM

¿Cómo se desencripta?

(2)

Texto	O	S	_	A
Clave Vigenere	A	Z	U	L
Resultado intermedio	P	Q	T	M
Substitución no lineal	N	V	S	K
Hill	U	Q	D	.
Clave Vigenere	R	E	M	O
Resultado final	L	V	P	O

(4)

Texto	M	A	_	Y
Clave Vigenere	A	Z	U	L
Resultado intermedio	N	_	T	I
Substitución no lineal	.	A	S	Ñ
Hill	L	R	Z	D
Clave Vigenere	R	E	M	O
Resultado final	B	W	K	S

(6)

Texto	S	I	S	S
Clave Vigenere	A	Z	U	L
Resultado intermedio	T	E	M	C
Substitución no lineal	S	Z	K	L
Hill	X	R	F	D
Clave Vigenere	R	E	M	O
Resultado final	Ñ	W	R	S

(7)

Texto	I	P	P	I
Clave Vigenere	A	Z	U	L
Resultado intermedio	J	Ñ	J	B
Substitución no lineal	E	D	E	P
Hill	T	E	.	Y
Clave Vigenere	R	E	M	O
Resultado final	K	J	M	M

Simplemente hay que hacer las operaciones en orden inverso: es decir, primero restar la segunda clave Vigenere, luego multiplicar por la inversa de Hill, luego hacer la substitución inversa y finalmente restar la primera clave Vigenere. La matriz de Hill inversa (módulo 29) es:

WÑGZ
U I KM
I TF R
LXSD

La tabla de substitución inversa es:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	_	.
_	.	A	Ñ	J	U	F	E	X	K	M	C	H	P	I	Z	B	U	L	T	Y	O	Q	D	W	V	G	R	N

Bien, hasta aquí la descripción del sistema.
La tabla de substitución no lineal que está dada arriba es, como se ha dicho, más o menos arbitraria. A continuación, mostramos qué ideas se usaron para construirla y cómo podría construirse una tabla propia en forma similar. Algunas de las ideas introducidas abajo serán usadas, más adelante, para otro tema.

Primero veamos un poco de ecuaciones.

Las ecuaciones que nos interesan son de la forma aX=1. En ese caso, la solución es X=1/a. (salvo que a=0, en cuyo caso no tiene solución).

¿Qué pasa si planteamos la solución pero con módulo de algún número?
Queremos resolver la ecuación aX=1 mod n, para algún n.

(Usaremos la notación z=w mod n para indicar que z es el resto de la división de w por n. No utilizamos la notación de congruencia sino la de igualdad, porque queremos enfatizar que el resultado z=w mod n está entre 0 y n-1).

Por ejemplo, supongamos que queremos resolver la ecuación 2X=1 mod 5. En este caso podríamos tomar todos los X posibles, multiplicarlos por 2 módulo 5, sólo consideramos los X no nulos:

2.1=2 2.3=6=1 mod 5
2.2=4 2.4=8= 3 mod 5

Vemos que la ecuación 2X=1 mod 5 tiene efectivamente solución, y más aún, es única. Pero esto no siempre ocurre, por ejemplo, miremos la ecuación 2X=1 mod 6.
Tenemos:

2.1=2 2.3=6=0 mod 6 2.5=10=4 mod 6
2.2=4 2.4=8=3 mod 6

La ecuación 2X=1 mod 6 no tiene solución.

Básicamente, dado un número n nos preguntamos (según lo visto en el capítulo de la aritmética de los enteros) qué números tienen inverso módulo n**.** La respuesta es que sólo aquellos números coprimos con n tienen inverso. Pero sólo si n es un número p primo, como 5. Entonces, la ecuación aX=1 mod p tiene solución para todo ***a*** no nulo, y esa solución es única en {0, 1, 2,..., p-1}.

Denotaremos la solución a esa ecuación como 1/a mod p.

En resumen: la notación 1/a mod p denota el único X en {0,1,2,...,p-1} tal que aX=1 mod p.

Así, por ejemplo, arriba vimos que 1/2 mod 5=3.

Ejemplos

1/6 mod 7=6, pues 6.6=36=1 mod 7.
1/5 mod 7=3, pues 3.5=15=1 mod 7.

Para resolver

Ejercicio 5.2:

Calcular 1/5 mod 11, 1/7 mod 11, 1/6 mod 11, 1/5 mod 13, 1/ 2 mod 7. (Ayuda: en este caso, como los primos son chicos, la solución se puede encontrar simplemente buscando todos los posibles. Al final del capítulo veremos un ejemplo para calcularlos sin necesidad de tratar todos los casos posibles).

Bien, ahora que se tienen las herramientas matemáticas podemos describir un teorema criptográfico debido a Kaisa Nyberg, profesora de criptografía de la Universidad Tecnológica de Helsinki.

Ese teorema dice, en forma resumida, lo siguiente: si se toma la substitución que manda el 0 al 0, y para un A no nulo se lo manda a 1/A módulo p, con p primo, entonces esa substitución es "altamente no lineal".

Esa substitución es:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	1	15	10	22	6	5	25	11	13	3	8	17	9	27

15	16	17	18	19	20	21	22	23	24	25	26	27	28
2	20	12	21	26	16	18	4	24	23	7	19	14	28

Esa substitución tiene un par de problemas, entre ellos que manda el 0 en el 0, el 1 en el 1 y el 28 (es decir, el -1) en el 28. Por lo tanto, **luego** de hacer la substitución le sumo 2 módulo 29. La suma 2, al ser lineal, no cambia las propiedades de no linealidad (sería algo como "no lineal+lineal=no lineal") y evita que haya puntos fijos.

Esa transformación, traducida a letras, es la transformación que usamos antes, pero cada uno podría construir la que quiera simplemente en vez de sumarle 2 módulo 29, sumándole algún otro número. También se podría tomar un alfabeto que en vez de tener 29 símbolos tuviera por ejemplo 31, y realizar las operaciones módulo 31. O bien, un alfabeto con solo 23 símbolos y hacer las operaciones módulo 23, etc. Lo importante es que la cantidad de símbolos fuese un primo.

El cifer descripto es bastante seguro, pero una computadora moderna lo puede quebrar rápidamente con sólo chequear todas las claves.

¿Qué podemos hacer? Una forma de incrementar la seguridad en los cifrados modernos es añadir **rondas.** Es decir, en vez de usar el cifer anterior, podemos usar un cifer con una clave de 12 letras en lugar de 8 repitiendo lo anterior. Una ronda de encriptamiento sería Vigenere + substitución no lineal + Hill.

En lugar de hacer:

Texto original
Vigenere
Substitución no lineal
Hill
Vigenere

Hacemos:

Texto original
Vigenere
Substitución no lineal
Hill
Vigenere
Substitución no lineal
Hill
Vigenere
Texto cifrado

O si queremos más protección, en vez de agregar una ronda podemos agregar dos. Para un total de 3 rondas, tenemos:

Texto original
Vigenere
Substitución no lineal
Hill
Vigenere
Substitución no lineal
Hill
Vigenere
Substitución no lineal
Hill
Vigenere
Texto cifrado

Para un total de 16 letras de clave que por ahora incluso los computadores más rápidos no pueden revisar en un tiempo razonable.

¿Se utiliza un sistema como éste?
No exactamente éste. Porque si bien hemos agrandado la clave, no hemos agrandado el bloque, y un bloque de sólo 4 letras es fácilmente quebrable por una computadora. Pero éste es, esencialmente, el estándar criptográfico de algoritmos de bloque que se usa en la mayoría de los bancos y sistemas de seguridad del mundo.

□ 5.5. Un poco de historia moderna

En 1973 el gobierno de EEUU decidió publicar un estándar criptográfico seguro para que pudiera ser usado con confianza por bancos y otras compañías.

El sistema, aprobado finalmente en 1976, se llamó DES, que son las siglas en inglés de Estándar de Encriptamiento de Datos (Data Encryption Standard).

A mediados de los 90, se observó que DES ya no era un algoritmo muy seguro. Luego de una competencia internacional para elegir al sucesor, que ganaron dos profesores de Bélgica, resultó elegido el AES (Advanced Encryption Standard: Estándar de Encriptamiento Avanzado).

El AES tiene esencialmente la estructura que vimos antes. En cada ronda hay una mezcla con la clave tipo Vigenere, una substitución no lineal construida apoyándose en el teorema de Nyberg más una transformación lineal para evitar puntos fijos, y una transformación lineal tipo Hill.

En lugar de usar un bloque de 4 letras (más o menos 19 bits y medio) usan un bloque gigante de 128 bits; la clave que usan también es de 128 bits, y en vez de usar dos o tres rondas, usan 10. Además, como en las computadoras casi todas las cosas funcionan mejor en potencias de 2, las operaciones no las hacen módulo 29, sino relativas al número 256.

Ahora bien, 256 es **no** primo, así que no se puede usar el teorema de Nyberg en el con-

junto de residuos módulo 256. Pero, los autores construyen un conjunto que tiene 256 elementos, en el que pueden definir una suma y un producto que tienen las propiedades necesarias para que se pueda usar una versión del teorema de Nyberg. La matemática que utilizan es muy avanzada y tiene que ver con divisiones por polinomios.

Éste es el estándar que se está usando en casi todos los bancos, salvo algunos que todavía usan DES. Si estudiamos un poco el cifer podremos tener una idea aproximada de qué está protegiendo, en este momento, las comunicaciones del mundo.

Un cifer verdaderamente indescifrable

Vigenere puede ser descifrado, pero da origen a un cifer verdaderamente indescifrable, aunque un tanto inútil. Consiste en tomar una clave **tan larga** como el texto a cifrar. De esta manera, no se repite nunca la clave y la técnica de partir el texto cifrado en subtextos no puede hacerse.

Pero, para que este cifer sea realmente indescifrable, la clave **debe ser generada al azar.**

Tomar, como hacen algunos, como clave un texto para encriptar otro se quiebra muy fácilmente con un análisis de coincidencias y frecuencias. Este cifer se llama **one time pad**, que en inglés significa, más o menos, una hoja (con la clave) que se usa una sola vez. También se lo conoce como el cifer de Vernam, que fue quien lo descubrió; el alfabeto que usaba no eran letras, sino los puntos y rayas del sistema Morse.

La ventaja que tiene es que si la clave es realmente al azar, sin ella no hay forma de desencriptarlo. La desventaja es que necesita una clave tan larga como el mensaje a encriptar, y toda la idea de los algoritmos de encriptamiento es transformar un secreto corto (la clave) en uno largo (el mensaje).

Así para transmitir un mensaje en forma segura, primero debemos hallar una forma para transmitir toda la clave en forma segura. Por eso este cifer no es tan bueno.

Igualmente, el cifer Vernam se puede usar cuando es posible intercambiar la clave en forma personal algún tiempo antes de necesitarla. Por ejemplo, existe el rumor de que los EEUU usaban un sistema parecido en sus embajadas: se les daba una colección de CD con bits grabados al azar. Una copia de esos CD estaba en Washington y se usaba en orden para ir encriptando los mensajes. Luego de usados, se destruían.

Si bien este cifer tiene el inconveniente de que la clave debe ser tan larga como el mensaje, da origen a una serie de cifers que tratan de subsanar este problema y que se conocen con el nombre en inglés de Stream Ciphers, o cifers de flujo.

CIFERS DE FLUJO

En el **one time pad** se requiere una clave de longitud igual al mensaje, que sea completamente al azar. Los **cifers de flujo** son, esencialmente, el one time pad, pero tratan de crear la clave a partir de una clave más pequeña.

Obviamente, el resultado no es una clave al azar y, por lo tanto, estos cifers no son seguros como el **one time pad**. Pero los criptógrafos tratan de que la "regla" por la que se crea la clave grande a partir de la pequeña produzca un resultado que sea lo más parecido posible a una secuencia al azar. Por lo menos que sea muy difícil para alguien distinguir entre eso y el azar verdadero. En general esto es muy difícil.

Veamos una idea de uno de los cifers de flujo más conocidos, llamado **RC4.**

RC4 opera con bytes, es decir "letras" de 8 bits cada una, como un "alfabeto" de 256 letras. Como es muy complejo, sólo queremos dar una idea que además se pueda resolver "a mano". Usaremos las operaciones principales de RC4, pero reducidas a nuestro alfabeto de 27 letras.

Comencemos con una substitución cualquiera de las letras, esta será la clave.

Si entendemos como siempre A=1, B=2 ,..., Y=26, Z=0, llamaremos S[A] a la letra que será substituida por A, S[B] a la letra que será subsitutida por B, etc.

Ejemplo

Por ejemplo, si usamos la tabla dada al principio del capítulo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	X	H	Z	G	Ñ	P	W	E	R	Y	F	T	A	V	Q	B	S	C	I	N	L	J	M	O	U	K

tenemos que S[A]=D, S[B]=X, S[C]=H, ..., S[Z]=K.

Pero también, se identifican letras con números, así que también podemos escribir: S[1]=4, S[2]=25, etc.

Antes usábamos esta tabla para hacer una substitución directa de las letras, en cambio, ahora produciremos una sucesión de letras, que usaremos como si fueran la clave de un one time pad.

Concretamente, supongamos que vamos a encriptar ATACAREMOS ALABAMA Y MISSISSIPPI.

Produciremos una secuencia de letras K_1, K_2, K_3, ... Entonces, nuestro texto cifrado tendrá, como primera letra $A+K_1$ mod 27, como segunda $T+K_2$ mod 27,…, etc.

¿Cómo producimos la secuencia de letras?

Antes de avanzar, es necesario explicar una diferencia fundamental entre un cifer de flujo y uno de bloque. En principio, en el cifer de bloque se podría usar el mismo cifer con la misma clave para encriptar mensajes distintos. En un cifer de flujo esto no se puede hacer porque se produciría la misma secuencia de letras para encriptar, y entonces, el atacante simplemente tomaría los dos textos cifrados, los restaría uno de otro, y tendría la diferencia entre dos textos que no dependen de la clave. Después haría un análisis de frecuencias y recuperaría ambos textos.

Así que los cifers de flujo siempre se usan con dos claves: una que es secreta y fija, y otra que es variable de mensaje a mensaje, pero que no tiene por qué ser secreta. Esta clave variable se llama un "IV" (siglas en inglés de vector de inicialización).

Entonces, si Alicia le quiere mandar a Berto un texto cifrado con un cifer de flujo, además le tiene que mandar sin encriptar cuál es el IV. Alicia y Berto deben mezclar la clave secreta con el IV y tendrán una clave de sesión que usarán sólo para encriptar un mensaje. Si después quieren encriptar otro mensaje deberán cambiar el IV y tendrán otra clave de sesión.

Supongamos que nuestro IV es otra sustitución. Para hacerlo simple digamos que el IV está dado por el César A-->D, B-->E, etc.

Entonces, la clave de sesión sería tomar el resultado de la clave secreta dada arriba, y cambiarla haciéndole el César. El S[] que usaremos será S[1]=D+3=G, S[2]=X+3=A, etc.

El resultado completo sería:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	A	K	C	J	Q	S	Z	H	U	B	I	W	D	Y	T	E	V	F	L	P	Ñ	M	O	R	X	N

Ahora vamos a producir la secuencia. Mantendremos dos índices, *i* y *j*. Inicialmente *i* será 1 y *j* será 0.

En cada paso, a *j* le sumaremos S[*i*] módulo 27. Por ejemplo, en el primer paso sumamos a *j*=0 el valor S[1]. En nuestro caso, S[1]=7 por lo tanto el nuevo *j* será 0+7=7.

Ahora que tenemos *i*=1 y *j*=7, **intercambiamos** los valores de S[1] y de S[7]. Es decir, al principio tenemos que S[1]=7 y S[7]=S[G]=S=20 después de intercambiar S[1]=20 y S[7]=7.

Ya estamos listos para decir cuál será la letra que usaremos para encriptar la primera letra del texto a cifrar: es la letra S[S[1]+S[7] mod 27]. Es decir, S[1]+S[7] mod 27=20+7 mod 27=0. En este caso la letra que usaremos para encriptar es S[0]=N.

La primera letra encriptada es A+N=Ñ.

Para hallar la segunda letra, tomamos *i*=2. Le sumamos a *j* el valor S[2]. Es decir, *j* es 7 y le sumamos el valor S[2]=1. El nuevo *j* es *j*=8. Nuevamente, intercambiamos los valores de S[2] y S[8]. Como S[8]=0, luego del intercambio queda S[2]=0, S[8]=1.

La letra que usamos para encriptar es S[S[2]+S[8] mod 27]=S[0+1]=S[1]=20.

Entonces, la segunda letra encriptada es T+20=21+20 mod 27=41 mod 27=14=N.

Es decir, la clave va evolucionando lentamente, cambiando a medida que vamos avanzando en el encriptamiento. Los dos primeros pasos fueron:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	A	K	C	J	Q	S	Z	H	U	B	I	W	D	Y	T	E	V	F	L	P	Ñ	M	O	R	X	N

↓

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	A	K	C	J	Q	G	Z	H	U	B	I	W	D	Y	T	E	V	F	L	P	Ñ	M	O	R	X	N

↓

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	Z	K	C	J	Q	G	A	H	U	B	I	W	D	Y	T	E	V	F	L	P	Ñ	M	O	R	X	N

En general, iremos cambiando *i* sumándole 1 (módulo 27) y *j* sumándole S[*i*] (módulo 27). Luego, intercambiaremos los valores de S[*i*] y S[*j*] y usaremos para encriptar el valor S[S[*i*]+S[*j*] mod 27].

Hagamos algunos pasos más. Para la tercera letra, *i*=3, y a *j* que valía 8 le sumamos S[3]=K=11, el nuevo *j* es 8+11=19. Intercambiamos los valores de S[3] y S[19]. La tabla queda:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	Z	F	C	J	Q	G	A	H	U	B	I	W	D	Y	T	E	V	K	L	P	Ñ	M	O	R	X	N

La letra que usaremos para encriptar será S[S[3]+S[19] mod 27]=S[6+11]=S[17]=E=5. La tercera letra del texto cifrado es A+5=F. El texto cifrado correspondiente a ATA es ÑNF.

Veamos la cuarta letra: *i* vale 4. A *j*=19 le debemos sumar S[4]=3, el nuevo *j* es 22.(=U). Intercambiamos los valores de S[4] y S[22], la tabla queda:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	Z	F	Ñ	J	Q	G	A	H	U	B	I	W	D	Y	T	E	V	K	L	P	C	M	O	R	X	N

La letra que usamos para encriptar es S[S[4]+S[22] mod 27]=S[15+3]=S[18]=V=23.

La cuarta letra del texto a cifrar es C, así que la cuarta letra del texto cifrado es: C+23=26=Y.

Para acelerar la descripción iremos mostrando cómo obtenemos las letras para encriptar el "flujo". Luego escribiremos directamente todo el texto a cifrar, después el flujo y, por último, el texto cifrado.

Quinta letra: *i*=5, a *j* le debemos sumar S[5]=10, el nuevo *j* queda 22+10 mod 27=32 mod 27=5. Observar que en este caso *i*=*j*, así que el intercambio de S[*i*] por S[*j*] no produce cambios. La letra del flujo es S[S[5]+S[5]]=S[10+10]=S[20]=L.

Sexta letra: *i*=6, a *j*=5 le debemos sumar S[6]=18, el nuevo *j* queda 5+18=23. Intercambiando S[6] por S[23] nos queda la tabla:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	Z	F	Ñ	J	M	G	A	H	U	B	I	W	D	Y	T	E	V	K	L	P	C	Q	O	R	X	N

La sexta letra del flujo es S[S[6]+S[23] mod 27]=S[13+18 mod 27]=S[31 mod 27]=S[4]=Ñ.

Séptima letra: i=7, a j=23 hay que sumarle S[7]=7, el nuevo j es igual a 23+7 mod 27=30 mod 27=3. Intercambiando S[7] por S[3] queda la tabla:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	Z	G	Ñ	J	M	F	A	H	U	B	I	W	D	Y	T	E	V	K	L	P	C	Q	O	R	X	N

Hacemos S[S[7]+S[3] mod 27]=S[6+7]=S[13]=W.

Octava letra: i=8, a j=3 le sumamos S[8]=A, el nuevo j es j=4. Intercambiando S[8] con S[4] queda la tabla:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	Z	G	A	J	M	F	Ñ	H	U	B	I	W	D	Y	T	E	V	K	L	P	C	Q	O	R	X	N

S[S[8]+S[4]]=S[15+1]=S[16]=T.

Novena letra: i=9, a j=4 le sumamos S[9]=8. El nuevo j es 12. Intercambiando S[9] con S[12] tenemos:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	Z	G	A	J	M	F	Ñ	I	U	B	H	W	D	Y	T	E	V	K	L	P	C	Q	O	R	X	N

S[S[9]+S[12]]=S[9+8]=S[17]=E.

Décima letra: i=10, a j=12 le sumamos S[10]=22, el nuevo j es 12+22 mod 27=34 mod 27=7. Intercambiamos S[10] con S[7]:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	Z	G	A	J	M	U	Ñ	I	F	B	H	W	D	Y	T	E	V	K	L	P	C	Q	O	R	X	N

S[S[10]+S[7] mod 27]=S[22+6 mod 27]=S[28 mod 27]=S[1]=S.

Entonces tenemos:

A	T	A	C	A	R	E	M	O	S
N	S	E	V	L	Ñ	W	T	E	S
Ñ	N	F	Y	M	G	B	G	T	M

El texto cifrado correspondiente a ATACAREMOS es ÑNFYMGBGTM.

Continuando, tendríamos que para la decimoprimera letra, i=11, a j=7 le sumamos S[11]=2, el nuevo j es 9. Intercambiando S[11] con S[9] tenemos la tabla:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	Z	G	A	J	M	U	Ñ	B	F	I	H	W	D	Y	T	E	V	K	L	P	C	Q	O	R	X	N

S[S[11]+S[9]]=S[2+9]=S[11]=I.

En este ejemplo se observa que si se hace primero S[S[*i*]+S[*j*]] y después el intercambio, el resultado es distinto que si hace primero el intercambio y después se calcula S[S[*i*]+S[*j*]]. **RC4** especifica el cambio primero y por eso lo planteamos de esa forma.

Como vemos, el algoritmo es un tanto engorroso, pero la seguridad es fantástica en relación con tamaño pequeño y la simpleza.

Para ejemplificarlo creemos que ya hemos mostrado bastante, pero al que le interese puede seguir con el encriptamiento.

Vemos que *i* va avanzando sin pausas, uno a uno, cambiando eventualmente todas las entradas. Mientras tanto *j* se va moviendo más o menos al azar, así que los cambios no son predecibles.

El estado interno que un atacante debería adivinar tiene tamaño 27!.27 (debe adivinar la permutación más el *j*). Esto es aproximadamente 98 bits de información, así que no es factible un ataque de fuerza bruta. Un análisis de frecuencia no sirve porque el estado interno va cambiando constantemente. El único punto débil sería que en las primeras salidas, cuando el estado todavía no está bien mezclado, podría revelar la clave, si se usa la misma clave con muchos IV distintos. Por eso, en general se recomienda "tirar" sin usar las primeras salidas.

Como dijimos el **RC4** real es parecido, pero tiene un alfabeto de 256 letras, es decir, un estado interno de tamaño 256!.256 que es **muy** grande, y se usa en muchísimos programas de computación, aunque ya está un tanto viejo. Tiene 20 años, una eternidad en criptografía.

INTERCAMBIO DE CLAVES

Alicia: (en el teléfono) Bien, Berto, ya entendí el sistema que me mandaste y estoy segura de que Eva no podrá quebrarlo, pero...

*Berto: ¿P*ero? ¿Cuál es el problema?

Alicia: Bueno Berto. Estos sistemas son muy buenos, pero necesitamos una clave que sepamos sólo vos y yo. Si lo hubiera sabido, la última vez que nos vimos, hace tres meses, nos hubiéramos puesto de acuerdo con una clave, pero como no lo hicimos. ¡Qué hacemos ahora? No puedo mandarte la clave por teléfono porque Eva la sabría.

Berto: Ah, pero eso tampoco es problema. Te voy a enseñar un método para que vos y yo construyamos entre los dos una clave, y que además Eva no pueda saberla.

Alicia: Pero, Berto, Eva va a escuchar todo lo que me digas. Si yo puedo seguir tus instrucciones, también lo puede hacer Eva.

Berto: No. Te voy a dar instrucciones para que vos hagas algo con información que **sólo vos** conozcas, así que Eva no va a poder repetirlas.

Alicia: Pero si es información que sólo **yo** conozco ¿cómo vas a poder saber **vos** la clave? Me parece que estas un poco loco, Berto. No veo que haya ninguna forma para que vos y yo hagamos algo para obtener una clave en común, y que Eva, que está escuchando todo, no pueda repetir.

Berto: Estás equivocada, Alicia. Sí hay una forma. Eso sí, vas a necesitar una muy buena calculadora....

Todos los algoritmos que vimos hasta ahora requieren el conocimiento de una clave secreta **compartida** entre las dos personas que se quieren comunicar.

Supuestamente esas dos personas, digamos Alicia y Berto, se encontraron antes en algún lugar seguro y se intercambiaron las claves. Pero ¿qué pasa si no se pudieron encontrar de antemano y deben intercambiar la clave a través de un medio inseguro?

Dos criptografos llamados Whitfield Diffie y Martin Hellman resolvieron este problema, en forma más o menos sencilla, usando propiedades elementales de la matemática.

Primero, supongamos las siguientes operaciones:

$$2^1=2;\quad 2^2=4;\quad 2^3=8;\quad 2^4=16;\quad 2^5=32;\quad 2^6=64;\quad 2^7=128.$$

Podemos preguntarnos: dado un número z del conjunto {1, 4, 8, 16, 32, 64, 128} ¿Cuál es el número x, tal que $2^x = z$? Por ejemplo: si z=64, entonces x=6.

Esto es encontrar logaritmos (en base 2). Mucha gente tiembla al oír la palabra logaritmo, pero encontrar logaritmos es algo relativamente fácil. De hecho, hoy se pueden calcular en la mayoría de las calculadoras.

Supongamos que no queremos hacer las operaciones en los reales, sino módulo algún número primo. Por ejemplo, tomemos el primo p=7, y tomemos como base el número 2. Tenemos:

$\mathbf{2^1 \bmod 7 = 2}$	$\mathbf{2^4 \bmod 7 = 2}$
$\mathbf{2^2 \bmod 7 = 4}$	$\mathbf{2^5 \bmod 7 = 4}$
$\mathbf{2^3 \bmod 7 = 1}$	$\mathbf{2^6 \bmod 7 = 1}$

En este caso, los únicos números que podrían tener un logaritmo en base 2 módulo 7 son 1, 2 y 4, pero, a diferencia de los reales, no es único: tanto 2^2 como 2^5 dan 4 módulo 7.

Con otro número pueden ser todos distintos:

$\mathbf{3^1 \bmod 7 = 3}$	$\mathbf{3^4 \bmod 7 = 4}$
$\mathbf{3^2 \bmod 7 = 2}$	$\mathbf{3^5 \bmod 7 = 5}$
$\mathbf{3^3 \bmod 7 = 6}$	$\mathbf{3^6 \bmod 7 = 1}$

A partir de allí, sí empiezan a repetirse.

Si hacemos la cuenta veremos que $4^6 \bmod 7=1$, $5^6 \bmod 7=1$ y $6^6 \bmod 7=1$.

Eso pasa en general, para todo primo p y para todo número b con $0<b<p$, tenemos que $b^{p-1} \bmod p = 1$.

Pero, como en el caso del 2 arriba, puede ser que $b^q \bmod p=1$ para algún q menor que p-1. Como es seguro que en p-1 se empiezan a repetir, sólo nos fijamos en números menores o iguales que p-1.

De todos modos, lo que nos interesa no es si hay o no un único exponente, sino si somos capaces de encontrar **al menos uno**. Es decir, dado un z queremos un x tal que $b^x \bmod p=z$. Por lo dicho anteriormente, basta con buscar los x entre 1 y p-1, pero si p es muy grande esta búsqueda puede demorar mucho tiempo.

Si bien se conocen métodos que son un poco más rápidos que una búsqueda total, no son mucho más rápidos, y si el número p es **muy** grande, digamos de 300 cifras decimales, entonces toda la edad del universo no alcanzaría para encontrar el x.

El problema de dado z hallar un x tal que $b^x \bmod p=z$, se conoce como problema del

logaritmo discreto

Es un problema muy difícil que nadie sabe cómo resolver en un tiempo razonable. Pero esto, le permitió a Diffie y Hellmann inventar un lindo algoritmo para intercambiar una clave entre Alicia y Berto, aún si sólo se pueden comunicar por un canal inseguro. Suponemos que Eva puede ver todo lo que Alicia le manda a Berto y todo lo que Berto le manda a Alicia.

Alicia y Berto deben construir una clave entre ellos de forma que sólo ellos la conozcan, a pesar de que Eva esté escuchando todo lo que dicen. Parece imposible. ¿Verdad? Pero sí se puede hacer.

Para empezar, tomaremos el ejemplo con un primo p chico.

Tomemos como primo p=11. Hay que elegir también una base g. Alicia elige g=2 y le comunica a Berto que va a usar tanto p=11, como g=2. Eva escucha todo esto. Ahora, Alicia elige en secreto un número x que **no** le comunica a Berto. Digamos que Alicia elige el número x=4. A continuación, Alicia calcula el número $v=2^4 \bmod 11=16 \bmod 11=5$.

Alicia le manda ese número v a Berto.

Eva también sabe cuál es ese número porque lo ve; pero como el problema del logaritmo discreto es difícil, saber v no le facilita saber x (en este ejemplo, como los números son chicos podría encontrarlo por fuerza bruta, pero en la práctica p tiene cientos de dígitos).

Ahora bien, Berto tampoco tiene la menor idea de cuánto vale x. ¿Qué hacer? Berto hace lo mismo que Alicia: toma un número z, por ejemplo z=9. Con ese número que eligió calcula $w=g^z \bmod p$. En este caso, $w=2^9 \bmod 11=512 \bmod 11=6$. Berto le manda w a Alicia. Al igual que con v, Eva puede leer el w=6, pero como el problema del logaritmo discreto es difícil, no puede saber que w viene de z=9.

Veamos qué sabe cada uno en este momento:

Alicia sabe que x=4 y que w=6.

Berto sabe que v=5 y que z=9.
Eva sólo sabe que w=6 y que v=5.

Entonces, si bien Eva escucha todo lo que Alicia y Berto se dicen, no puede saber lo que **no** se dicen. Es decir, no puede saber x porque Alicia no se lo dice a Berto, ni puede saber z porque Berto no se lo dice a Alicia.

Ahora bien, supongamos que Alicia hace:

$w^x \bmod p = 6^4 \bmod 11 = (36)^2 \bmod 11 = 3^2 \bmod 11 = 9$

Como sólo Alicia sabe x, Eva no puede hacer ese cálculo. ¡Berto tampoco puede! Pero Berto sí puede hacer el cálculo $v^z \bmod p$:

$v^z \bmod p = 5^9 \bmod 11 = (25)^4 \ 5 \bmod 11 = 3^4 \ 5 \bmod 11 = 4.5 \bmod 11 = 9$.

¡Sorpresa! Alicia hizo un cálculo con la información que ella tenía y obtuvo 9.
Berto hizo un cálculo con la información que él tenía y también obtuvo 9.

Ahora, Alicia y Berto pueden usar 9 como su clave común, porque Eva no la puede calcular.

Esto puede parecer casualidad, veamos otro ejemplo.
Tomemos como primo p=53 y como g=2. Aprovechamos este nuevo ejemplo, para explicar cómo se efectúan estos cálculos con números grandes.

Supongamos que debemos calcular $2^{123455636789} \bmod 154667$

Sería una locura calcular $2^{123455636789}$ y luego tomar módulo. Entre otras cosas, porque no hay suficientes átomos en el universo para escribir el número $2^{123455636789}$ en dígitos decimales.

La solución obvia sería tomar t=2 y hacer 123455636789 veces t=2t mod 154667. Pero, si se supone que uno está tomando un número p lo suficientemente grande para que el problema del logaritmo discreto sea difícil de resolver, entonces calcular t=2t mod p un número x de veces no sería factible de hacer en tiempo razonable. Si lo fuera, Eva podría ir haciendo t=2t mod p, una cierta cantidad de veces hasta hallar v.

Entonces, ¿cómo se hacen los cálculos con números grandes?

El truco está en la descomposición binaria de x. Suponemos que Alicia elige x=15. Podemos escribir 15 como 15=8+4+2+1. Es decir, en el sistema binario se escribe como "1111". Por lo tanto, $2^{15}=2^8 2^4 2^2 2$.

Entonces, en vez de hacer 2^{15}, alcanza calcular 2, 2^2, 2^4 y 2^8, módulo 53, y luego multiplicarlos también módulo 53. Es fácil calcular 2, 2^2, 2^4 y 2^8 porque cada uno es el cuadrado del anterior, por lo tanto, sólo necesitamos una operación para calcular cada uno de ellos. En definitiva, para calcular 2^{15} no necesitamos hacer 15 multiplicaciones sino sólo 4 elevaciones al

cuadrado y cuatro productos. No parece mucho ahorro, pero es que 15 es un número bajo.

Si tuviésemos que hacer $2^{1.048.575}$, este método permitiría en vez de hacer un millón y pico de multiplicaciones calcularlo con sólo 20 multiplicaciones y 20 elevaciones al cuadrado. En el caso de los números que realmente se usan en criptografía por este método se requieren varios cientos de multiplicaciones y elevaciones al cuadrado, pero por el método directo toda la edad de este universo más varios universos paralelos no alcanzaría.

Calculemos 2^{15} mod 53.

Este caso es simple porque no hay 0s en la expansión binaria de 15. Usaremos dos variables: la variable t para calcular 2, 2^2, 2^4 y 2^8. Al principio tomamos t=2 y luego la vamos elevando al cuadrado. Además necesitamos otra variable, a la que llamaremos r. En esta variable, al final de todos los cálculos debería encontrarse la respuesta que buscamos, es decir 215 mod 53. Para hacer eso, simplemente inicializamos la variable como r=1, y luego en cada paso hacemos simplemente r=rt mod p.

Entonces, primero tomamos t=2, r=1.

En el primer paso sólo hay que hacer r=1.2=2.

En el segundo paso elevamos t al cuadrado y multiplicamos r por el resultado: r:

$$t=2^2=4,\ r=2.4=8.$$

En el tercer paso hacemos lo mismo:

$$t=4^2=16,\ r=8.16 \bmod 53=128 \bmod 53=22.$$

En el cuarto y último paso:

$$t=(16)^2 \bmod 53=256 \bmod 53=44 \text{ y:}$$
$$r=22.44 \bmod 53=968 \bmod 53=14$$

También podríamos haber hecho: r=22.44 mod 53=22.(-9) mod 53=-198 mod 53=14)

Por lo tanto, 2^{15} mod 53=14.

Este es el número v que Alicia le manda a Berto. Como antes, Eva puede leerlo.

Berto elije z=22. Berto debe calcular w=2^{22} mod 53.

Veamos cómo se hace con el método de la expansión binaria:

Primero, escribimos 22 en binario: 22(decimal)=10110(binario).

Entonces, $2^{22}=2^{16}2^4 2^2$. Debemos calcular esos números y luego multiplicarlos. Como antes, fijamos t=2, r=1, e iremos haciendo t=t^2 mod p y r=rt mod p, pero esto último **sólo**

lo hacemos cuando haya un 1 en la expansión binaria. En el caso de 2^{15} lo hacíamos siempre porque 15(decimal)=1111(binario).

Entonces, en el primer caso hacíamos r=1.2, pero ahora no lo hacemos porque el primer dígito binario de 22 (leyendo de derecha a izquierda) es cero. Luego del primer paso, sigue siendo r=1, t=2.

En el segundo paso hacemos $t=2^2=4$, y como el segundo dígito binario de 22 es 1, también hacemos $r=r.t=1.4=4$.

En el tercer paso hacemos $t=4^2=16$, y como el tercer dígito binario de 22 es 1 también hacemos $r=r.t \bmod p=4.16 \bmod 53=64 \bmod 53=11$.

En el cuarto paso hacemos $t=(16)^2 \bmod 53=256 \bmod 53=44$, pero como el cuarto dígito binario de 22 es 0, dejamos r como está.

En el quinto y último paso hacemos: $t=44^2 \bmod 53=(-9)^2 \bmod 53=81 \bmod 53=28$, y como el quinto digito binario de 22 es 1, hacemos $r=r.t \bmod p=11.28 \bmod 53=308 \bmod 53=43$.

Entonces, Berto le manda w=43 a Alicia. Eva también ve esto, pero no puede hacer nada de nada.

Alicia debe hacer ahora $43^{15} \bmod 53$. El método es igual que antes, sólo que ahora t comienza en t=43.

En el primer paso, como 15(decimal)=1111(binario), hacemos $r=1.43=43$.

En el segundo paso hacemos: $t=(43)^2 \bmod 53=(-10)^2 \bmod 53=100 \bmod 53=-6 \bmod 53=47$. Y $r=43.47 \bmod 53=(-10)(-6) \bmod 53=60 \bmod 53=7$.

En el tercer paso hacemos: $t=(47)^2 \bmod 53=(-6)^2 \bmod 53=36$. Y $r=7.36 \bmod 53=252 \bmod 53=40$.

En el cuarto y último paso hacemos: $t=36^2 \bmod 53=(-17)^2 \bmod 53=289 \bmod 53=24$. Y $r=40.24 \bmod 53=2.480 \bmod 53=2.(-50) \bmod 53=2.3 \bmod 53=6$.

Alicia tiene ahora una clave igual a 6.

Berto había recibido v=14 de Alicia y él había elegido z=22. Debe hacer $14^{22} \bmod 53$. Como antes, 22(decimal)=10110(binario).

Toma t=14, r=1 y en el primer paso no hace nada, pues el primer dígito binario de 22 es 0.

En el segundo paso hace: $t=14^2 \bmod 53=196 \bmod 53=37$ y $r=1.37=37$.

En el tercer paso hace: $t=37^2 \bmod 53=(-16)^2 \bmod 53=44$ (antes hicimos este cálculo) y

r=37.44 mod 53=(-16).(-9) mod 53=-144 mod 53=-15 mod 53=38.

En el cuarto paso hace: t=44^2 mod 53=$(-9)^2$ mod 53=81 mod 53=28. Y r queda como está, pues el cuarto dígito binario de 22 es 0.

En el quinto, y último paso, hace: t=28^2 mod 53=784 mod 53=42.
Y r=38.42 mod 53=(-15).(-11) mod 53=165 mod 53=6.

Berto, luego de todos estos cálculos, también obtiene lo mismo que Alicia.

Ambos pueden usar entonces el número **6** como clave, a pesar de que llegaron a él por distintos caminos. Eva no puede hacer ninguno de esos cálculos y no sabe cuál es la clave de sesión.

Pero ¿por qué funciona?

La respuesta es muy simple: básicamente, porque "**el orden de los factores no altera el producto**". Resumamos qué es lo que pasa en el caso general:

Alicia elige un x, calcula v=g^x mod p y le manda v a Berto.
Berto elige un z y le manda w=g^z mod p a Alicia.
Alicia calcula clave A=w^x mod p.
Berto calcula clave B=v^z mod p.
Alicia usa clave A y Berto usa clave B.

Para que esto funcione, debemos probar que clave A = clave B.

Pero clave A = w^x mod p=$(g^z$ mod $p)^x$ mod p=$(g^z)^x$ mod p=g^{zx} mod p, mientras que, clave B = v^z mod p=$(g^x$ mod $p)^z$ mod p=$(g^x)^z$ mod p= g^{xz} mod p, y, por lo tanto, sólo estamos diciendo que para que las claves sean iguales debe ser válido que zx=xz, lo cual es cierto.

Ejercicio 5.3:

Para resolver

a) Calcular 2^{32} mod 37.
b) Alicia y Berto quieren intercambiar claves usando p=23 y g=3. Alicia elige x=18 y Berto elige z=14. Hallar la clave común.

5.6. Clave pública y privada

Los algoritmos de bloque y de flujo que hemos visto son llamados de clave simétrica. Porque si Alicia quiere hablar con Berto, tanto Alicia como Berto deben tener la misma clave.

Esto está bien para dos personas, pero supongamos que tenemos a Alicia, Berto, Cecilia, Daniel, Ernestina, Federico, Gabriela, Hernando, Inés y Juanita que quieren hablar en secreto

entre ellos. Además, Alicia no quiere que lo que le dice a Berto pueda ser leído por Ernestina, ni quiere que lo que le dice a Ernestina pueda ser leído por Berto, y así sucesivamente. O bien, no les importa que entre sí se puedan leer los mensajes, pero son parte de una organización clandestina y, si atrapan a uno de ellos, no quieren que se conozcan los secretos de todos. Entonces, cada par de personas debería tener una clave distinta. ¿Cuántas claves distintas necesitan?

Son 10 personas. ¿Cuántos conjuntos de dos personas pueden formarse a partir de un conjunto de 10 personas? Del capítulo de combinatoria, recordemos que esto se puede hacer en 10.9/2=45 formas distintas. Por lo tanto, necesitaremos 45 claves distintas.

¿Y si hubiesen sido 100 personas? Necesitaríamos 100.99/2=4.950 claves distintas. Si fuese una organización realmente grande, con digamos 5.000 personas, requerimos 5.000 . 4.999/2=12.497.500 claves.

Por 1970, se inventaron algunas formas de lograr que el número de claves no necesitara ser tan alto. Además, solucionaron otro problema. Supongamos que una organización tiene 1.000 miembros y el Zorro se une a ella. De la forma usual, el Zorro, para establecer su clave debería comunicarse, de alguna forma segura, con cada uno de los 1.000 miembros.

En cambio, la nueva forma funciona así: cada persona de la organización tiene dos claves, una privada que sólo él o ella conoce, y otra pública, que conocen todos. Cuando alguien se incorpora a la organización, no es necesario crear 1.000 claves o las que sean. Independientemente del número de integrantes de la organización se crean sólo dos claves. En el caso anterior, se crea una clave pública para el Zorro que se publica, y una clave privada que sólo sabrá él. Sí habrá que darle al Zorro el listado de las claves públicas de todos los otros integrantes, pero él no necesita comunicarse con ellos para obtener las claves o para generar su propia clave.


Taher ElGamal

Cuando Alicia quiera mandarle un mensaje al Zorro, ella simplemente buscará la clave pública del Zorro y encriptará un mensaje para el Zorro con esa clave. El Zorro (y sólo él) usará su clave privada para leerlo. Nadie más, ni Berto, ni Cecilia, ni Daniel, etc, podrán leer ese mensaje. Más aún, si Alicia pierde el mensaje original que ella misma encriptó, ni siquiera ella podrá desencriptar el mensaje que le mandó al Zorro.


Los autores de RSA

¿Cómo puede existir un sistema así? Puede, con la ayuda de las matemáticas.

El sistema más conocido de este tipo es el sistema **RSA** que son las iniciales de sus autores, **Rivest, Shamir y Adleman**. (Rivest es también el inventor de **RC4**).

En las figuras podemos ver los autores de RSA y a Taher ElGamal.

Otro sistema muy usado es el sistema ElGamal, llamado así por su inventor. ElGamal es un intercambio de claves Diffie-Hellman disfrazado, seguido de un encriptamiento que es, simplemente, multiplicar por la clave producida por Diffie-Hellmann.

Veamos cómo se procede en ElGamal. Supongamos que Alicia quiere crearse una clave pública/privada. Básicamente, lo que hace es iniciar la mitad de Diffie-Hellmann: primero debe elegir un primo p muy grande y un número g entre 2 y p-2. En realidad, p y g pueden

ser el mismo para todos los integrantes de la organización. Luego, elige un número x que será su clave privada. El número x también tiene que estar entre 2 y p-2, en principio, se supone que debe ser un número más bien grande para que sea difícil de adivinar.

Una vez elegido x, Alicia calcula $v=g^x \bmod p$, y publica v (junto con p y g, si es necesario) como su clave pública. Es decir, hizo lo que haría con Diffie-Helmmann, sólo que en vez de mandárselo a Berto, simplemente lo publica.

Supongamos ahora que Berto desea mandarle a Alicia un mensaje. Todo lo que debe hacer Berto es, básicamente, completar Diffie-Hellman y encriptar el mensaje multiplicándolo por la clave común que obtendrá.

Veamos un ejemplo. Alicia escoge p=53, g=2 y como clave privada x=15, obtiene como clave pública v=14.

Supongamos que Berto quiere encriptar el mensaje 50.

Deberá hacer lo siguiente: primero, elegir un número al azar z menor que 53. Supongamos que elige 22. Con ese número calcula $g^z \bmod p$. En este caso, $2^{22} \bmod 53$=**43** (este cálculo se realizó antes en el texto).

Ésta es la primera parte del mensaje encriptado, que podemos llamar a.

Luego, debe tomar la clave pública v y hacer $v^z \bmod p$. En nuestro caso, $14^{22} \bmod 53$ (este cálculo se realizó antes en el texto) y su resultado es 6. Multiplica este resultado módulo 53 por el mensaje (en nuestro caso, 50) y obtiene la segunda parte del cifrado, que podemos llamar ***b.***

En nuestro caso: $b=6.50 \bmod 53=6(-3) \bmod 53=-18 \bmod 53$=**35.**

En conclusión, Berto le manda a Alicia el mensaje $(a,b)=(43,35)$.

¿Cómo recupera Alicia el mensaje original?

Básicamente, completando Diffie-Hellmann: usando "***a***" y su clave privada x calcula $a^x \bmod p$, en nuestro caso $43^{15} \bmod 53$, que también es una cuenta que hicimos y sabemos que da 6. Ahora bien, tal como explicamos cuando vimos el teorema de Nyberg, al ser 53 primo, 6 tiene un "inverso" módulo 53. Es decir, hay un único número que podemos denotar como 1/6 mod 53 tal que multiplicado por 6 módulo 53 se obtiene 1. Por ahora, no explicaremos cómo se calcula, pero en este caso 1/6 mod 53 es igual a 9, pues $9.6=54=1 \bmod 53$.

Al conocer ese inverso, Alicia simplemente hace $9.b \bmod p=9.35 \bmod 53=315 \bmod 53=50$ y recupera el mensaje.

□ 5.7. RSA

El sistema más famoso de clave pública/privada no es ElGamal, sino el sistema RSA.

Este sistema no se basa en la dificultad del logaritmo discreto, sino en la dificultad de factorizar un número. En vez de tomar un primo, Alicia debe tomar dos: p y q. Para mostrarlo con primos chicos, tomemos por ejemplo p=11 y q=17.

Hacemos el producto de ellos: $n=pq$=11.17=187. Éste será una parte de la clave pública, los primos p y q **no** son parte de la clave pública, sólo el producto es parte de ella.

Para seleccionar la clave privada y la otra parte de la clave pública, Alicia debe hacer el producto $(p-1)(q-1)$, en este caso, el producto 10.16=160. Luego, debe encontrar dos números e y d tales que ed=1 mod 160. En realidad, basta elegir cualquier número e coprimo con 160 (se puede saber si dos números son coprimos sin necesidad de factorizarlos), y luego también hay una forma rápida de encontrar el d.

En realidad, $d=1/e$ mod $(p-1)(q-1)$ que existe pues suponemos que e es coprimo con $(p-1)(q-1)$. Recordar del capítulo de la aritmética del reloj que la ecuación ax=1 mod n tiene solución si el máximo común divisor entre a y n es uno.

Una vez que tenemos e y d, uno de ellos (por ejemplo e) forma parte de la clave pública junto con n, y el otro es la clave privada.

Observar que si Eva es capaz de factorizar n, al obtener p y q puede calcular $(p-1)(q-1)$ y puede entonces, como sabe e, calcular d. Por eso la seguridad de RSA depende de que sea difícil factorizar n.

En nuestro caso, supongamos que Alicia elige e=7 y d=23. Como 7.23=161=1 mod 160, estos números andan bien, porque como se explicó arriba, el producto de d por e debe ser igual a uno módulo $(p-1)(q-1)$. Entonces, la clave pública es el par (n,e)=(187,7) y la clave privada es d=23.

Supongamos ahora que Berto desea encriptar un mensaje para Alicia. Para encriptar un mensaje se lo parte en bloques de longitud menor que n=187.

¿Cómo se encripta cada bloque? Simplemente, dado M se hace M^e mod m. En nuestro caso, supongamos que Berto quiere encriptar M=100. Debe hacer 100^7 mod 187.

Como vimos antes, se hace descomponiendo 7 en binario: 7(decimal)=111(binario).
Entonces tomamos t=100, r=1. En el primer paso hacemos $r=rt$ mod 187=100.

En el segundo paso hacemos $t=100^2$ mod 187=10000 mod 187=89.
Y r=100.89 mod 187=8900 mod 187=111.

En el tercer paso, hacemos $t=89^2$ mod 187=7921 mod 187=67.
Y r=111.67 mod 187=7437 mod 187=144.

Ése es el mensaje encriptado C que Berto le manda a Alicia.

¿Como hace Alicia para leerlo?
Simplemente hace C^d mod n, en nuestro caso, debe hacer 144^{23} mod 187.

Para calcularlo, escribimos 23 en binario: 23(decimal)=10111(binario). Tomamos t=144, r=1.

Primer paso: r=144.1=144.

Segundo paso: t=144^2 mod 187=$(-43)^2$ mod 187=1849 mod 187=166.
Y r=144.166 mod 187=(-43)(-21) mod 187=903 mod 187=155.

Tercer paso: t=166^2 mod 187=$(-21)^2$ mod 187=441 mod 187=67.
Y r=155.67 mod 187=(-32).67 mod 187=-2144 mod 187=-87 mod 187=100.

Cuarto paso: t=67^2 mod 187=4489 mod 187=1 y r queda como esta, pues el cuarto dígito binario de 23 es 0.

Quinto paso: t=1^2 mod 187=1, y r=100.1=100. Que era el mensaje que mandó Berto.

Para resolver

Ejercicio 5.4.:

Usando los primos p=7, q=11, y e=13, calcular las encriptaciones de los números 10, 2, 5 y 22 usando RSA.

1) Con números chicos como ejemplo, se corre el riesgo de no tener muchas claves posibles. Por ejemplo, en la actividad anterior las claves deben ser coprimas con (p-1)(q-1)=6.10=60. Calcular cuántas claves posibles hay entre 2 y 59.

2) Repetir 1) con primos p=11, q=17 y e=9.

3) Con números chicos algunas cosan más sorprendentes pueden pasar. Tomar p=7, q=5 para formar una clave RSA. Tomar cualquier número que Ud. quiera como clave pública e. (Recuerde que puede ser cualquiera, siempre que sea coprimo con (p-1)(q-1) que en este caso es 24). Ahora haremos un Acto de Magia: piense en un número entre 2 y 34. Encripte esa número DOS VECES con RSA con su clave pública. Debería sorprenderse de la respuesta.

Ejercicio 5.5., para pensar, más dificil:

1) (Para pensar) Dar una explicación matemática del fenómeno del ítem 4 arriba.

2) (Para hacer un poco de manipulación algebraica) El lector atento podría ver que Eva en realidad no necesita saber p y q: sólo necesita saber (p-1)(q-1). Como Eva sabe pq, se podría pensar que en una de esas hay alguna forma de deducir (p-1)(q-1) a partir de pq sin necesidad de hallar p y q. Mostrar que esto es falso: cualquiera que conozca (p-1)(q-1) y pq puede hallar p y q. (Advertencia: debe saber resolver ecuaciones de segundo grado para hacer esto. Solo recomendado para el muy interesado)

Un último comentario: está probado que si Eva es capaz de averiguar d a partir de pq y de e, entontes Eva puede factorizar pq y encontrar los factores p y q.

□ 5.8. Apéndice: ¿Cómo calcular 1/*a* mod *p*?

En algunas partes fue necesario calcular 1/*a* mod *p*. Incluso en RSA para calcular la clave pública de la privada, o viceversa, debemos calcular inversos mod (*p*-1)(*q*-1).

¿Cómo se calculan estos inversos?

Recordemos del capítulo de la aritmética del reloj, que un número *a* tendrá un inverso módulo *n*, si y sólo si, el máximo común divisor entre *a* y *n* es 1. Recordemos también de ese capítulo, que el máximo común divisor entre dos números se puede escribir como combinación lineal entera de ellos. Es decir, encontraremos números enteros *k* y *j* tales que 1=*ak*+*jn*. Pero esto significa que *ak*=1 mod *n*, por lo tanto *k* mod *n* es el inverso de *a*.

Ejemplos

Veamos algunos ejemplos.

1) Calcular 1/5 mod 29, 1/7 mod 29 y 1/15 mod 31.
2) El máximo común divisor entre 5 y 29 es 1. De hecho, podemos escribir 1=30-29=6.5-29. Esto dice que 6.5 mod 29=1. Por lo tanto, 1/5 mod 29=6.
3) El máximo común divisor entre 7 y 29 es 1 y de hecho podemos escribir 1=29-28=29-4.7. Esto dice que -4.7 mod 29=1 y por lo tanto 1/7 mod 29=-4 mod 29=25.
4) Para el último caso también escribimos 1=31-30=31-2.15, con lo cual -2.15 mod 31=1, es decir, 1/15 mod 31=-2 mod 31=29.

En estos ejemplos, nos fue fácil escribir 1 en la forma en que necesitamos. Pero a veces no es tan obvio. Por ejemplo, supongamos que queremos calcular 1/35 mod 97.

Lo que hacemos es calcular el máximo común divisor con la siguiente observación: mcd(*a,b*)=mcd(*b,a* mod *b*)

Dividiendo 97 por 35 tenemos 97=2.35+27, por lo tanto 97 mod 35=27.
Dividiendo 35 por 27 tenemos 35=27.1+8, por lo tanto 35 mod 27=8.
Dividiendo 27 por 8 tenemos 27=3.8+3, por lo tanto 27 mod 8=3.
Dividiendo 8 por 3 tenemos 8=2.3+2 por lo tanto 8 mod 3=2.

Finalmente, está claro que el mcd(3,2)=1.

Vamos a ir para atrás en la cadena de razonamientos previa. Escribimos 1 en términos de los últimos números que obtuvimos, que son simples, y luego vamos reemplazando para atrás hasta llegar a los números originales:

Es decir, empezamos con: 1=3-2.

Luego, usamos 8=2.3+2 para escribir 2=8-2.3, lo que nos permite escribir el 1 en términos del 8 y del 3:

$$1=3-2=3-(8-2.3)=3-8+2.3=3.3-8.$$

Luego, usamos 27=3.8 + 3 para escribir 3=27 - 8.3 y escribir 1 en términos de 8 y 27:

1=3.3 – 8=3.(27 - 8.3) – 8=3.27 – 8.3.3 – 8=3.27 – 10.8.

Luego, usamos 35=27.1+8 para escribir 8=35 – 27 y escribir el 1 en términos de 35 y 27:

1=3.27 – 10.8=3.27 – 10.(35 – 27)=3.27 – 10.35 + 10.27 =13.27 – 10.35.

Finalmente, usamos 97=2.35+27 para escribir 27=97 - 2.35 y poder expresar el 1 en términos de 97 y 35:

1=13.27 – 10.35=13.(97 – 2.35) – 10.35= 13.97 – 26.35 – 10.35=13.97 – 36.35

Esto dice que -36.35 mod 97=1, por lo tanto 1/35 mod 97=-36 mod 97=61.

Este cálculo se puede hacer muy rápido incluso para números grandes.

Ejemplo

Veamos un último ejemplo:

Supongamos que en RSA tomamos primos p=83 y q=113. El producto es n=9.379. Supongamos que deseamos tomar como clave pública e=17. ¿Cuál es la clave privada?

Debemos primero calcular (p-1)(q-1). En nuestro caso, obtenemos 82.112=9.184.

Dividiendo 9.184 por 17 tenemos: 9.184=540.17 + 4.

En este caso, no necesitamos hacer muchos más cálculos, porque podemos escribir fácilmente 1 en términos de 17 y 4 como 1=17-4.4. Luego reemplazamos:

1= 17 – 4.4
= 17 – 4.(9184 – 540.17)
= 17 - 4.9184 +4.540.17
= 17 - 4.9184 +2160.17
= 2161.17 - 4.9184

Esto dice que 2.161.17 mod 9.184=1 y, por lo tanto, d=1/e mod (p – 1)(q – 1)= =1/17 mod 9.184=2.161.

Para resolver

Ejercicio 5.6:

1) Tomando p=89, q=97 y e=23 calcular la clave privada d.
2) Repetir con p=59, q=101 y e=31.

6. Soluciones de los ejercicios

□ Capítulo 1

1.1. 73, 173, 373, 673, 773, primos;

273 = 3 x 7 x 13; 473 = 11 x 43; 573 = 3 x 191;
873 = 3 x 3 x 97; 973 = 7 x 139; 1.073 = 29 x 37.

1.2. $4.875 = 3 \times 5^3 \times 13$ $18.207 = 3^2 \times 7 \times 17^2$ $236.769 = 3 \times 13^2 \times 467$
$710.073 = 3^2 \times 7 \times 13 \times 17^2$

1.3. 322.423 = 503 x 641.

1.4. Porque no aparecen primos pequeños. Ambos son grandes y difíciles de encontrar.

1.5. 3.571.

1.6. 1,220703125 = 1,1920928955078125 x 1,024 = 78.125/65.536 x 128/125.

1.7. No, porque todo número racional *a* se parte como suma de *a*/2 + *a*/2.

1.8. Los compuestos son los múltiplos de 4. Los irreducibles son los pares que tienen resto 2 al dividir por 4.

1.9. $226.738.512 = 2^4 \times 3^2 \times 7 \times 11^3 \times 13^2$

1.10. $3.772.486.575 = 3^3 \times 5^2 \times 11^3 \times 13 \times 17 \times 19$.

1.11. 1 = 42 x 5 - 19 x 11.

1.12. Con 17 pesas de 70 g en el platillo que hay 10 y 5 pesas de 240 g en el otro.

1.13. No se puede como resta de un múltiplo de 11 menos un múltiplo de 42. Sí se puede como resta de un múltiplo de 7 menos un múltiplo de 18: 1 = 13 x 7 - 5 x 18.

1.14. Primero escribimos $1 = a \times n - b \times p$, con *a* y *b* positivos. Ahora observamos que $1 = a \times n - b \times p + k \times p \times n - k \times p \times n = (a - k \times p) \times n - (b - k \times n) \times p$ para todo número *k* positivo. Tomando *k* suficientemente grande como para que $(a - k \times p)$ y $(b - k \times n)$ sean negativos, si llamamos $a_1 = -(a - k \times p)$ y $b_1 = -(b - k \times n)$ obtenemos que $1 = b_1 \times p - a_1 \times n$

1.15. Empezando con 2, 3 y 5 aparecen los primos 31, luego 7, 7 y 19, luego 139 y 6229, luego 751 y 998.218.981, etc.

1.16. La lista de números 7, 43, 1.807, 3.263.443 se obtiene mediante la siguiente recursión: $a_{n+1} = a_n (a_n - 1) + 1$. Esto lleva a que si a_n termina en 3 el a_{n+1} termina en 7 y si el a_n termina en 7 el a_{n+1} termina en 3. Por lo tanto nunca será a_n un múltiplo de 5.

□ Capítulo 2

2.1. $9 (4 + 4 + 2 + 2) = 108$.

2.2. a) $41 . 25 . 9 = 9.225$.
b) $41 . 25 . 9 .3! = 55.350$.
c) $(41 + 25 + 9)(41 + 25 + 9 - 1)(41 + 25 + 9 - 2). 3! = 75 . 74 . 73.6 = 2.430.900$

2.3. $26^3.10^3 = 17.576.000$

2.4. a) $3! 7! 8 = 241.920$.
b) $7! 6 . 5 . 4 = 604.800$.

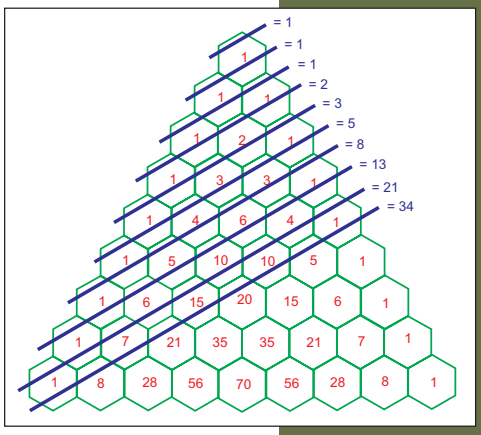
2.5. Como $600 = 2^3. 3 . 5^2$, hay $4 . 2 . 3 = 24$ posibles divisores de 600.

2.6. 10.9^{n-1}

2.7. Más regularidades en el Triángulo de Pascal.


Triángulo de Sierpinski

a) Los números naturales: Cualquiera de las dos segundas diagonales.
b) Los números triangulares: Las terceras diagonales.
c) Los números tetraedros: Las cuartas diagonales.
d) Números pares e impares. Si coloreamos los números pares de un color y los impares de otro, obtenemos el denominado triángulo de Sierpinski.
e) Potencias de dos: Se obtienen sumando las filas:



$1 = 2^0$ $\qquad$ $1 + 2 + 1 = 2^2$
$1 + 1 = 2^1$ $\qquad$ $3 + 3 + 3 = 2^3$

y así sucesivamente.

f) Secuencia de Fibonachi:
g) Potencias de 11. Las filas forman los dígitos de las potencias:

$1 = 11^0$ $\qquad$ $131 = 11^3$
$11 = 11^1$ $\qquad$ $14.641 = 11^4$
$121 = 11^2$ $\qquad$ $151.151 = 11^5$

Y así sucesivamente. Notar que cuando el número tiene dos o más dígitos, ellos deben sumarse.

2.8. Para probar la identidad basta ver que cada miembro corresponde a la cardinalidad del mismo conjunto: las distintas maneras de armar una comisión de m integrantes de un grupo de n personas junto con una subcomisión de r personas, $0 \le r \le m \le n$. Podemos primeros elegir la comisión y luego de ella sacar la subcomisión, o bien podemos elegir primero la subcomisión de r integrantes, y luego completar hasta m la comisión con los $n - r$ restantes. Esas cardinalidades son las correspondientes a ambos miembros.

2.9. Calculamos $\binom{n+r}{r} = \frac{(n+r)(n+r-1)....(n-r)!}{(n-r)!r!}$

$= \frac{(n+r)(n+r-1)...(n+1)}{r!}$ de donde sigue el resultado.

2.10. a) $\binom{11}{5} = 462$ b) $\binom{4}{2}\binom{7}{3} = 210$ c) $\binom{4}{3}\binom{7}{2} + \binom{4}{4}\binom{7}{1} = 84 + 7 = 91$

d) $\binom{11}{5} - \binom{9}{3} = 378$

2.11. El alumno debe caminar 5 cuadras hacia el este (de acuerdo al dibujo) y 2 cuadras hacia el norte. En total 7 cuadras. Contamos las veces que decide subir las dos cuadras. Ellas son $\binom{7}{2}$ .O lo que es equivalente contamos las veces que decide ir hacia el este $\binom{7}{5}$, que como sabemos por la propiedad de simetría, son iguales. Ese número, son las posibilidades de caminatas del alumno.

2.12. a) Tenemos $\binom{3+1}{1}$ hasta llegar a *a,* y $\binom{3+5}{3}$ hasta llegar a P. Como son independientes, tenemos un total de $\binom{4}{1}\binom{8}{3} = 224$

b) Contamos hasta llegar a *a*, y luego desde *b* hasta P: $\binom{4}{1}\binom{3+4}{3} = 140$

c) Análogamente, $\binom{4}{1}\binom{4}{1}\binom{4}{2} = 96$

d) Si la calle *ab* está cerrada, calculamos el complemento y luego se lo restamos del total. Notemos que el complemento es exactamente lo que hicimos en el punto b):

2.13. Por cada dos científicos, debe haber al menos una cerradura que no puedan abrir y los otro 4 tienen llave de ésa. Por lo que se necesita 1 cerradura por cada par de científicos, es decir $\binom{6}{2}$ = 15 cerraduras en total, y cada uno lleva $\binom{6-1}{2}$ = 10 llaves, una por cada par de los restantes 5.

2.14. Ordenamos primero los símbolos, de 6! maneras. Quedan entre ellos 5 lugares para ubicar los espacios blancos. De los 18 uso los 2.5 = 10 necesarios quedando 8 por ubicar en (6 + 10 - 1) lugares. Por lo que tenemos un total de $6!\binom{15}{8}$ posibilidades.

2.15. a) 6^{10}

b) $\binom{10}{3}\binom{7}{3}4!$ $\binom{12}{4} - 140 = 355$

2.16. Es el problema de los sombreros para $n = 10$.

2.17. Sea A el conjunto de múltiplos de 4 en el rango requerido. Sea B el conjunto de múltiplos de 100 en ese rango. Entonces $A \cap B$ serán los múltiplos de 400 en ese rango.

Fácilmente se calcula que $|A| = 499$, $|B| = 11$ y $|A \cap B| = 5$, por lo que calculamos $|A| - |B| + |A \cap B| = 499 - 11 + 5 = 485$.

2.18. Sean A el conjunto de números divisibles por 2 en ese rango y B el de los divisibles por 3. Entonces $A \cap B$ son los divisibles por 6 en ese rango.

$|A| = 500.000$, $|B| = 333.333$, $|A \cap B| = 166.666$.

Por lo que $|A \cup B| = 500.000 + 333.333 - 166.666 = 666.667$

2.19. Las cajas son los 12 meses, hay $13 = 1.12 + 1$ objetos (personas), por lo que hay 2 en una misma caja o mes.

2.20. Los días del año son las 365 cajas. Como hay $3.000 \geq 8.365 + 1 = 2.920$, tendremos 8 + 1 personas en una caja, es decir 9 personas que comparten el día de cumpleaños.

2.21. Supongamos que existen cinco números sin la propiedad requerida. Todos ellos tienen resto 0 , 1 o 2 al dividirlo por 3. Si tuviéramos uno con cada uno de los restos posibles, tendríamos que su suma nos daría múltiplo de tres, lo cual es absurdo por la hipótesis. Por lo que hay sólo dos posibles restos. Esas serán las cajas. Como $5 = 2.2+1$, significa que hay una caja en la que hay 3. Lo cual es un absurdo ya que la suma de esos, por tener el mismo resto al dividirlo por tres daría múltiplo de 3. Por lo tanto se cumple lo enunciado.

2.22. Si sumamos los números del uno al quince obtenemos más de 100, lo que prueba lo deseado.

□ Capítulo 3

3.1. Hay 6 correspondencias biunívocas entre {1, 2, 3} y {*A, B, C*} , que son:

$1 \leftrightarrow A, 2 \leftrightarrow B, 3 \leftrightarrow C$; $1 \leftrightarrow A, 2 \leftrightarrow C, 3 \leftrightarrow B$; $1 \leftrightarrow B, 2 \leftrightarrow A, 3 \leftrightarrow C$;
$1 \leftrightarrow B, 2 \leftrightarrow C, 3 \leftrightarrow A$; $1 \leftrightarrow C, 2 \leftrightarrow A, 3 \leftrightarrow B$; $1 \leftrightarrow C, 2 \leftrightarrow B, 3 \leftrightarrow A$.

Y hay 24 entre {1, 2, 3, 4} y {*A, B, C, D*}. Denotando por *n*! al producto de

los primeros n números naturales, es decir a $(n-1)\,(n-2)\cdots 3.2.1$, llamado factorial de n, se ve que hay 3! en el primer caso, y 4! en el segundo. En general, si los dos conjuntos tienen n elementos, entonces la cantidad de correspondencias biunívocas entre ellos es $n!$.

3.2. Las siguientes son correpondencias biunívocas entre los conjuntos dados.

De **N** en **NI**: $n \mapsto 2 \times n - 1$; de **NP** en **CP:** $n \mapsto \left(\frac{n}{2}\right)^2$

3.3. Sí, el conserje puede ubicarlas. Es un problema similar al planteado por el Maestro cuando imaginó que llegaba un contingente con infinitas personas, numeradas 1, 2, 3, 4, 5,… La solución más sencilla es simplemente ubicar primero al contingente de personas a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8,... y luego al contingente b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8,...

Otra solución válida es así: se le pide a cada persona que se mueva de su habitación número k a la habitación número $3k$. De este modo, quedan ocupadas las habitaciones numeradas con múltiplos de 3, es decir las habitaciones número 3, 6, 9, 12, 15,…. Y las restantes habitaciones quedan vacías. Luego, se ubica a la persona a_k en la habitación $3k$ - 2 y a la b_k en la habitación $3k$ - 1.

3.4. Sí, el conserje puede ubicarlas. El problema es un poco más complicado que el anterior, pero se puede resolver con ideas del mismo tipo. Una forma sería, nuevamente, ubicar primero al primer contingente, luego al segundo, luego al tercero, etc., cuidando de que a cada huésped se lo moleste sólo una cantidad finita de veces. Hay otras soluciones también, aunque quizá convenga intentar resolver este problema después de leer hasta el final del capítulo, donde ya se habrán adquirido más herramientas**.**

3.5. Sabiendo la fórmula general, es muy fácil. Por ejemplo:

$$S_{10} = 2 - \frac{1}{2^{10}} = \frac{2\,.\,2^{10} - 1}{2^{10}} = \frac{2^{11} - 1}{2^{10}} = \frac{2.047}{1\,024} = 1{,}999023437$$

$$S_{20} = 2 - \frac{1}{2^{20}} = \frac{2^{21} - 1}{2^{20}} = \frac{2097151}{1048576} = 1.99999904632568359375$$ Análogamente,

(El símbolo $\cong$ significa “aproximadamente igual a”.)

$$S_{100} = \frac{25353012004564588029934064107 51}{12676506002282294014967032053 76} \cong 1.99999999999999999999999999999992$$

Para obtener la fórmula, basta con notar que $1 + 1 = 2, 2 + 2 = 2^2, \ldots, 2^k + 2^k = 2^{k+1}$,

luego $S_n = 1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots + \frac{1}{2^n} = \frac{2^n + 2^{n-1} + \cdots + 2^2 + 2 + 1 + (1 - 1)}{2^n} = \frac{2^{n+1} - 1}{2^n}$

3.6. La serie tiende a $\frac{3}{2}$, pues $\frac{1}{1 - \frac{1}{3}} = \frac{1}{\frac{2}{3}} = \frac{3}{2}$.

3.7. Nos alcanza con tomar $n = 1 + 2^1 + 2^2 + 2^3 + 2^4 + \ldots + 2^{49}$, y vimos que esto es igual a $2^{50} - 1$. Por lo tanto, $n = 2^{50} - 1$ es una respuesta apropiada (también lo es cualquier número mayor que éste).

3.8. Se puede proceder exactamente como se hizo con **N** y **Z**. Una correspondencia biunívoca entre $\mathbf{Q}^+$ y **Q** es:

$\mathbf{Q}^+$	q_1	q_2	q_3	q_4	q_5	q_6	q_7	q_8	q_9	q_{10}	q_{11}	.....
Q	0	q_1	$-q_1$	q_2	$-q_2$	q_3	$-q_3$	q_4	$-q_4$	q_5	$-q_5$	.....

3.9. Consideramos que $A = \{a_1, a_2, a_3, a_4, a_5, \ldots\}$ y $B = \{b_1, b_2, b_3, b_4, b_5, \ldots\}$.
Luego, se hace el cuadro con los elementos de A y de B.
Finalmente, se nombran los elementos siguiendo las diagonales desde abajo izquierda hacia arriba derecha, es decir, (a_1,b_1), (a_2,b_1), (a_1,b_2), (a_3,b_1), (a_2,b_2), (a_1,b_3),...

	b_1	b_2	b_3	$\cdots$
a_1	(a_1,b_1)	(a_1,b_2)	(a_1,b_3)	$\cdots$
a_2	(a_2,b_1)	(a_2,b_2)	(a_2,b_3)	$\cdots$
a_3	(a_3,b_1)	(a_3,b_2)	(a_3,b_3)	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

3.10. Siguiendo la ayuda, sabemos que $A \times B$ es numerable, y que C es numerable, entonces el producto cartesiano de $A \times B$ por C es numerable, y es equivalente a $A \times B \times C$.

3.11. Si se razona como en el problema anterior, se ve que el producto de cuatro conjuntos numerables es numerable, y así sucesivamente, el producto $A_1 \times A_2 \times A_3 \times \cdots \times A_n$ es numerable cuando tenemos n conjuntos numerables , $A_1 \times A_2 \times A_3 \times \cdots \times A_n$ $n \in \mathbf{N}$.

3.12. Si se identifica el polinomio $a \cdot x^2 + b \cdot x + c$ con la terna ordenada de enteros (a, b, c), se ve que este conjunto es identificable con el producto cartesiano $\mathbf{Z} - \{0\} \times \mathbf{Z} \times \mathbf{Z}$. Entonces es el producto de tres conjuntos numerables, por lo tanto es numerable.

3.13. Es la unión de los conjuntos de polinomios con coeficientes enteros de grado 0, 1, 2, 3,…. Como cada uno de estos conjuntos es numerable, entonces su unión también, por ser unión numerable de conjuntos numerables.

3.14. Llamemos $\mathbf{A}_n$ a los números algebraicos obtenidos como raíces de polinomios de grado n, es decir, $\mathbf{A}_n = \{ \alpha \in \mathbf{A} : \alpha$ es raíz de un polinomio con coeficientes enteros de grado $n\}$. Ahora, **A** es la unión (numerable) de los $\mathbf{A}_n$. Como sabemos que unión numerable de conjuntos numerables es numerable, basta ver que cada $\mathbf{A}_n$ es un conjunto numerable. Y esto sale porque a $\mathbf{A}_n$ es la unión de las raíces correspondientes a los polinomios de grado n con coeficientes enteros, que era un conjunto numerable. Es decir, $\mathbf{A}_n$ es "unión numerable de conjuntos finitos", por lo tanto es numerable.

3.15. Si **I** fuera numerable, entonces, como **Q** lo es, también lo sería $\mathbf{Q} \cup \mathbf{I}$. Pero $\mathbf{Q} \cup \mathbf{I} = \mathbf{R}$, por lo que **R** sería numerable. ¡Absurdo! ¡Contradicción! Porque sabemos que **R** no es numerable. El absurdo proviene de haber supuesto

inicialmente que **I** era numerable. Luego, **I** no puede ser numerable.

3.16. Siguiendo los pasos, en el punto (iv) se logra construir una correspondencia biunívoca entre D - B y D, en consecuencia estos dos conjuntos son coordinables.

3.17. Es completamente análogo al problema anterior, puesto que los trascendentes también se pueden obtener de los reales quitándoles un conjunto infinito numerable (el de los algebraicos).

3.18. La (iii). La (ii) también es distinta de todas las filas, pero no corresponde al método de la diagonal.

3.19. a) $\frac{1}{3} = 0{,}333333\ldots$; $\frac{17}{20} = 0{,}85$; $\frac{8}{7} = 1{,}14285714285714\ldots$; $\frac{13}{4} = 3{,}25$; $\frac{96}{25} = 3{,}84$; $\frac{21}{12} = 1{,}75$. Notar que este último tiene desarrollo decimal finito aún cuando el 12 tiene un 3 como factor. Esto se debe a que $\frac{21}{12} = \frac{7}{4}$, y esta última es la fracción irreducible.

b) Si una fracción es de la forma $\frac{m}{10^k}$, con m entero, entonces es claro que su desarrollo decimal es finito. Por ejemplo, $\frac{1}{10} = 0{,}1$ y $\frac{3}{10^2} = 0{,}03$. En general, para $\frac{m}{10^k}$, solo pueden ser distintos de cero los primeros k lugares después de la coma. Ahora si tenemos la fracción $\frac{m}{2^j \cdot 5^k}$, entonces, como $2 \times 5 = 10$, podemos multiplicar numerador y denominador por 10^n, con n igual al máximo entre j y k, nos aseguramos que da entero.

c) Se ve que multiplicando la fracción por cualquier potencia de 10 nunca se llega a obtener un entero, puesto que no se puede simplificar el factor primo del denominador.

d) Es consecuencia de los incisos (b) y (c).

3.20. (i) Es así, porque la función o asignación propuesta, $x \mapsto 2 \cdot x$, del **(0,1)** → **(0,2)**, es una correspondencia biunívoca entre estos dos intervalos.

(ii) Nuevamente, resulta del hecho que la asignación propuesta es una correspondencia biunívoca.

(iii) Si llamamos Φ a la correspondencia biunívoca entre el **(0,1)** y $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, y Ψ a la correspondencia biunívoca entre $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ y **R**, entonces el diagrama muestra que se puede establecer una correspondencia entre **(0,1)** y **R** **(0,1)** $\overset{\Phi}{\longleftrightarrow} \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \overset{\Psi}{\longleftrightarrow}$ R.

3.21. Hay una cantidad numerable de subconjuntos de **N** de un solo elemento. Lo mismo ocurre con los subconjuntos de **N** de dos elementos. También para tres. Y así sucesivamente, Luego, la unión de estos conjuntos es numerable. A su vez esta unión es igual a $P_f(\mathbf{N})$, las partes finitas de **N**.

□ Capítulo 4

4.1. $\mathbf{4 + 3 - 2 \equiv 5}$ ***mod*** $\mathbf{(6)}$ $\qquad$ $\mathbf{10 + 9 - 4 \equiv 4}$ ***mod*** $\mathbf{(11)}$

4.2. $\mathbf{10 + 6 - 3 + 11 \equiv 1}$ ***mod*** $\mathbf{(12)}$; $\quad$ $\mathbf{10 + 6 - 3 + 11 \equiv 9}$ ***mod*** $\mathbf{(15)}$;
$\mathbf{10 + 6 - 3 + 11 \equiv 6}$ ***mod*** $\mathbf{(18)}$; $\quad$ $\mathbf{10 + 6 - 3 + 11 \equiv 2}$ ***mod*** $\mathbf{(22)}$.

4.3. 10+10+10+…=100 y $\mathbf{100 \equiv 1}$ ***mod*** $\mathbf{(11)}$ pues 99 = 9 x 11;
$\mathbf{100 \equiv 4}$ ***mod*** $\mathbf{(12)}$ pues 96 = 8 x 12;
$\mathbf{100 \equiv 0}$ ***mod*** $\mathbf{(20)}$ pues 100 = 5 x 20.

4.4. Los números pares son congruentes a $\mathbf{0}$ ***mod*** $\mathbf{(2)}$ y los impares son congruentes a $\mathbf{1}$ ***mod*** $\mathbf{(2)}$**.** Para calcular $\mathbf{1 + 2 + 3 + \ldots + 98 + 99 + 100}$ ***mod*** $\mathbf{(2)}$ notamos que hay 49 impares y luego la suma es congruente a $\mathbf{49}$ ***mod*** $\mathbf{(2)}$ que es a su vez congruente a $\mathbf{1}$ ***mod*** $\mathbf{(2)}$**.**

4.5. Como $\mathbf{3 + 3 + 3 = 9}$ y $\mathbf{9 \equiv 0}$ ***mod*** $\mathbf{(9)}$, si la cantidad de sumandos el múltiplo de 3 el resultado es 0. Si en cambio la cantidad de sumandos tiene resto 1 en la división por 3, el resultado de la suma es 3 y si la cantidad de sumandos tiene resto 2 en la división por 3, la suma es igual a 6.

4.6. Si $\boldsymbol{m}$ es impar $\boldsymbol{m}$**-1** es par. La suma $\mathbf{1 + 2 + 3 + \ldots + (m - 1) + m}$ es congruente a la suma sin el último sumando $\boldsymbol{m}$, pues $\boldsymbol{m} \equiv \mathbf{0}$ ***mod*** $\mathbf{(m)}$. Luego queda un número par de sumandos que podemos agrupar de a dos. El 1 con el $\boldsymbol{m}$-1, el 2 con el $\boldsymbol{m}$-2, etc. Todas estas sumas de dos sumandos dan $\boldsymbol{m}$. Luego la suma total es congruente a 0 módulo $\boldsymbol{m}$.

4.7. $\mathbf{3 = 0 \times 13 + 3}$; $\mathbf{-3 = -1 \times 13 + 10}$; $\mathbf{3 = 0 \times (-13) + 3}$; $\mathbf{-3 = 1 \times (-13) + 10}$.

4.8. $\mathbf{0 = 0 \times n + 0}$; $\mathbf{n = 1 \times n + 0}$; $\mathbf{-n = -1 \times n + 0}$; $\mathbf{n = -1 \times (-n) + 0}$; $\mathbf{-n = 1 \times (-n) + 0}$.

4.9. Si **n** es positivo: $\mathbf{n = 0 \times 2n + n}$; $\mathbf{-n = -1 \times 2n + n}$; $\mathbf{2n = 2 \times n + 0}$; $\mathbf{-2n = -2 \times n + 0}$.
Si **n** es negativo: $\mathbf{n = 1 \times 2n - n}$; $\mathbf{-n = 0 \times 2n - n}$; $\mathbf{2n = 2 \times n + 0}$; $\mathbf{-2n = -2 \times n + 0}$.

4.10. $\mathbf{13 \equiv 6}$ **mod** $\mathbf{(7)}$**,** $\qquad$ $\mathbf{-18 \equiv 3}$ **mod** $\mathbf{(7)}$**,** $\qquad$ $\mathbf{1743 \equiv 0}$ **mod** $\mathbf{(7)}$**.**

4.11. **26.**

4.12. No, $\mathbf{23 \equiv 7}$ **mod** $\mathbf{(8)}$**.** No, $\mathbf{42 \equiv 0}$ **mod** $\mathbf{(7)}$**.** No, $\mathbf{-37 \equiv 2}$ **mod** $\mathbf{(3)}$**.**

4.13. $\mathbf{76 \equiv 4}$ **mod** $\mathbf{(8)}$ $\qquad$ $\mathbf{83 \equiv 6}$ **mod** $\mathbf{(7)}$ $\qquad$ $\mathbf{-22 \equiv 2}$ **mod** $\mathbf{(3)}$

4.14. Los cuadrados perfectos son:

Para $\boldsymbol{Z}_2$: 0, 1. $\quad$ Para $\boldsymbol{Z}_3$: 0, 1. $\quad$ Para $\boldsymbol{Z}_4$: 0, 1.
Para $\boldsymbol{Z}_5$: 0, 1, 4 $\quad$ Para $\boldsymbol{Z}_6$: 0, 1, 3, 4 $\quad$ Para $\boldsymbol{Z}_7$: 0, 1, 2, 4
Para $\boldsymbol{Z}_8$: 0, 1, 4

4.15. Si **a** y **b** son unidades, entonces existen **c** y **d** tales que $\mathbf{ac \equiv 1}$ y $\mathbf{bd \equiv 1}$. Luego, como

el producto es asociativo y conmutativo, tenemos que: **(ab)(cd) ≡ (ac)(bd) ≡ 1**. Es decir **ab** es una unidad y su inverso multiplicativo es **cd**.

4.16. Tiene 3 soluciones: **5**, **12** y **19**.

4.17. No tiene solución.

4.18. Una manera de encontrarlos es calcular los cuadrados de todos los números de 1 a 12 módulo 13 y listar los posibles resultados y luego hacer lo mismo con 17. Así los residuos cuadráticos módulo 13 son: 1, 3, 4, 9, 10 y 12. Los residuos cuadráticos módulo 17 son: 1, 2, 4, 8, 9, 13, 15 y 16.

4.19. La primera no tiene, pues **$-7 \equiv 6 \bmod (13)$** y vimos que 6 no es residuo cuadrático. La segunda ecuación es equivalente a **$x^2 \equiv 16 \bmod (13)$**, que se obtiene de la anterior multiplicando ambos miembros por 8 el inverso de 5. Luego ya vimos que 16 no es residuo cuadrático módulo 13, por lo tanto la segunda tampoco tiene solución. Finalmente la tercera, si tiene: x=3, la satisface.

4.20. Tenemos que $\left(\frac{11}{29}\right)\left(\frac{29}{11}\right) = (-1)^{5\times 14} = 1$. Es decir $\left(\frac{11}{29}\right)=\left(\frac{29}{11}\right)$. Ahora $\left(\frac{29}{11}\right)=\left(\frac{7}{11}\right)$ pues $29 \equiv 7 \bmod (11)$, y $\left(\frac{7}{11}\right)\left(\frac{11}{7}\right) = (-1)^{3\times 5} = -1$. Es decir $\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right)$.

Sabemos que $-\left(\frac{4}{7}\right)=\left(\frac{2}{7}\right)\left(\frac{2}{7}\right) = 1$. Así concluimos que = 1.

De manera análoga calculamos que $\left(\frac{23}{61}\right) = 1$.

4.21. Con **m = 6**: ZXGOMGT GMAG E VGT
Con **m = 11**: ECLTRLY LRFL J ALY
Con **m = 19**: MKTBZTG TZNT R ITG

4.22. FELICITACIONES LO LOGRASTE

□ Capítulo 5

Ejercicio 5.1:

a) (agrupada en bloques de 4 letras para mejor lectura)

PCQL PAEF BHYP ABWZ KFVE UCSL PH

b) QMZP HQHT ORXB IHTB PAHB DOPR QOAT ATWP EFUI

Ejercicio 5.2:

1/5 mod 11=9 (observar que 9.5=45=44+1 es congruente a 1 modulo 11).
1/7 mod 11=8 (observar que 7.8=56=55+1 es congruente a 1 modulo 11)

1/6 mod 11=2 (observar que 2.6=12=11+1 es congruente a 1 modulo 11).
1/5 mod 13=8 (observar que 5.8=40=39+1 es congruente a 1 modulo 13)
1/2 mod 7=4 (observar que 2.4=8=7+1 es congruente a 1 modulo 7).

Ejercicio 5.3:

a) 7 b) 8

Ejercicio 5.4:

1) 10, 30, 26, 22 2)15. 3)109, 138, 97, 165
4) Debería obtener el número que pensó. Por ejemplo, tomando como clave 7, y encriptando el número 2, la primera encriptación da el número 23, encriptando este, obtenemos otra vez el número 2.

Ejercicio 5.5, para pensar, más difícil:

ANTES DE LEER ESTAS SOLUCIONES OTRA VEZ RECOMENDAMOS HACERLAS ANTES.

1) Como deben ser coprimas con 24, las únicas claves posibles son 5,7, 11, 13, 17, 19 y 23.
Recordemos que dada una clave pública e, la clave privada es el único d tal que $e.d$ es congruente a 1 módulo $(p-1)(q-1)$. Pero es fácil ver que cada uno de los números e=5,7,11,13,17,19,23 satisface $e.e$=1 mod 24. Por lo tanto, son todos su propia clave privada de desencriptacion, lo que significa que al encriptar dos veces en realidad encriptamos y desencriptamos, con lo que obtenemos el número original.

2) El que conozca pq y $(p-1)(q-1)=pq-(p+q)+1$, haciendo $pq-(p-1)(q-1)+1$ obtiene $p+q$. Por lo que conoce pq y $p+q$. Pero es bien sabido que el que conoce la suma y el producto de dos números los puede calcular pues p y q son las raíces de la ecuación $x^2-(p+q)x+pq=0$.

Ejercicio 5.6:

1) (89-1)(97-1)=8448,
8448=23.367+7;
23=3.7+2;
7=3.2+1:

Por lo tanto, podemos escribir:
1=7-2.3=7-(23-3.7).3=10.7-23.3=10.(8448-23.367)-23.3=10.8448-23.3673

La clave privada sería entonces (-3673) mod 8448=8448-3673=4777.

2) (59-1)(101-1)=5800;
5800=31.197+3;
31=3.10+1;

Por lo tanto:
1=31-3.10=31-(5800-31.187).10=31.1871-58000

Con lo cual la clave privada es 1871.

Bibliografía y Referencias

- **Aritmética elemental en la formación matemática I**, OMA 1992
- Bogart, Kennet P.; Doyle, Peter G **Non-sexist solution of the ménage problem**, (1986)". American Mathematical Monthly 93(7) 514-519. http://math.dartmouth.edu/~doyle/docs/menage/menage/menage.html
- Burger E. B.; Starbird M. **Heart of Mathematics**, (2006).
- Chen Chuan-Chong, Koh Khee-Meng **Principles and Techniques in Combinatorics**,Word Scientific, 1992.
- Courant R, Robbins H.**¿Qué es la Matemática?** R. Courant y H. Robbins (1955). Traducción del Original: What is Mathematics? (1941)
- Enzensberger Hans Magnus **El diablo de los números,** Siruela (1997).
- Gentile Enzo **Notas de álgebra I**, , Editorial Eudeba 1984
- Kemeny, Snell, Thompson **Introduction to Finite Mathematics**,. Prentice-Hall, Inc, 1956.
- Kisbye N. Patricia , MiatelloRoberto J. **Notas Álgebra I - Matemática Discreta I**, FAMAF UNC, Serie C.
- Paenza Adrián **Matemática… ¿estás ahí?** (4 Episodios). Colección Ciencia que ladra, Siglo XXI, (2005). Editorial: Perro que ladra.
- Slomson, Alan **An Introduction to Combinatorics**,. Chapman & Hall/Crc, 1991.
- Steward Ian **De aquí al infinito**. Drakontos 1998
- Tahan Malba **El Hombre que Calculaba**.
- Tait P.G. **On knots, i, ii, iii**,.. In Scientific Papers. Páginas. 273-347. Cambridge Univ. Press, Cambridge, 1898.
- Touchard J. **Sur un problème des permutations**.. C. R. Acad. Sciences Paris, 198:631-633, 1934.

Sitios web:

- http://es.wikipedia.org/wiki/Número_primo
- http://es.wikipedia.org/wiki/Teorema_fundamental_de_la_Aritmética
- http://es.wikipedia.org/wiki/Test_de_primalidad
- http://primes.utm.edu/

Leandro Cagliero
Doctor en Matemática

Paulo Tirao
Doctor en Matemática

Daniel Penazzi
Doctor en Matemática

Juan Pablo Rossetti
Doctor en Matemática

Ana Sustar
Licenciada en Matemática

"Aventuras Matemáticas".

¿Sabías que estás rodeado de matemática y hacés matemática a diario?

¿Sabías que cuando recargás tu celular se procesan números primos enormes?

Si tu ómnibus salió a las 10 de la noche y demoró 9 horas, ¿a qué hora llegaste?

¿Te diste cuenta que a veces $10 + 9 = 7$?

Aunque te parezca increíble, en cualquier fiesta, ¡siempre hay dos personas que han saludado a la misma cantidad de invitados!

¿Podés creer que hay exactamente la misma cantidad de números naturales que de números pares?

¿Sabías que hay un premio de 1 millón de dólares para quien descubra cómo están distribuidos los números primos entre los números naturales?

¡Qué atrapante es la matemática!

En este libro encontrarás algunas de estas verdades y misterios tratados de manera amena y profunda.

Ministerio de Educación
Presidencia de la Nación

OEI

inet
Instituto Nacional de Educación Tecnológica