1. Los maravillosos números primos

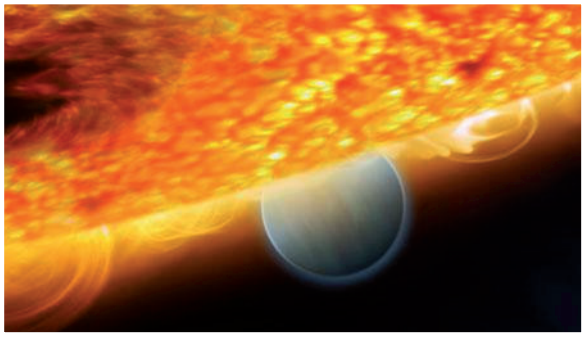
Por Leandro Cagliero

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

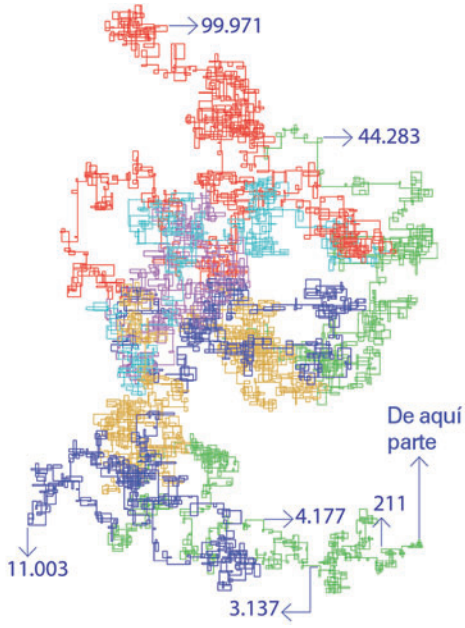
Descubrir planetas fuera del sistema solar que contengan dióxido de carbono en su composición química.

"... 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.

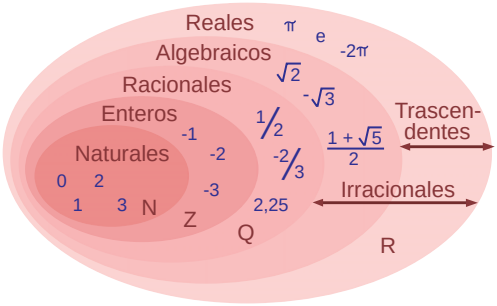
1.1. Los números naturales, cimientos de la matemática

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:

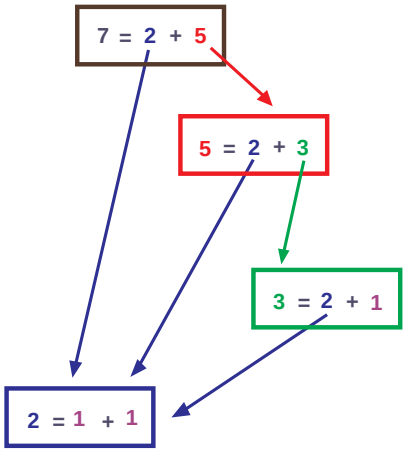


Figura 1.1: Partición del número 7 con la adición

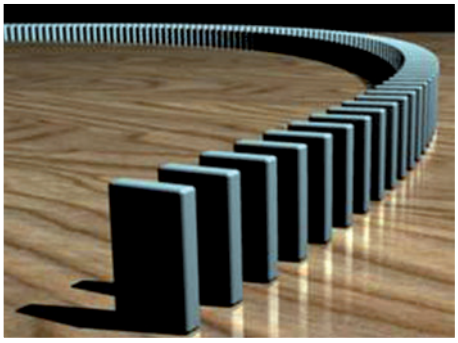
a.- utilizando la adición, ¿cómo están hechos los números naturales?;
b.- utilizando la multiplicación, ¿cómo están hechos los números naturales?

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.

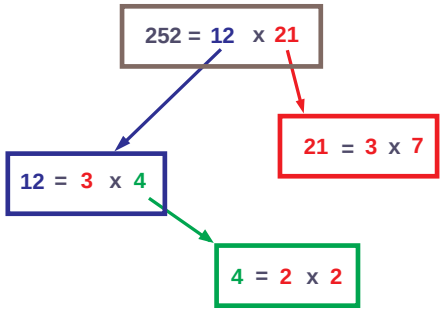


Figura 1.2: Partición del número 252 con la multiplicación.

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

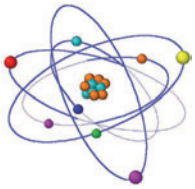
¿Cómo son los siguientes números? ¿Es alguno de ellos primo?

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**):

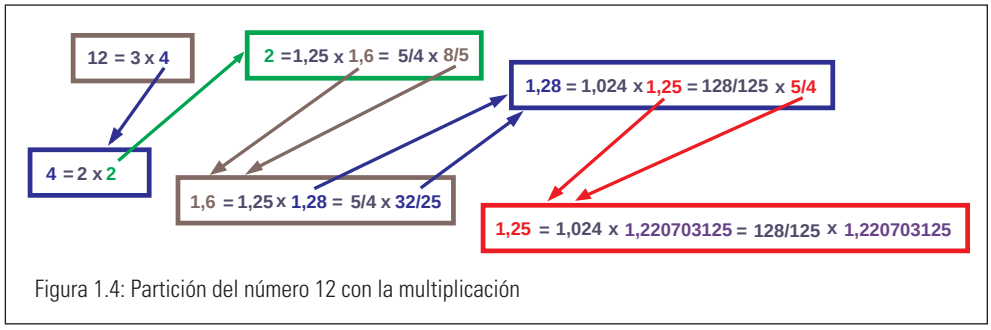


Figura 1.4: Partición del número 12 con la multiplicación

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***?

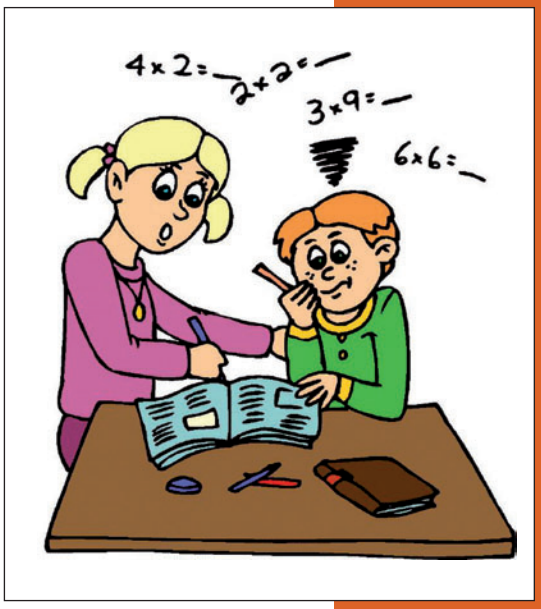
Para resolver

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%.

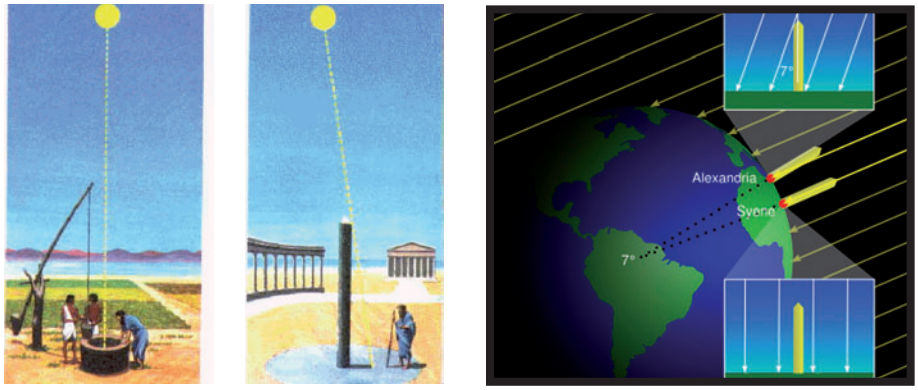


Figura 1.5 Eratóstenes mide el radio de la Tierra durante el solsticio de verano en Egipto

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"*.

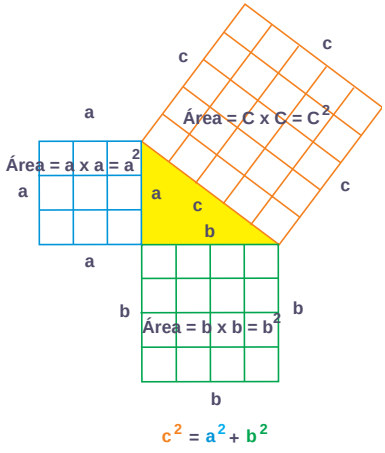


Figura 1.6 Ternas pitagóricas

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, viâ
Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS

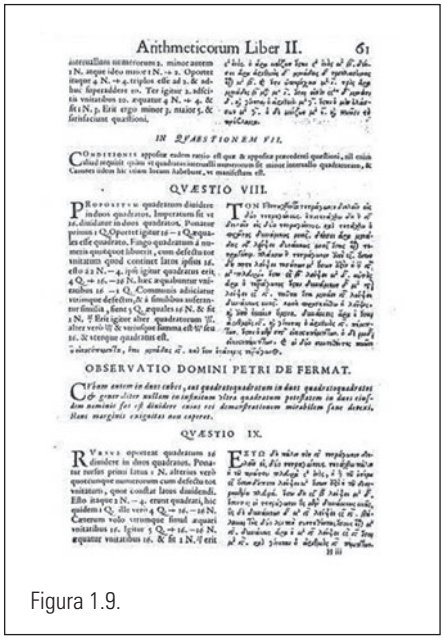
Figura 1.7.


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	

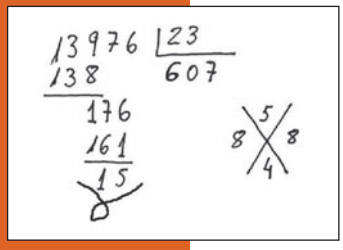
La factorización en primos de 12.345.678 es $2 \times 3^2 \times 47 \times 14.593$.

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

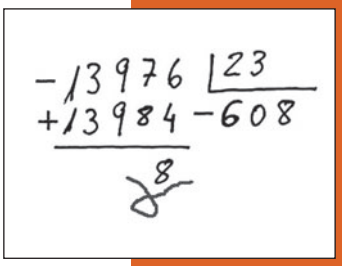


Antes de seguir adelante con las preguntas de la **Sección 2** recordemos el *algoritmo de división*, porque es una herramienta fundamental para trabajar con números naturales o enteros.

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:
0, 18, 36, 54, 72, 90, 108, …

Múltiplos de 7:
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:

$$r_0 = a \times n - b \times p \quad (1)$$
$$t \times r_0 = t \times a \times n - t \times b \times p \quad (2)$$
$$t \times r_0 + r = t \times a \times n - t \times b \times p + r \quad (3)$$
$$p = t \times a \times n - t \times b \times p + r \quad (4)$$

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:

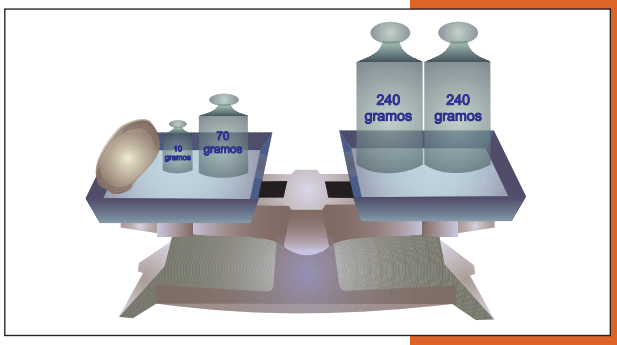
$$a \times m \times n - b \times p \times n = n$$

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.

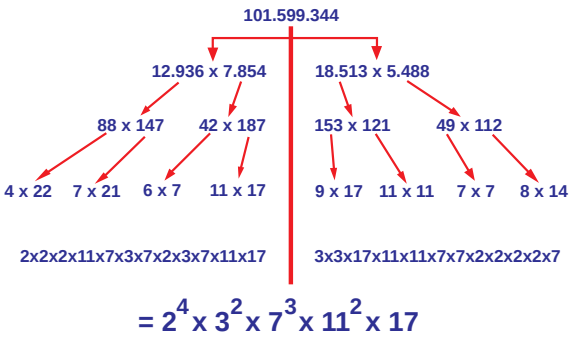


Figura 1.10 Dos caminos para el factoreo del número 101.599.344

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%

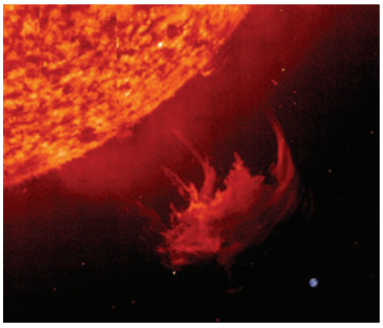


Figura 1.11 Foto del Sol de la NASA en la cual se ha incorporado a la Tierra en tamaño relativo

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

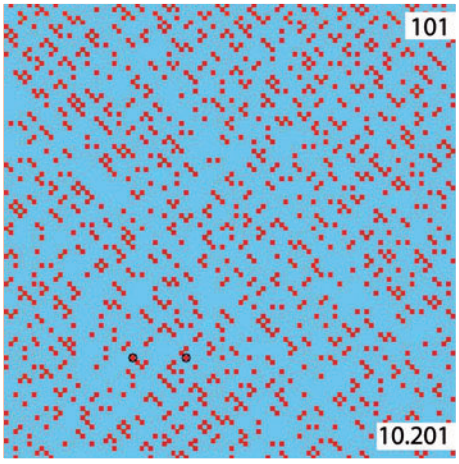


Figura 1.13 Criba de Eratóstenes hasta el número 10.201, cuya raíz cuadrada es 101.

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.

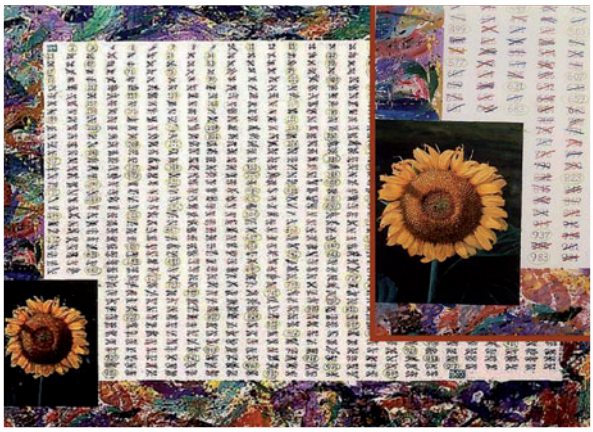
¿Qué sería lo ideal? Sería encontrar un método para factorear tal que la cantidad de operaciones requerida sea lo más cercana posible a la **cantidad de cifras del número**. Hoy se conocen buenos métodos de factoreo, pero para nada se está cerca de encontrar uno que requiera una cantidad de operaciones 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 $a2$:
Paso tipo 2: $a2$ es $2 \times 617.283.945.505.560.657.075.808.590.960$ (sencillo).
Paso tipo 1: 2 es primo (sencillo).
Paso tipo 2: 617.283.945.505.560.657.075.808.590.960 es $2 \times$
$\times$ 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 $2 \times$
$\times$ 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 $2 \times$
$\times$ 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 $2 \times$
$\times$ 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 $5 \times$
$\times$ 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 $3 \times$
$\times$ 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 $\times$
$\times$ 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 $\times$ 2.375.923.237.887.317 $\times$
(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:

$a3$ = 123.456.789.101.112.131.415.161.718.192.021.222.324.252.627.282.930
= $2 \times 3 \times 5 \times 13 \times 49.269.439 \times 370.677.592.383.442.753 \times$
$\times$ 17.333.107.067.824.345.178.861

Tardó 80 segundos en encontrar la factorización de:

$a4$ = 12.345.678.910.111.213.141.516.171.819.202.122.232.425.262.728.293.031.
323.334.353.637.383.940
= $2 \times 5 \times 3.169 \times 60.757 \times 579.779 \times 4.362.289.433 \times 79.501.124.416.220.680.469 \times$
$\times$ 15.944.694.111.943.672.435.829.023

Tardó 8 minutos en encontrar la factorización de:

$a5$ = 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;
= $2 \times 3 \times 5 \times 13 \times 211 \times 20.479 \times 160.189.818.494.829.241 \times 46.218.039.785.302.111.919 \times$
$\times$ 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 $P(N)$ 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

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

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.

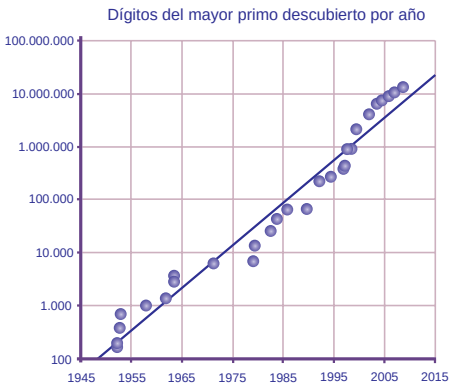
Los primos que se obtienen con la fórmula $2^p - 1$, con p primo, se conocen como primos de Mersenne. En el año 1856 Édouard Lucas descubre un método muy rápido para determinar si $2^p - 1$ es primo o compuesto. Desde entonces y hasta hoy, han sido la principal fuente de récord para primos grandes. A 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:

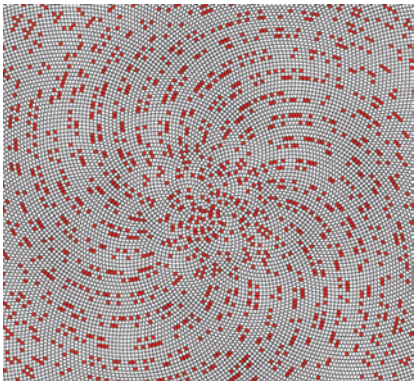
$$2^{43.112.609} - 1 \text{ y } 2^{32.582.657} - 1$$

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.



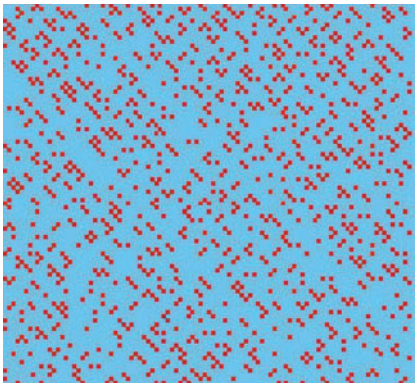


Figura 1.14 Abajo: primos menores que 10.201 distribuidos en un cuadrado de lado 101. Arriba: imagen extraída del la página web del Prof. Mark Dickinson (www.pitt.edu/~dickinsm/), del Dto. de Matemática de la Universidad de Pittsburg, se distribuyeron los primos en un esquema de flor de girasol.

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.

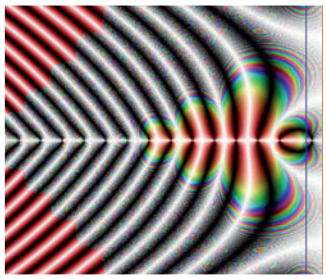


Figura 1.15. Gráfico del argumento de ζ, la línea azul corresponde a parte real 1/2.

- 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

Bernhard Riemann 1826 - 1866

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

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.