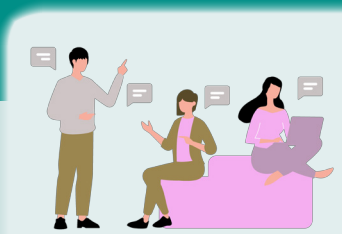
Leñitas Geométricas*

para el Fogón Matemático de los Festivales

De OMA para estudiantes, profesores y maestros en actividad

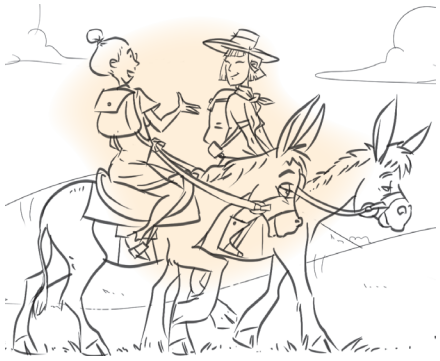
7ª época • Nº 1 • 27 de marzo de 2025



"[...] más valioso que acumular información es interiorizarse de métodos para saber qué propósitos tienen, es decir, de dónde parten y adónde llevan. Los métodos tienen una orientación y una dinámica de las cuales los resultados y teoremas aislados carecen". *Dr. Alberto Calderón*

I. Dialogando con los maestros sobre los números y las transformaciones rígidas

¿Qué es la matemática y la... imaginación, creatividad y aventuras del pensamiento?

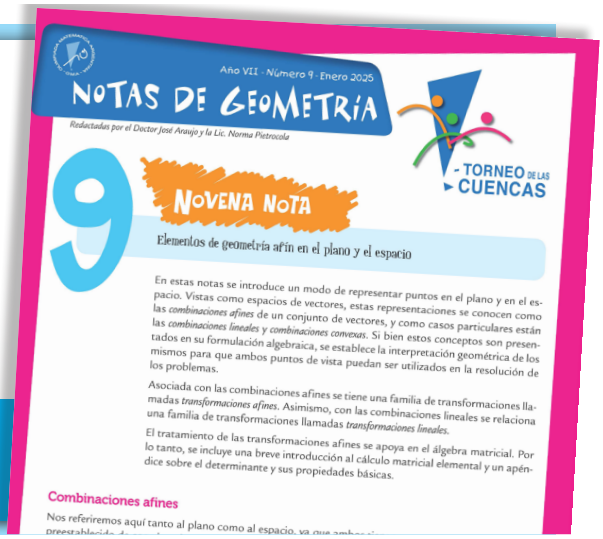


Desde hace más de dos milenios, una cierta familiaridad con la matemática ha sido considerada virtud indispensable de la formación intelectual de toda persona cultivada. En la actualidad, sin embargo, se halla en grave peligro el puesto ocupado tradicionalmente en la educación por esta disciplina; y por desgracia, algunos de los profesionales que la representan comparten la responsabilidad de tal situación. La enseñanza de la matemática ha degenerado con frecuencia en un vacío entrenamiento de resolución de problemas que, si bien puede desarrollar una habilidad formal, no conduce en cambio a una comprensión efectiva ni a una mayor independencia intelectual.

La investigación matemática muestra una tendencia hacia la súperespecialización y una excesiva insistencia en lo abstracto; las aplicaciones y conexiones con otros campos del saber han sido descuidadas. Sin embargo, tal estado de cosas no debe justificar una política de retraimiento. Por el contrario, la reacción opuesta puede y debe partir de aquellos que se sienten conscientes del valor de la disciplina intelectual. Profesores, estudiantes y público culto piden una reforma constructiva y no una resignación siguiendo la línea de menor resistencia. La meta será una verdadera comprensión de la matemática como un todo orgánico y como base para el pensamiento y la acción científicos.

Algunos libros espléndidos de biografía e historia y otros más populares han estimulado el interés general latente; pero el conocimiento no puede adquirirse utilizando únicamente medios indirectos. La comprensión

Elementos de geometría afín en el plano y en el espacio



fenchu@oma.org.ar

11 4826 8976

+54 9 11 5035 7537

red olímpica

¡Hacé tu pedido!

En la Red Olímpica realizamos envíos de todos nuestros títulos a todo el país bajo el sistema contra reembolso o delivery.

* Recordamos a los lectores que los temas editados en *Leñitas Geométricas* son material preparado y en gran parte desarrollado y sugerido por el doctor Miguel de Guzmán y los doctores Richard Courant, Herbert Robbins y Roger Penrose.

de la matemática no puede ser transmitida indirectamente o como un juego sin dificultades, como tampoco pueden adquirir una educación musical a través de reseñas periodísticas brillantes aquellos que no hayan escuchado buena música con frecuencia. Un contacto real con el contenido de la matemática viva es necesario.

Sin embargo, cabe evitar algunos detalles de técnica y muchas digresiones; la presentación de la matemática debe estar tan libre de excesos de rutina como del dogmatismo prohibitivo que rehúye revelar el motivo o la meta y que constituye así un obstáculo de mala fe a un esfuerzo honesto. Es posible seguir una ruta directa a partir de los elementos fundamentales hasta puntos avanzados, desde los cuales puedan divisarse la sustancia y las fuerzas directrices de la matemática moderna.

Desde hace tiempo hacemos un intento en esta dirección. Y en tanto que presupone únicamente los conocimientos que pueden adquirirse en la enseñanza media, puede considerarse como elemental. No obstante, no constituye una concesión a la tendencia peligrosa que consiste en soslayar toda dificultad. Su lectura requiere un cierto grado de madurez intelectual y un deseo de tener pensamientos propios. Está escrito para principiantes y entendidos, para estudiantes y profesores, para filósofos e ingenieros, tanto como para preparar texto o como consulta. Seguramente tenemos una intención demasiado ambiciosa. De todos modos, se espera que pueda servir un propósito útil y constituir una contribución a la educación.

Introducción. ¿Qué es la matemática?

La matemática, como una expresión de la mente humana, refleja la voluntad activa, la razón observadora y el deseo de perfección estética. Sus elementos básicos son: lógica e intuición, análisis y construcción, generalidad y particularidad. Aunque diversas tradiciones han destacado aspectos diferentes, es únicamente el juego de estas fuerzas opuestas y la lucha por su síntesis lo que constituye la vida, la utilidad y el supremo valor de la ciencia matemática.

Sin duda, todo el desarrollo matemático ha tenido sus raíces psicológicas en necesidades más o menos prácticas. Pero una vez en marcha, bajo la presión de las aplicaciones necesarias, dicho desarrollo gana impulso en sí mismo y trasciende los confines de una utilidad inmediata. Esta tendencia de la ciencia aplicada hacia la teórica aparece tanto en la historia antigua como en muchas de las contribuciones a la matemática moderna debidas a ingenieros y físicos.

La historia de las matemáticas comienza en Oriente donde, hacia el año 2000 a. C., los babilonios poseían ya una gran cantidad de material que podría ser clasificado hoy como perteneciente al álgebra elemental. Pero como ciencia, en el sentido moderno, la matemática aparece más tarde, en Grecia, entre los siglos V y IV a. C. El contacto creciente entre el Oriente y los griegos, que comienza en los tiempos del imperio persa y culmina en el periodo que sigue a las expediciones de Alejandro, puso a los griegos al corriente de los conocimientos de los babilonios en matemática y astronomía.

La matemática fue sometida entonces a las discusiones filosóficas que florecieron en las ciudades griegas. Los pensadores griegos se dieron pronto cuenta de las grandes dificultades inherentes a los conceptos matemáticos de continuidad, movimiento e infinitud, así como al problema de medir magnitudes arbitrarias con unidades prefijadas.

Entonces, fue llevado a cabo un admirable esfuerzo para vencerlas y el resultado, la teoría de Eudoxio del continuo geométrico, fue de tal perfección que para encontrar algo que pudiera comparársele fue necesario que, dos milenios más tarde, apareciera la teoría moderna de los números irracionales.

La tendencia axiomático-deductiva en matemáticas tuvo su origen en tiempos de Eudoxio (390-337 a. C.) y cristalizó en los *Elementos* de Euclides. Sin embargo, aunque la tendencia teórica y axiomática de la matemática griega es una de sus más importantes características y ha ejercido una influencia enorme, nunca se insistirá demasiado en que las aplicaciones y conexiones con la realidad física desempeñaron un papel importante como parte de la matemática de la Antigüedad, y que en muchas ocasiones fue preferido un modo de exposición menos rígido que el de Euclides.

Es muy posible que el descubrimiento de las dificultades relacionadas con las cantidades inconmensurables desviara a los griegos del desarrollo del cálculo numérico, alcanzado con anterioridad en Oriente. En su lugar, se abrieron camino a través de la geometría axiomática pura. Y así comenzó un extraño rodeo en la historia

de la ciencia, y quizá se perdió una gran oportunidad. Durante casi dos mil años el peso de la tradición geométrica griega retrasó la inevitable evolución del concepto de número y el desarrollo del cálculo algebraico que, más tarde, habían de ser la base de la ciencia moderna.

Después de un periodo de preparación lenta, la revolución en la matemática y en la ciencia comenzó su fase vigorosa en el siglo XVII, con la geometría analítica y el cálculo diferencial e integral. Mientras la geometría griega conserva aún un lugar destacado, el ideal griego de cristalización axiomática y de deducción sistemática desaparece durante los siglos XVII y XVIII. Razonamientos lógicos rigurosos, a partir de definiciones claras y no contradictorias, axiomas evidentes fueron cuestiones sin importancia para los nuevos exploradores de la ciencia matemática. En una verdadera orgía de conjeturas intuitivas, de razonamientos convincentes entrelazados con un misticismo sin sentido, con una confianza ciega en el poder sobrehumano de los procesos formales, conquistaron un mundo matemático de inmensas riquezas.

Luego, gradualmente, la exaltación del progreso dejó el paso a un espíritu de autocrítica. En el siglo XIX, la necesidad inmanente de consolidar y el deseo de una mayor seguridad en la extensión de la enseñanza superior, que había impulsado la Revolución francesa, condujeron inevitablemente a una revisión de los fundamentos de la nueva matemática, en particular del cálculo diferencial e integral, así como del concepto fundamental de límite. Así, el siglo XIX constituyó no solo un periodo de nuevos avances, sino que además puede caracterizarse por un afortunado retorno al ideal clásico de precisión y demostraciones rigurosas. Y en este sentido llegó a superar al modelo de la ciencia griega. Una vez más, el péndulo se inclinó del lado de la pureza lógica y de la abstracción. Actualmente vivimos aún en este periodo, aunque es de esperar que la desafortunada separación entre la matemática pura y las aplicaciones a la vida, quizá inevitable en tiempos de revisión crítica, venga seguida de una era de íntima unidad.

La renovada solidez interna y, sobre todo, la simplificación enorme alcanzada sobre la base de una comprensión más clara hacen posible hoy dominar la teoría matemática sin perder de vista las aplicaciones. Establecer de nuevo una unión orgánica entre ciencia pura y ciencia aplicada y un equilibrio estable entre la generalidad abstracta y la individualidad concreta puede ser muy bien la tarea universal de la matemática en el futuro inmediato.

No es este el lugar para un análisis filosófico o psicológico detallado de la matemática. Únicamente podemos destacar algunos puntos. Parece existir un grave peligro en el excesivo predominio del carácter axiomático-deductivo de las matemáticas. Ciertamente, el elemento de invención constructiva, de intuición directora, escapa a una simple formulación filosófica; sin embargo, continúa siendo el núcleo de todo resultado matemático, aun en los campos más abstractos.

Si la forma deductiva cristalizada es la meta, la intuición y la construcción son, cuando menos, las fuerzas directrices. Una amenaza seria para la verdadera vida de la ciencia aparece contenida en la afirmación de que la matemática no es más que un sistema de conclusiones derivadas de definiciones y postulados que deben ser compatibles, pero que, por lo demás, pueden ser creación de la libre voluntad del matemático. Si esta descripción fuera exacta, la matemática no podría interesar a ninguna persona inteligente. Sería un juego con definiciones, reglas y silogismos, sin meta ni motivo alguno.

La noción de que el intelecto puede crear sistemas de postulados plenos de significado de modo arbitrario es una verdad a medias decepcionante. Únicamente bajo una disciplina de responsabilidad frente a un todo orgánico, guiada solo por necesidades intrínsecas puede la mente libre obtener resultados de valor científico.

Aunque la tendencia contemplativa del análisis lógico no puede representar toda la matemática, ha conducido, sin embargo, a una comprensión más profunda y clara de los hechos matemáticos y de su interdependencia, y también a una mayor penetración en la esencia de los conceptos matemáticos. A partir de ella se ha desarrollado un punto de vista moderno en las matemáticas, que es característico de una actitud científica universal.

Cualquiera que sea el punto de vista filosófico, para todos los propósitos de observación científica, un objeto agota en sí la totalidad de relaciones posibles respecto del observador o del instrumento. Naturalmente, la simple percepción no constituye conocimiento; debe ser coordinada e interpretada con referencia a alguna entidad subyacente, una cosa en sí, que no es un objeto de la observación física directa, sino que pertenece a la metafísica.

Sin embargo, en el proceso científico es importante descartar los elementos de carácter metafísico y considerar los hechos observables como la última fuente de nociones y construcciones. Renunciar a la meta de

comprender la "cosa en sí", de conocer la "realidad última", de desentrañar la esencia más íntima del mundo, puede ser psicológicamente penoso para entusiastas ingenuos, pero de hecho es uno de los sacrificios de consecuencias más fecundas en el pensamiento moderno.

Algunos de los mayores avances en la física han sido el premio a una adhesión decidida al principio de eliminar la metafísica. Cuando Albert Einstein consiguió reducir la noción de sucesos simultáneos que ocurren en lugares distintos a fenómenos observables; cuando señaló como prejuicio metafísico la creencia de que este concepto debe tener un significado científico en sí mismo, encontró la clave de su teoría de la relatividad. Cuando Niels Bohr y sus discípulos analizaron el hecho de que toda observación física va acompañada de un "efecto del instrumento observación sobre el objeto observado", se hizo claro que el intento de fijar simultáneamente la posición y la velocidad de una partícula no es posible en el sentido de la física. Las consecuencias de este descubrimiento, contenidas en la teoría moderna de la mecánica cuántica, son hoy familiares a todo físico.

En el siglo XIX prevaleció la idea de que las fuerzas mecánicas y los movimientos de partículas en el espacio eran cosas en sí mismas, mientras que electricidad, luz y magnetismo debían ser reducidos o explicados como fenómenos mecánicos, de la misma manera que se hacía con el calor. El éter fue inventado como medio hipotético capaz de los movimientos mecánicos no explicados satisfactoriamente y que aparecían bajo las formas de luz y electricidad. Poco a poco se comprendió que el éter era necesariamente inobservable; por consiguiente, no pertenecía a la física, sino a la metafísica. Con pena por algunos y con satisfacción por otros, las explicaciones mecánicas de la luz y la electricidad, y con ellas el éter, debieron ser finalmente abandonadas.

Una situación análoga, quizá más acentuada, existe en la matemática. A través de los tiempos, los matemáticos consideraron sus objetos, tales como números, puntos, etc., como cosas sustanciales en sí. Pero en vista de que estos entes desafiaban siempre los intentos para una descripción adecuada, los matemáticos del siglo XIX llegaron paulatinamente a la convicción de que el problema de la significación de dichos objetos como cosas sustanciales no tenía en modo alguno sentido dentro de la matemática. Las únicas proposiciones relativas a ellos que pueden importar no se refieren a su realidad sustancial; representan únicamente las relaciones mutuas entre objetos "matemáticamente indefinidos" y las reglas que rigen las operaciones con ellos.

Lo que "realmente" son los puntos, las rectas y los números ni se puede ni es necesario discutirlo en la ciencia matemática. Lo que interesa y lo que corresponde a hechos comprobables es su estructura y relación: que dos puntos determinan una recta, que los números se combinan según ciertas reglas para formar otros números, etc. La percepción clara de la necesidad de una axiomatización de los conceptos matemáticos elementales ha sido uno de los resultados más importantes y fecundos del desarrollo moderno de la matemática.

Por suerte, las mentes creadoras olvidan las creencias filosóficas dogmáticas cuando la persistencia en ellas podría impedir resultados constructivos. Tanto para entendidos como para profanos, no es la filosofía, y sí únicamente la experiencia activa en matemáticas la que puede responder a la pregunta: ¿qué es la matemática?

Los números naturales

INTRODUCCIÓN

Los números son la base de la matemática moderna. Ahora bien: ¿qué es un número? ¿Qué significado tiene decir $\frac{1}{2}+\frac{1}{2}=1$, $\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{4}$ y $(-1)(-1) = 1$? En la segunda enseñanza se aprende el manejo de las fracciones y de los números negativos, pero una comprensión efectiva de los sistemas de números requiere investigar sus elementos más simples. Mientras los griegos hacen de los conceptos geométricos de punto y recta la base de sus matemáticas, hoy se admite como principio director que todas las proposiciones matemáticas pueden ser reducidas en última instancia a proposiciones sobre los números naturales: 1, 2, 3, ... "Dios creó los números naturales; el resto es obra de los hombres": con estas palabras Leopold Kronecker (1823-1891) señaló la base precisa sobre la cual puede construirse el edificio de la matemática.

Creados por la mente humana para contar objetos agrupados de diversos modos, los números no contienen referencia alguna a las características de los objetos contados. El número 6 es una abstracción obtenida a

partir de todas las colecciones que contienen seis cosas; no depende de las cualidades específicas de dichas cosas ni de los símbolos usados para representarlas. Solo en etapas avanzadas del desarrollo intelectual llega a percibirse con toda claridad el carácter abstracto de la idea de número. Para los niños, los números están siempre ligados a objetos tangibles, tales como dedos o bolas, y los lenguajes primitivos dan a los números un sentido concreto, designando con palabras distintas los números que incumben a diferentes tipos de objetos.

Por suerte, los matemáticos no tienen que ocuparse del aspecto filosófico de la transición que da el paso de colecciones de objetos concretos al concepto abstracto de número. Consideraremos, por tanto, como dados los números naturales, junto con las dos operaciones fundamentales, adición y multiplicación, mediante las cuales pueden ser combinados.

CÁLCULO CON NÚMEROS ENTEROS

1. Leyes de la aritmética

La teoría matemática de los números naturales o enteros positivos se conoce con el nombre de *aritmética*. Se basa en el hecho de que la adición y la multiplicación de enteros están regidas por ciertas leyes. Para enunciar estas leyes con toda generalidad no podemos limitarnos a usar símbolos tales como 1, 2, 3, que se refieren a enteros particulares. La proposición

$$1 + 2 = 2 + 1$$

es únicamente un caso particular de la ley general que dice que la suma de dos enteros no depende del orden en que estos se consideren. En consecuencia, si queremos expresar el hecho de que una cierta relación entre enteros es válida, cualesquiera que sean los valores de los enteros considerados, debemos representarlos simbólicamente mediante letras: a, b, c, ... De acuerdo con esto podemos enunciar las conocidas cinco leyes fundamentales de la aritmética:

1) $a + b = b + a$.

2) $a\,b = b\,a$.

3) $a + (b + c) = (a + b) + c$.

4) $a\,(b\,c) = (a\,b)\,c$.

5) $a\,(b + c) = a\,b + a\,c$.

Las dos primeras son las leyes *conmutativas* de la adición y de la multiplicación; indican que el orden de los elementos que intervienen en dichas operaciones puede ser alterado. La tercera, que es la ley *asociativa de la adición,* dice que en la adición de tres números se obtiene el mismo resultado si se añade al primero la suma del segundo y el tercero, o al tercero la suma del primero y el segundo. La cuarta es la ley *asociativa de la multiplicación*. La última, que es la ley *distributiva*, expresa que para multiplicar una suma por un entero se puede multiplicar cada término de la suma por dicho entero y sumar luego los productos obtenidos.

Estas leyes de la aritmética son muy simples e incluso parecen evidentes. Sin embargo, pueden no ser aplicables a otros entes distintos de los números enteros. Así, si a y b son símbolos no de enteros, sino de sustancias químicas, y si *adición* se entiende en su sentido corriente, es evidente que la ley conmutativa no es siempre válida; por ejemplo, si se añade ácido sulfúrico al agua se obtiene una solución diluida, mientras que la adición de agua a ácido sulfúrico puro puede acarrear consecuencias catastróficas para el experimentador.

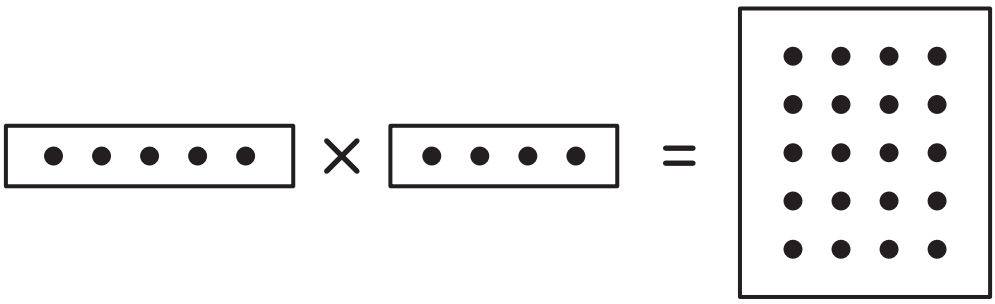
Análogas consideraciones probarían que, en este tipo de "aritmética" química, las leyes asociativa y distributiva de la adición pueden muy bien no ser ciertas. Asimismo, es probable imaginar tipos de aritméticas en las cuales alguna o varias de las leyes 1) a 5) no sean válidas. De hecho, tales sistemas son estudiados efectivamente en la matemática moderna.

Un modelo concreto para el concepto abstracto de entero indicará bien las bases intuitivas sobre las que reposan las leyes 1) a 5). En vez de usar los símbolos habituales 1, 2, 3, ..., representemos los enteros que dan el número de objetos de una colección determinada (por ejemplo, colección de manzanas de un árbol particular) mediante puntos situados en casillas rectangulares, de modo que a cada objeto corresponda un punto. Operando con estos rectángulos se pueden estudiar las leyes de la aritmética de los enteros. Para

sumar dos enteros *a* y *b*, dispongamos los rectángulos correspondientes uno contiguo al otro, suprimiendo la raya de separación.

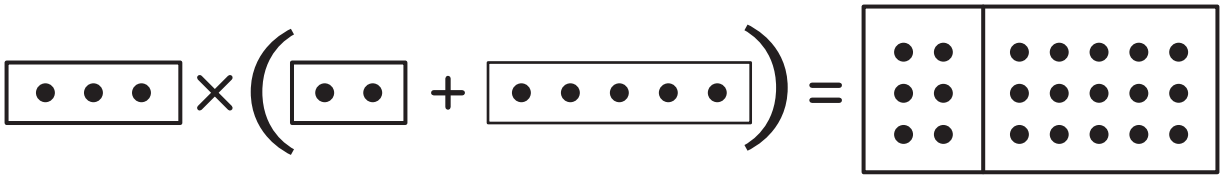
Adición.

Para multiplicar *a* por *b*, coloquemos los puntos de los dos rectángulos en filas y formemos un nuevo rectángulo con *a* filas y *b* columnas de puntos.



Multiplicación.

Corresponderán entonces de modo intuitivo a propiedades evidentes de las operaciones indicadas con los rectángulos. Las reglas 1) a 5) corresponden a las propiedades intuitivas obvias de cada operación con rectángulos o celdas, como la propiedad distributiva.

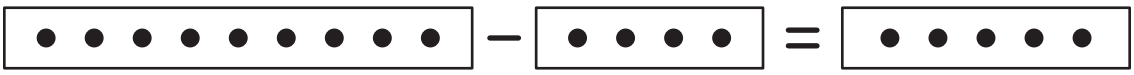


Ley distributiva.

A partir de la definición de adición de dos enteros se puede definir la relación de desigualdad. Las dos proposiciones equivalentes $a < b$ (léase *a* menor que *b*) y $b > a$ (léase *b* mayor que *a*) significan que el rectángulo *b* puede obtenerse a partir del *a* mediante la adición de un tercer rectángulo conveniente *c*, de modo que se tenga $b = a + c$. Si escribimos esto en la forma

$$c = b - a,$$

definimos la operación llamada *sustracción*.



Sustracción.

La adición y la sustracción se llaman *operaciones inversas*, ya que, si la adición del entero *d* al entero *a* es seguida de la sustracción del entero *d* de la suma obtenida, el resultado es el entero inicial *a*:

$$(a + b) - d = a.$$

Debe observarse que el entero $b - a$ ha sido definido únicamente en el caso en que se tenga $b > a$. La interpretación del símbolo $b - a$ como *entero negativo* cuando sea $b < a$ será discutida más adelante. A menudo es conveniente usar una de las notaciones equivalentes, $b \geq a$ (léase *b* mayor o igual que *a*) o $a \geq b$ (léase *a* menor o igual que *b*), para indicar la proposición contraria de la $a > b$; por ejemplo, escribiremos: $2 \geq 2$ y $3 \geq 2$.

Haremos ahora una pequeña ampliación del dominio de los enteros positivos representados por rectángulos con puntos introduciendo el entero cero, que representaremos por un rectángulo vacío. Denotando este con el habitual símbolo 0, se tiene, de acuerdo con nuestra definición de adición y multiplicación:

$$a + 0 = a, \qquad a \cdot 0 = 0$$

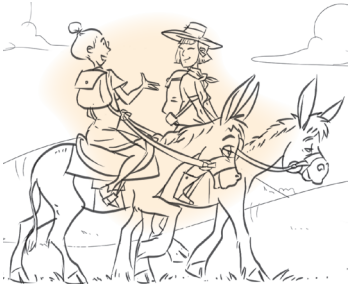
cualquiera que sea el entero a. En efecto, $a + 0$ indica la adición de un rectángulo vacío al rectángulo a, mientras que $a \cdot 0$ indica un rectángulo sin columnas, es decir, vacío. Parece entonces natural extender también la definición de sustracción, poniendo

$$a - a = 0$$

para todo entero a. Se tienen asi las propiedades aritméticas características del cero.

Modelos geométricos análogos a los rectángulos de puntos, tales como los antiguos ábacos, fueron usados frecuentemente hasta fines de la Edad Media; pero quedaron desplazados poco a poco por otros métodos simbólicos más cómodos, basados en el sistema decimal.

2. Representación de los números enteros



Ha de distinguirse netamente entre un número entero y los símbolos 5, o V, usados para representarlo. En el sistema *decimal*, los diez símbolos 0, 1, 2, 3, ..., 9 se utilizan para representar el cero y los nueve primeros enteros positivos. Un entero mayor, por ejemplo, el "trescientos setenta y dos", puede expresarse en la forma

$$300 + 70 + 2 = 3 \cdot 10^2 + 7 \cdot 10 + 2,$$

y se representa en el sistema decimal por el símbolo 372. Es de fundamental importancia observar que aquí la significación de los símbolos 3, 7, 2 es *relativa* y depende de su *posición* en el lugar de las unidades, decenas o centenas. Con esta notación relativa se puede representar cualquier entero utilizando únicamente los símbolos de los diez primeros números en varías combinaciones. La regla general consiste en expresar todo entero en la forma ilustrada por el ejemplo

$$z = a \cdot 10^3 + b \cdot 10^2 + c \cdot 10 + d,$$

donde los números a, b, c, d son enteros de cero a nueve. El entero z se representa entonces en la forma abreviada $abcd$.

Notemos de paso que los coeficientes d, c, b, a son los restos obtenidos mediante divisiones sucesivas de z por 10; así

10|	372	resto
10|	37	2
10|	3	7
	0	3

La expresión particular dada antes para z puede servir únicamente para números menores que 10 000, ya que para enteros mayores serán necesarias más de cuatro cifras. Si z es un entero comprendido entre 10 000 y 100 000, podremos escribirlo en la forma

$$z = a \cdot 10^4 + b \cdot 10^3 + c \cdot 10^2 + d \cdot 10 + e,$$

y representarlo por el símbolo $abcde$. Análogas consideraciones valen para enteros comprendidos entre 100 000 y 1 000 000, etcétera.

Será conveniente disponer de un modo de indicar el resultado con toda generalidad mediante una sola fórmula. Para ello designemos los distintos coeficientes: c, d, e, ... con una sola letra afectada de "subíndices": a_0, a_1, a_2, a_3, … e indiquemos el hecho de que las potencias de 10 pueden ser tan grandes como sea necesario designando la mayor potencia que interviene no con 10^3 o 10^4, como en los ejemplos anteriores, sino con 10^n, donde n ha de interpretarse como un entero arbitrario. Entonces, el método general para representar un entero z en el sistema decimal consistirá en expresar z en la forma

$$z = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_1 \cdot 10 + a_0, \qquad (1)$$

y representarlo por el símbolo

$$a_n a_{n-1} a_{n-2} \ldots a_1 a_0.$$

Como en los casos anteriores, los números a_0, a_1, a_2, … a_n, comprendidos entre 0 y 9, serán precisamente los restos sucesivos de dividir *z* repetidamente por 10.

En el sistema decimal, el número 10 ha sido tomado especialmente para servir de base. A primera vista quizá no resalte el hecho de que la elección del 10 no es esencial, y que cualquier entero mayor que uno habría podido servir para el mismo objeto; por ejemplo, podría usarse un sistema *septimal* (de base 7). En dicho sistema, un entero se expresaría en la forma

$$b_n \cdot 7^n + b_{n-1} \cdot 7^{n-1} + \ldots + b_1 \cdot 7 + b_0, \qquad (2)$$

donde las *b* serían enteros elegidos entre 0, 1, ... y 6, y se representaría por el símbolo

$$b_n b_{n-1} \ldots b_1 b_0.$$

Así, "ciento nueve" se representaría en el sistema septimal por el símbolo 214, que significaría

$$2 \cdot 7^2 + 1 \cdot 7 + 4.$$

Como ejercicio, podemos probar la regla general que permite pasar de la base diez a otra base cualquiera *B*, y que consiste en efectuar divisiones sucesivas del número *z* por *B*; los restos sucesivos serán las cifras del número en el sistema de base *B*; por ejemplo:

7|	109	resto
7|	15	4
7|	2	1
	0	2

109 (en el sistema decimal) = 214 (en el sistema septimal).

Es natural preguntarse: ¿cuál será la base más conveniente? Puede verse que bases muy pequeñas presentan inconvenientes, mientras que una base grande requiere la utilización de muchas cifras distintas y, en particular, una tabla de multiplicación extensa. La elección de doce como base ha sido defendida por muchos; como ventajas señalan que 12 es divisible por 2, 3, 4 y 6, y, como consecuencia, el cálculo que implique divisiones y fracciones se simplificaría frecuentemente. Para escribir un número en base doce (sistema *duodecimal*) se necesitan dos nuevas cifras para el 10 y el 11. Indiquemos el 10 con α y el 11 con β. En el sistema duodecimal, "doce" se escribiría 10; "veintidós" sería 1 α; "veintitrés" sería 1 β, y "ciento treinta y uno" se escribiría α β.

La invención de la notación posicional, atribuida a los sumerios o babilonios y desarrollada por los indios, fue de enorme trascendencia para la civilización. Los sistemas anteriores de numeración estaban basados en un estricto principio aditivo. En el simbolismo romano, por ejemplo, se escribía

$$\text{CXVIII} = 100 + 10 + 5 + 1 + 1 + 1.$$

Los sistemas egipcio, hebraico y griego eran de un tipo parecido al de los romanos. Un inconveniente de la notación aditiva es que cuanto mayor es el número, mayor es también el conjunto de nuevos símbolos necesarios para representarlo. (Claro está que los científicos antiguos no utilizaban las modernas magnitudes astronómicas o atómicas.) Pero el defecto fundamental de los antiguos sistemas, tales como el romano, residía en el hecho de que el cálculo era tan complicado que únicamente los especialistas podían manejar los problemas de cálculo no triviales.

Las cosas pasan de modo distinto con el sistema indio de *valor relativo* hoy en uso. Este sistema fue introducido en Europa durante la Edad Media por comerciantes italianos, quienes lo habían aprendido de los árabes. Tiene la propiedad cómoda de que todos los números, grandes o pequeños, pueden representarse mediante un pequeño conjunto de cifras diferentes (en el sistema decimal, mediante las "cifras árabes" 0, 1, 2, ..., 9). Esto lleva consigo la importante ventaja de la facilidad de los cálculos.

Las reglas de cálculo en los sistemas de notación basados en el valor relativo pueden establecerse en forma de tablas de adición y multiplicación para números de una sola cifra y pueden ser aprendidas de memoria y retenidas para siempre. Existen pocos ejemplos de adelantos científicos que hayan afectado tan profundamente y facilitado tanto la vida diaria como el actual sistema de numeración decimal.

3. Cálculo numérico en sistemas distintos del decimal

El uso del 10 como base de numeración se remonta a los primeros tiempos de la civilización y es debido indudablemente al hecho de que son diez los dedos con los que se acostumbra contar. Sin embargo, las palabras que sirven para designar algunos números en distintos idiomas parecen reminiscencias del uso de otras bases, especialmente 12 y 20. En inglés y en alemán, las palabras para 11 y 12 no están construidas según el principio decimal de combinar 10 con los números de una cifra, como ocurre para los comprendidos entre 13 y 19, sino que son lingüísticamente independientes de la palabra que corresponde a 10. En francés, las palabras *vingt* y *quatre-vingts*, para 20 y 80, sugieren que para algunas cuestiones se haya usado un sistema de base 20.

En danés, la palabra *halvfirsinds-tyve*, para 70, significa a medio camino (a partir de tres veces) de cuatro veces veinte. Los astrónomos de Babilonia utilizaban un sistema que en parte era sexagesimal (base 60); la creencia en este hecho se apoya en la habitual división de la hora y del grado angular en 60 min.

En un sistema distinto del decimal, las reglas de la aritmética son las mismas que en este, sin tablas para la adición y la multiplicación de los números de una cifra. Acostumbrados al sistema decimal y ligados a él por gran número de palabras de nuestro lenguaje, surge al comienzo alguna confusión. Ensayemos un ejemplo de multiplicación en el sistema septimal; antes será conveniente escribir a continuación las tablas de sumar y multiplicar que usaremos en la operación:

+	1	2	3	4	5	6
1	2	3	4	5	6	10
2	3	4	5	6	10	11
3	4	5	6	10	11	12
4	5	6	10	11	12	13
5	6	10	11	12	13	14
6	10	11	12	13	14	15

×	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	11	13	15
3	3	6	12	15	21	24
4	4	11	15	22	26	33
5	5	13	21	26	34	42
6	6	15	24	33	42	51

Sea multiplicar 265 por 24, siendo estos símbolos que representan números en el sistema septimal. (En el sistema decimal sería equivalente a multiplicar 145 por 18.) Las reglas de la multiplicación son las mismas que en el sistema decimal.

$$\begin{array}{r} 265 \\ 24 \\ \hline 1\,456 \\ 563 \\ \hline 10\,416 \end{array}$$

Comenzamos multiplicando 5 por 4, que da 26, como resulta de la tabla de multiplicar. Escribimos 6 en el lugar de las unidades y "llevamos" el 2 para sumarlo a la cifra siguiente. Luego buscamos

$$4 \times 6 = 33 \text{ y } 33 + 2 = 35.$$

Escribimos 5, y procedemos de igual forma hasta que hayamos multiplicado todos los números. Sumando 1 456 + 5 630, se obtiene 6 + 0 = 6 en el lugar de las unidades, 5 + 3 = 11 en el lugar de las septenas. De nuevo escribimos 1 y conservamos 1 para el lugar de los cuarenta y nueve, con lo que tenemos 1 + 6 + 4 = 14. El resultado final es 265 × 24 = 10 416.

Para comprobar este resultado, podemos multiplicar los mismos números en el sistema decimal. El número 10 416 (en el sistema septimal) puede escribirse en el sistema decimal calculando las potencias de 7 hasta la cuarta:

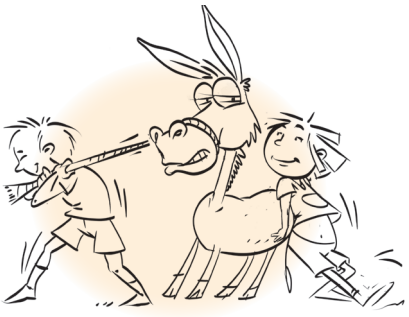
$$7^2 = 49,\ 7^3 = 343,\ 7^4 = 2\,401.$$

De donde

$$10\,416 = 2\,401 + 4 \times 49 + 7 + 6$$

este cálculo está hecho en el sistema decimal. Sumando estos números, resulta que 10 416 en el sistema septimal es igual a 2 610 en el sistema decimal. Luego, multipliquemos 145 por 18 en el sistema decimal; el resultado es 2 610, lo que confirma el cálculo anterior.

Ejercicios de entrenamiento



1. Constrúyanse las tablas de adición y multiplicación en el sistema duodecimal y háganse algunos ejemplos en este sistema.
2. Exprésense 30 y 136 en los sistemas de bases 5, 7, 11 y 12.
3. ¿Qué representan los símbolos 11111 y 21212 en dichos sistemas?
4. Fórmense las tablas de adición y multiplicación en los sistemas de bases 5, 11 y 13.

El sistema de valor relativo de base 2 está caracterizado por ser el de base más pequeña. Las únicas cifras en este sistema *diádico* son 0 y 1; cualquier otro número *z* vendrá representado por una sucesión de estos dos símbolos. Las tablas de adición y multiplicación se reducen a las reglas $1 + 1 = 10$ y $1 \times 1 = 1$.

El inconveniente de este sistema es evidente: hacen falta expresiones muy largas para representar números pequeños. Así, 79, que puede expresarse en la forma $1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1$, se escribe en el sistema diádico 1 001 111.

Como ilustración de la sencillez de la multiplicación en el sistema diádico haremos la multiplicación de 7 por 5, números que se representan, respectivamente, por 111 y 101. Recordando que en este sistema se tiene $1 + 1 = 10$, resulta:

$$\begin{array}{r} 111 \\ 101 \\ \hline 111 \\ 111\ - \\ \hline \end{array}$$

$$100011 = 2^5 + 2 + 1,$$

es decir, 35, como debía ser.

Gottfried Wilhelm Leibniz (1646-1716), una de las mayores inteligencias de su tiempo, fue un apasionado del sistema diádico. Pierre-Simon Laplace escribe al respecto que Leibniz veía en el sistema diádico la imagen de la creación. Consideraba que la unidad representaba a Dios y el cero, la nada; que el ser supremo creaba todos los seres de la nada, del mismo modo que la unidad y el cero expresaban todos los números de su sistema de numeración.

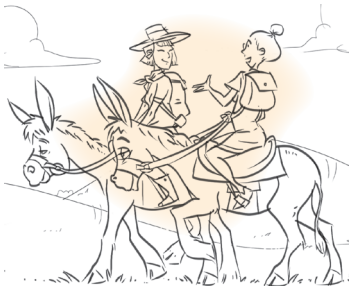
Ejercicio de rutina. Considérese la cuestión de representar los enteros en la base *a*. Para nombrar los enteros en este sistema se necesitan palabras para los números 0, 1, …, $a - 1$ y para las sucesivas potencias de a: a, a^2, a^3, … ¿Cuántas palabras distintas son necesarias para designar todos los números de 0 a 1 000, para $a = 2, 3, 4, 5, \ldots, 15$? ¿En qué base son necesarias menos palabras?

Ejemplos. Si $a = 10$, se necesitan diez palabras para los números de una cifra, además de las palabras para 10, 100 y 1 000, lo que hace 13 en total. Para $a = 20$, se necesitan veinte palabras para los números de una cifra, más las correspondientes a 20 y 400; en total, 22. Si es $a = 100$, se necesitan 101 palabras.

II. Dialogando con los profesores sobre los sistemas numéricos y las transformaciones afines

¿Qué es la matemática y la... imaginación, creatividad y aventuras del pensamiento?

Para Tales... "la cuestión primaria no era qué sabemos, sino cómo lo sabemos". Aristóteles



Los números y las transformaciones afines

CONGRUENCIAS

1. Conceptos generales

Siempre que se presenta la cuestión de la divisibilidad de enteros por un entero fijo d, el concepto y la notación de *congruencia* (debidos a Carl Friedrich Gauss) sirven para aclarar y facilitar el razonamiento. Para introducir este concepto, consideremos los restos que dan los sucesivos enteros al dividirlos por 5. Se tiene:

$0 = 0 \cdot 5 + 0$	$7 = 1 \cdot 5 + 2$	$-1 = -1 \cdot 5 + 4$
$1 = 0 \cdot 5 + 1$	$8 = 1 \cdot 5 + 3$	$-2 = -1 \cdot 5 + 3$
$2 = 0 \cdot 5 + 2$	$9 = 1 \cdot 5 + 4$	$-3 = -1 \cdot 5 + 2$
$3 = 0 \cdot 5 + 3$	$10 = 2 \cdot 5 + 0$	$-4 = -1 \cdot 5 + 1$
$4 = 0 \cdot 5 + 4$	$11 = 2 \cdot 5 + 1$	$-5 = -1 \cdot 5 + 0$
$5 = 1 \cdot 5 + 0$	$12 = 2 \cdot 5 + 2$	$-6 = -2 \cdot 5 + 4$
$6 = 1 \cdot 5 + 1$	etc.	etc.

Observamos que el resto de cualquier entero es uno de los números 0, 1, 2, 3, 4. Diremos que dos enteros a y b son congruentes módulo 5 si ambos dan el mismo resto al ser divididos por 5. Así,

$$2, 7, 12, 17, 22, \ldots, -3, -8, -13, -18, \ldots$$

son todos congruentes módulo 5, puesto que todos dan de resto 2. En general, diremos que dos enteros a y b son *congruentes módulo d*, siendo d un entero dado, si a y b dan el mismo resto al dividirlos por d, lo que equivale a decir que hay un entero n tal que $a - b = na$. Por ejemplo, 27 y 15 son congruentes módulo 4, puesto que

$$27 = 6 \cdot 4 + 3, \qquad 15 = 3 \cdot 4 + 3.$$

El concepto de congruencia es tan útil que resulta conveniente disponer de una notación sencilla para él. Escribiremos:

$$a \equiv b \ (\text{mód } d)$$

para expresar que a y b son congruentes módulo d. En los casos en que no haya duda acerca de cuál sea el módulo, el "mód d" de la fórmula puede ser omitido. [Si a no es congruente con b módulo d, escribiremos $a \not\equiv b$ (mód d).]

Las congruencias aparecen frecuentemente en la vida diaria; por ejemplo, las manecillas de un reloj indican la hora módulo 12, y el cuentakilómetros de un coche da el total de kilómetros recorridos módulo 100 000.

Antes de proceder a una discusión detallada de las congruencias, debemos observar las siguientes proposiciones, que son todas ellas equivalentes:

1) a es congruente con b módulo d.

2) $a = b + nd$ para un cierto entero n.

3) d divide a $a - b$.

La utilidad de la notación de Gauss para las congruencias se basa en el hecho de que la congruencia respecto de un módulo fijo tiene varias de las propiedades formales de la igualdad ordinaria. Las propiedades formales más importantes de la relación $a = b$ son las siguientes:

1) Se tiene siempre $a = a$.

2) De $a = b$ se sigue $b = a$.

3) De $a = b$ y $b = c$ se sigue $a = c$.

Además, de $a = a'$ y $b = b'$ se sigue

4) $a + b = a' + b'$.

5) $a - b = a' - b'$.

6) $a \cdot b = a' \cdot b'$.

Estas propiedades siguen siendo lícitas si se reemplaza la relación $a = b$ por la de congruencia $a \equiv b$ (mód d). Así:

1′) Se tiene siempre $a \equiv a$ (mód d).

2′) De $a \equiv b$ (mód d) se sigue $b \equiv a$ (mód d).

3′) De $a \equiv b$ (mód d) y $b \equiv c$ (mód d) se sigue $a \equiv c$ (mód d).

Dejamos al cuidado del lector el comprobar estos hechos.

Además, de $a \equiv a'$ (mód d) y $b \equiv b'$ (mód d) se sigue

4′) $a + b \equiv a' + b'$ (mód d).

5′) $a - b \equiv a' - b'$ (mód d).

6′) $a \cdot b \equiv a' \cdot b'$ (mód d).

Resulta, en consecuencia, que **varias congruencias respecto del mismo módulo pueden sumarse, restarse y multiplicarse.**

Para probar estas tres proposiciones es suficiente observar que si

$$a = a' + rd, \quad b = b' + sd,$$

se tiene

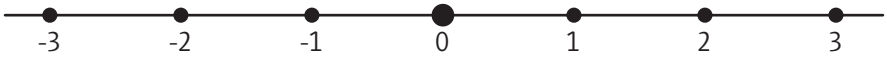
$$a + b = a' + b' + (r + s)d,$$

$$a - b = a' - b' + (r - s)d,$$

$$ab = a'b' + (a's + b'r + rsd)d,$$

de donde resultan las conclusiones deseadas.

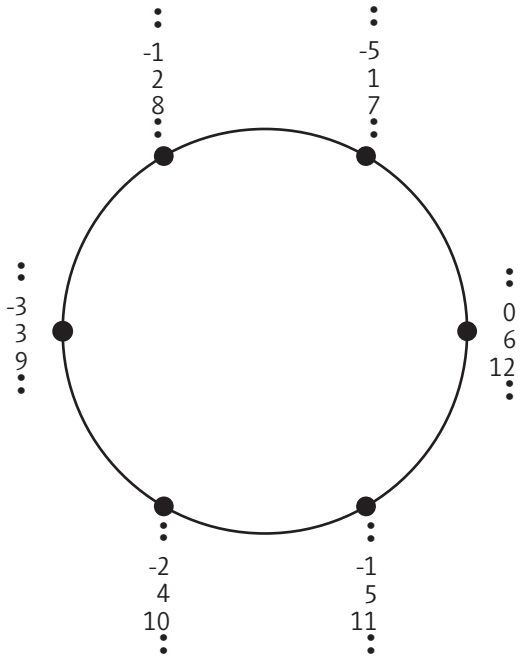
El concepto de congruencia tiene una interpretación geométrica muy intuitiva. De ordinario, cuando se quiere representar los enteros geométricamente, se elige un segmento de longitud unidad y se llevan este y sus múltiplos en los dos sentidos. De este modo se hace corresponder a cada entero un punto sobre la recta, como en la figura siguiente.



Representación geométrica de los números enteros.

Si se trata de los enteros módulo *d*, dos números congruentes se consideran como uno mismo en lo que a la división por *d* se refiere, puesto que los dos dan el mismo resto. Para ver esto geométricamente, utilicemos una circunferencia dividida en *d* partes iguales.

Cualquier entero dividido por *d* da de resto uno de los *d* números 0, 1, …, *d* – 1, que están situados a intervalos iguales sobre la circunferencia. Cualquier entero es congruente módulo *d* con uno de estos *d* números y, por tanto, puede ser representado geométricamente por uno de esos puntos; dos números son congruentes si están representados por el mismo punto.



Representación geométrica de los números enteros respecto del módulo 6.

La figura de arriba está dibujada para el caso *d* = 6. La esfera de un reloj es otro ejemplo tomado de la vida corriente.

Como aplicación de la propiedad multiplicativa 6') de las congruencias, determinaremos los restos de las sucesivas potencias de 10 respecto de un número dado; por ejemplo,

$$10 \equiv -1 \text{ (mód 11)},$$

ya que $10 = -1 + 11$. Por multiplicaciones sucesivas de esta congruencia por sí misma se obtiene

$$10^2 \equiv (-1)(-1) = 1 \text{ (mód 11)}$$
$$10^3 \equiv -1 \text{ (mód 11)}$$
$$10^4 \equiv 1 \text{(mód 11) etc.}$$

Como consecuencia, se puede probar que cualquier entero

$$z = a_0 + a_1 10 + a_2 10^2 + \ldots + a_n 10^n$$

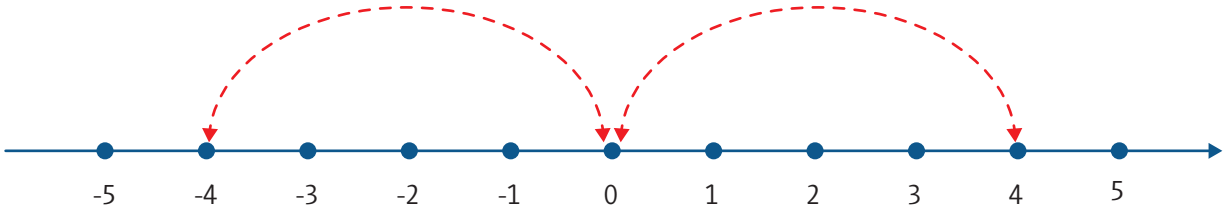
expresado en el sistema decimal da al dividirlo por 11 el mismo resto que la suma de sus cifras, tomadas alternativamente con los signos más y menos,

$$t = a_0 - a_1 + a_2 - a_3 + \ldots$$

En efecto, se puede escribir

$$z - t = a_1 \cdot 11 + a_2(10^2 - 1) + a_3(10^3 + 1) + a_4(10^4 - 1) + \ldots$$

Y como todos los números 11, $10^2 - 1$, $10^3 + 1$, … son congruentes con 0 módulo 11, también lo será $z - t$; por consiguiente, z da el mismo resto que t al dividirlo por 11. Resulta en particular que un número es divisible por 11 (es decir, da de resto 0) cuando, y únicamente entonces, la suma alternada de sus cifras es divisible por 11. Por ejemplo, puesto que $3 - 1 + 6 - 2 + 8 - 1 + 9 = 22$, el número $z = 3\,162\,819$ es divisible por 11.



Representación geométrica de los numeros enteros respecto del módulo 4.

Encontrar una regla de divisibilidad por 3 o por 9 es más sencillo aún, puesto que $10 \equiv 1$ (mód 3 o 9) y, por consiguiente, $10^n \equiv 1$ (mód 3 o 9) para todo n. Resulta así que para que un número z sea divisible por 3 o por 9 es necesario y suficiente que la suma de sus cifras

$$s = a_0 + a_1 + a_2 + \ldots + a_n$$

sea también divisible por 3 o por 9, respectivamente.

Para las congruencias módulo 7 se tiene

$$10 \equiv 3, \quad 10^2 \equiv 2, \quad 10^3 \equiv -1, \quad 10^4 \equiv -3, \quad 10^5 \equiv -2, \quad 10^6 \equiv 1.$$

Los restos sucesivos se repiten, de donde resulta que para que z sea divisible por 7 es necesario y suficiente que la expresión

$$r = a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + \ldots$$

sea divisible por 7.

Ejercicio para pensar. Hállese una regla análoga para la divisibilidad por 13.

Sumando o multiplicando congruencias respecto de un módulo fijo, por ejemplo, $d = 5$, podemos evitar los números muy grandes al reemplazar cualquier número a por el del conjunto 0, 1, 2, 3, 4 congruente con él. Así, para calcular sumas y productos módulo 5 necesitamos únicamente las siguientes tablas de adición y multiplicación:

$a + b \equiv$

+	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

$a \times b \equiv$

×	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

De la segunda de esas tablas resulta que un producto $a\,b$ es congruente con 0 (mód 5) únicamente si a o b son $\equiv 0$ (mód 5).

Esto sugiere la ley general

7) $a\,b \equiv 0$ (mód d) únicamente si $a \equiv 0$ o $b \equiv 0$ (mód d),

la cual resultaría como una extensión de la ley ordinaria para enteros que dice que se tiene $ab = 0$ únicamente si es $a = 0$ o $b = 0$. Ahora bien: **la ley 7) es válida solamente cuando el módulo d es un número primo**. En efecto, la congruencia

$$a\,b \equiv 0 \text{ (mód } d)$$

significa que d divide a ab, y hemos visto antes que un número primo divide a un producto ab únicamente si divide a a o a b; esto es, únicamente si

$$a \equiv 0 \text{ (mód } d) \quad \text{o} \quad b \equiv 0 \text{ (mód } d).$$

Si d no es primo, esta regla no vale en general, puesto que si es $d = r \times s$, siendo r y s menores que d, se tiene

$$r \not\equiv 0 \text{ (mód } d), \quad s \not\equiv 0 \text{ (mód } d),$$

y, en cambio, es

$$rs = d \equiv 0 \text{ (mód } d).$$

Por ejemplo, $2 \not\equiv 0$ (mód 6) y $3 \not\equiv 0$ (mód 6); sin embargo, $2 \times 3 = 6 \equiv 0$ (mód 6).

Ejercicio. Pruébese que la siguiente regla de simplificación es válida para congruencias respecto de un módulo primo:

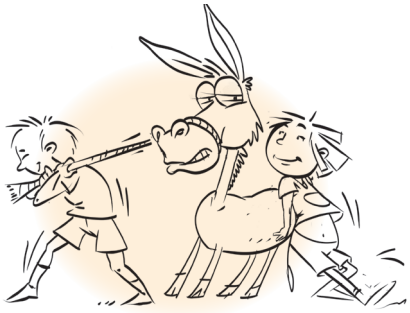
Si es $ab \equiv ac$ y $a \not\equiv 0$, se tiene $b \equiv c$.

Ejercicios de entrenamiento

1. ¿Con qué número entre 0 y 6 incluidos es congruente módulo 7 el producto $11 \cdot 18 \cdot 2\,322 \cdot 13 \cdot 19$?

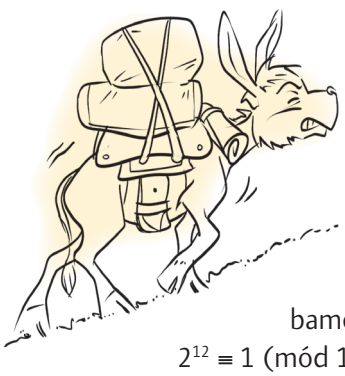
2. ¿Con qué número comprendido entre 0 y 12 incluidos es congruente módulo 13 el producto $3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 113$?

3. ¿Con qué número entre 0 y 4 incluidos es congruente módulo 5 la suma $1 + 2 + 21 + \ldots + 211$?



Dialogando con los profesores...

2. Pequeño teorema de Fermat



En el siglo XVII, Pierre de Fermat, el fundador de la moderna teoría de números, descubrió un teorema muy importante: si p es un número primo que no divide al entero a, se tiene:

$$a^{p-1} \equiv 1 \text{ (mód } p\text{)},$$

lo que significa que la potencia $(p-1)$-ésima de a da resto 1 al dividirla por p. Su interés principal está en su aplicación al problema de la primalidad y a la criptografía.

Algunos de nuestros cálculos anteriores confirman este teorema; por ejemplo, encontrábamos que $10^6 \equiv 1$ (mód 7), $10^2 \equiv 1$ (mód 3), y $10^{10} \equiv 1$ (mód 11). Del mismo modo se vería que es $2^{12} \equiv 1$ (mód 13) y $5^{10} \equiv 1$ (mód 11). Para comprobar las últimas congruencias no es necesario calcular efectivamente las potencias indicadas, ya que pueden utilizarse ventajosamente las propiedades multiplicativas de aquellas:

$2^4 = 16 \equiv 3$	(mód 13)
$2^8 = 9 \equiv -4$	(mód 13)
$2^{12} = -4 \times 3 = -12 \equiv 1$	(mód 13)

$5^2 \equiv 3$	(mód 11)
$5^4 \equiv 9 \equiv -2$	(mód 11)
$5^8 \equiv 4$	(mód 11)
$5^{10} \equiv 3 \cdot 4 \equiv 12 \equiv 1$	(mód 11)

Para demostrar el teorema de Fermat, consideremos los múltiplos de a:

$$m_1 = a,\ m_2 = 2a,\ m_3 = 3a,\ \ldots,\ m_{p-1} = (p-1)a.$$

Ningún par de estos enteros puede estar formado por números congruentes módulo p; de lo contrario, p sería un factor de $m_r - m_s = (r-s)a$ para algún par r, s, siendo $1 \le s < r \le (p-1)$. Pero la regla 7) indica que esto no puede ocurrir; puesto que $r - s$ es menor que p, p no puede ser factor de $(r-s)$, y habíamos supuesto que p no dividía a a.

Asimismo, ninguno de aquellos múltiplos puede ser congruente con 0. Por consiguiente, los números m_1, m_2, m_3, …, m_{p-1} deben ser congruentes con los números 1, 2, 3, …, $p-1$ tomados en orden conveniente. Resulta, como consecuencia,

$$m_1 m_2 \ldots m_{p-1} = 1 \cdot 2 \cdot 3 \ldots (p-1)a^{p-1} \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \text{ (mód } p\text{)},$$

o, si escribimos por brevedad K en vez de $1 \cdot 2 \cdot 3 \ldots (p-1)$,

$$K(a^{p-1} - 1) \equiv 0 \text{ (mód } p\text{)}.$$

Pero K no es divisible por p, ya que no lo es ninguno de sus factores; por tanto, en virtud de la regla 7), $(a^{p-1} - 1)$ debe ser divisible por p; es decir,

$$a^{p-1} - 1 \equiv 0 \text{ (mód } p\text{)},$$

que es el teorema de Fermat.

Para comprobar el teorema una vez más, tomemos $p = 23$ y $a = 5$. Se tiene, entonces, (mód 23) $5^2 \equiv 2$, $5^4 \equiv 4$, $5^8 \equiv 16 \equiv -7$, $5^{16} \equiv 49 \equiv 3$, $5^{20} = 12$, $5^{22} \equiv 24 \equiv 1$. Con $a = 4$, en vez de 5, se obtendría, también (mód 23), $4^2 \equiv -7$, $4^3 \equiv -28 \equiv -5$, $4^4 \equiv 20 \equiv 3$, $4^8 \equiv 9$, $4^{11} \equiv -45 \equiv 1$, $4^{22} \equiv 1$.

En el ejemplo anterior con $a = 4$, $p = 23$ y en otros, se observa que no solamente la potencia $(p-1)$-ésima de a, sino también otras potencias menores pueden ser congruentes con 1. Pero ocurre siempre que la menor de dichas potencias, en este caso 11, es un divisor de $p - 1$. (Véase el Ejercicio 3 siguiente.)

Ejercicios de entrenamiento

1. Compruébese mediante cálculos análogos a los anteriores que $2^8 \equiv 1$ (mód 17); $3^8 \equiv -1$ (mód 17); $3^{14} \equiv -1$ (mód 29); $2^{14} \equiv -1$ (mód 29); $4^{14} \equiv 1$ (mód 29); $5^{14} \equiv 1$ (mód 29).

2. Compruébese el teorema de Fermat para $p = 5, 7, 11, 17, 23$ con diferentes valores de a.

3. Demuéstrese el teorema general siguiente: El menor entero positivo e para el que se tenga $a^e \equiv 1 \pmod{p}$, siendo p primo, debe ser un divisor de $p - 1$.

[**Indicación:** Dividiendo $p - 1$ por e, se obtendría $p - 1 = ke + r$, siendo $0 \leq r < e$; utilícese el hecho de que $a^{p-1} \equiv a^e \equiv 1 \pmod{p}$.

3. Restos cuadráticos o ley de reciprocidad cuadrática

Por los ejemplos considerados en relación con el teorema de Fermat, se ha visto que no solamente es siempre $a^{p-1} \equiv 1 \pmod{p}$, sino que (si p es un número primo distinto de 2 y, por consiguiente, impar y de la forma $p = 2p' + 1$) para algunos valores de a, $a^{p'} = a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Este hecho sugiere otras varias cuestiones interesantes. Podemos escribir el teorema en la siguiente forma:

$$a^{p-1} - 1 = a^{2p'} - 1 = (a^{p'} - 1)(a^{p'} + 1) \equiv 0 \pmod{p}.$$

Puesto que un producto es divisible por p cuando uno al menos de los factores lo es, resulta inmediatamente que, o bien $a^{p'} - 1$ o $a^{p'} + 1$ debe ser divisible por p, de modo que para cualquier primo $p > 2$ y cualquier número a no divisible por p, se tiene

$$a^{\frac{p-1}{2}} \equiv 1 \text{ o } a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Desde el comienzo de la moderna teoría de números los matemáticos se han interesado por el problema de determinar qué números a pertenecen a la primera clase y cuáles a la segunda. Supongamos que a es congruente módulo p con el cuadrado de otro entero x : $a \equiv x^2 \pmod{p}$.

Entonces, se tendrá: $a^{\frac{p-1}{2}} \equiv x^{p-1}$ y, de acuerdo con el teorema de Fermat, congruente con 1 módulo p. Un número a, no múltiplo de p, que sea congruente módulo p con el cuadrado de otro entero se llama *resto cuadrático* de p, mientras que un número b, no múltiplo de p, que no sea congruente con ningún cuadrado, se llama *no-resto cuadrático* de p.

Acabamos de ver que todo resto cuadrático a de p satisface la congruencia $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Sin grandes dificultades, se puede probar que para cualquier no-resto b se tiene la congruencia $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Por otra parte, vamos a demostrar que entre los números 1, 2, 3, ..., $p - 1$ hay precisamente $(p - 1)/2$ restos cuadráticos y $(p - 1)/2$ no-restos.

Aun siendo posible obtener muchos datos empíricos por cálculo directo, al comienzo no fue fácil descubrir leyes generales que rigieran la distribución de los restos y no-restos cuadráticos. La primera propiedad importante de los restos fue observada por Adrien-Marie Legendre (1752-1833) y designada más tarde por Gauss con el nombre de *ley de reciprocidad cuadrática*. Esta ley se refiere al comportamiento de dos números primos distintos p y q, y dice que q es un resto cuadrático de p cuando, y solo entonces, p es resto cuadrático de q, si el producto $[(p - 1)/2][(q - 1)/2]$ es par. En el caso en que dicho producto sea impar, la situación es la inversa, de modo que p es resto de q si q es no-resto de p. Uno de los descubrimientos juveniles de Gauss fue la primera demostración rigurosa de este teorema, que durante mucho tiempo había desafiado al mundo matemático.

Carl Friedrich Gauss

Adrien-Marie Legendre

La primera demostración de Gauss no era sencilla y aún hoy la ley de reciprocidad no es fácil de establecer, a pesar de que se han dado de ella numerosas demostraciones. Su verdadera significación aparece claramente

cuando se establece su conexión con los descubrimientos modernos en la teoría de los números algebraicos. Como ejemplo para ilustrar la distribución de los restos cuadráticos, tomemos $p = 7$. Entonces, puesto que se tiene

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 2,\ 4^2 \equiv 2,\ 5^2 \equiv 4,\ 6^2 \equiv 1,$$

todas módulo 7, y ya que los cuadrados restantes repiten esta sucesión, los restos cuadráticos de 7 son los números congruentes con 1, 2 o 4, mientras que los no-restos son congruentes con 3, 5 o 6. En el caso general, los restos cuadráticos de p son los números congruentes con $1^2, 2^2, \ldots, (p-1)^2$. Pero estos son congruentes a pares, pues se tiene

$$x^2 \equiv (p-r)^2 \pmod{p} \quad [\text{por ejemplo, } 2^2 \equiv 5^2 \pmod 7].$$

por ser $(p-x)^2 = p^2 - 2px + x^2 \equiv x^2 \pmod p$. Resulta así que la mitad de los números $1, 2, \ldots, p-1$ son restos cuadráticos de p y la otra mitad son no-restos cuadráticos.

Como ejemplo de la ley de reciprocidad, tomemos $p = 5$, $q = 11$. Por ser $11 \equiv 1^2 \pmod 5$, 11 es resto cuadrático (mód 5); y como el producto $\left[\frac{5-1}{2}\right]\cdot\left[\frac{11-1}{2}\right]$ es par, la ley de reciprocidad dice que 5 es resto cuadrático (mód 11). En confirmación de esto, observemos que se tiene $5 \equiv 4^2 \pmod{11}$.

Por otra parte, si $p = 7$, $q = 11$, el producto $\left[\frac{7-1}{2}\right]\cdot\left[\frac{11-1}{2}\right]$ es impar, y en efecto 11 es un resto cuadrático (mód 7) [ya que $11 \equiv 2^2 \pmod 7$], mientras que 7 es no-resto cuadrático (mód 11).

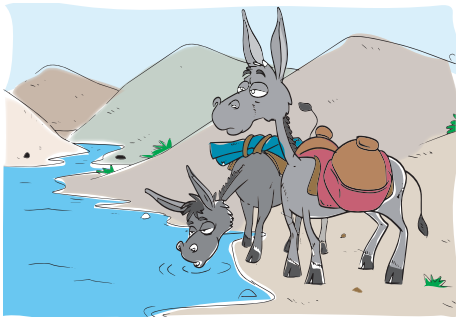
Ejercicios de entrenamiento

1. $6^2 = 36 \equiv 13 \pmod{23}$. ¿Es 23 resto cuadrático (mód 13)?

2. Hemos visto que $x^2 \equiv (p-x)^2 \pmod p$. Demuéstrese que esas son las únicas congruencias módulo p entre los números $1^2, 2^2, 3^2, \ldots, (p-1)^2$.

Tiempo de imaginación, creatividad y aventuras del pensamiento

El sistema ático de numeración



El cuadro de la matemática pitagórica está basado en su mayor parte en informaciones de comentaristas que vivieron muchos siglos más tarde y que estaban, casi sin excepción, interesados principalmente en los aspectos filosóficos del pensamiento. Aunque parece perfectamente verosímil suponer, de acuerdo con los comentaristas, que fueron los pitagóricos los principales responsables de la concepción abstracta e intelectual que transformó la matemática en una disciplina liberal, el nivel de sofisticación durante los siglos VI y V a. C. pudo no haber sido tan alto como el que le atribuye la tradición. Tiene que haber resultado demasiado tentador para los seguidores tardíos de una escuela filosófica tal como la pitagórica el hecho de exagerar los logros del fundador y de los primeros miembros de la secta.

Es muy probable que durante las primeras etapas del pitagorismo estuvieran presentes ciertos elementos primitivos que no pasaron a la historia, aunque es obvio también que la actitud hacia la matemática que representaban los pitagóricos fue, casi con toda certeza, atípica dentro del pensamiento griego considerado globalmente.

Los helenos se hicieron famosos como hábiles mercaderes y negociantes. Por lo tanto, tuvo que haber un nivel inferior de la aritmética o del cálculo numérico que pudiera satisfacer las necesidades de la gran mayoría de los ciudadanos griegos. Este tipo de actividad numérica quedaría en todo caso muy por debajo del campo de atención de los filósofos y no es lógico esperar que en sus bibliotecas se encontraran exposiciones de aritmética práctica. Así, pues, si no han llegado hasta nosotros ni siquiera fragmentos de las posibles obras pitagóricas más sofisticadas, está claro que no sería razonable contar con que los manuales de matemática comercial hubieran resistido los estragos del paso del tiempo.

Como consecuencia, no podemos decir en esta instancia cómo se efectuaban los procesos ordinarios de la aritmética en Grecia hace 2.500 años; lo mejor y casi lo único que podemos hacer es describir los sistemas de numeración que parecen haber sido utilizados.

En términos generales, parecen haber existido dos sistemas de numeración principales en Grecia: uno de ellos, probablemente el más antiguo, recibe el nombre de sistema de notación *ático* o *herodiánico*, mientras que al otro se le conocía como sistema *jónico* o *alfabético*. Para representar los números naturales, ambos sistemas se basan en una escala de base diez, pero el primero es el más primitivo, ya que consiste en un simple esquema iterativo que se encuentra ya en la numeración jeroglífica egipcia anterior a esta y también en los numerales romanos posteriores.

Sistema ático de numeración.

En el sistema ático (representación de arriba), los números de uno a cuatro se representaban por medio de palotes verticales repetidos; para el cinco se adoptó un símbolo nuevo que era la primera letra Π (o Γ) de la palabra usada para el cinco, penta. (Hay que advertir que en aquella época se utilizaban únicamente las letras mayúsculas, tanto en las obras literarias como en la matemática, mientras que las letras minúsculas fueron inventadas a finales de la edad antigua o comienzos del período medieval.)

Para los números del seis al nueve, el sistema ático combinaba el símbolo Γ con palotes unitarios, de manera que ocho, por ejemplo, se escribía como ΓIII. Para las potencias enteras positivas de la base diez se utilizaban las letras iniciales de las palabras correspondientes: Δ para *deka* (diez), H para *hekaton* (cien), X para *khilio* (mil) y M para *myrioi* (diez mil).

Excepto en la forma de los símbolos, el sistema ático se parece mucho al romano, pero tenía una ventaja: mientras que en el mundo latino se adoptaron símbolos especiales para 50 y para 500, los griegos escribían estos números combinando las letras para 5, 10 y 100, de manera que 50 venía representado como se indica en la tabla de arriba o por combinación: ΓΔ 5 por 10, y 500, por ΓH 5 por 100. Análogamente, escribían como indica la tabla o con ΓX para 5 000 y ΓM para 50 000; así pues, el número 45 678, por ejemplo, se escribiría en notación ática de la forma MMMM[ΓXΓHHΓΔΔΓIII].

El sistema de numeración jónico

El sistema de notación ático (conocido también como herodiánico debido a que aparece descrito en un trozo atribuido a Herodiano, un gramático del siglo II) aparece con inscripciones de diversas fechas que van del 454 al 95 a. C., pero a comienzos de la época alejandrina, aproximadamente durante el reinado de Ptolomeo Filadelfo, se vio desplazado por el sistema jónico o alfabético para los numerales.

Sistemas alfabéticos análogos fueron utilizados en una u otra época por varios pueblos semíticos, incluidos los hebreos, sirios, arameos y árabes, así como por otros no semíticos tales como los godos, pero estos sistemas parecen haber sido adoptados por influencia de la notación griega. El sistema jónico probablemente se utilizaba ya durante el siglo V a. C., e incluso quizá tan temprano como en el siglo VIII a. C.; una de las razones para situar los orígenes de este sistema de notación relativamente pronto es la de que este esquema requiere 27 letras del alfabeto: nueve para los enteros menores que 10, nueve para los múltiplos de 10 menores que 100 y nueve para los múltiplos de 100 menores que 1 000.

Ahora bien, el alfabeto griego clásico contiene solo 24 letras. Por lo tanto, se hizo uso de un alfabeto más antiguo que incluía tres letras arcaicas adicionales, la Ϝ (vau, digamma o stigma), la ϙ (koppa) y la Ϡ (sampi), para establecer la siguiente asociación entre letras y números:

Sistema jónico de notación.

Y como las tres letras arcaicas ocuparon en este esquema para los numerales las mismas posiciones que tenían en el alfabeto más antiguo, se ha sugerido que quizá se introdujo el sistema jónico antes de que fueran abandonadas estas tres letras, es decir, hacia el siglo VIII a. C. Sin embargo, este punto de vista resulta menos convincente si nos paramos a considerar el largo intervalo de tiempo transcurrido entre esta hipotética introducción y el triunfo final del sistema en el siglo III a. C.

La ventaja obvia de concisión que tiene el sistema alfabético debería haber conducido a una adopción más rápida de este sistema que no con el retraso mencionado de medio milenio. El cifrado del sistema de notación jónico guarda esencialmente la misma relación con la numeración ática que la hierática egipcia con la jeroglífica más complicada, donde la superioridad de la escritura cursiva estuvo muy clara para los escribas desde antiguo.

Después de la introducción de las letras minúsculas en Grecia, la asociación entre letras y números quedó de la forma siguiente:

α	apha	1
β	beta	2
γ	gamma	3
δ	delta	4
ε	epsilon	5
ϛ	stigma	6
ζ	zeta	7
η	eta	8
ϑ	theta	9

ι	iota	10
κ	kappa	20
λ	lambda	30
μ	mu	40
ν	nu	50
ξ	xi	60
ο	omicron	70
π	pi	80
ϙ	koppa	90

ρ	rho	100
σ	sigma	200
τ	tau	300
υ	upsilon	400
ϕ	phi	500
χ	chi	600
ψ	psi	700
ω	omega	800
ϡ	sampi	900

Como estas formas son las más familiares hoy, las usaremos en lo que sigue. Para los nueve primeros múltiplos de 1 000 se adoptaron en el sistema jónico las nueve primeras letras del alfabeto, de nuevo, en un uso al menos parcial del principio posicional, pero para mayor claridad y evitar las ambigüedades, estas letras son precedidas por un acento:

,α	,β	,γ	,δ	,ε	,ϑ	,ζ	,η	,θ
1 000	2 000	3 000	4 000	5 000	6 000	7 000	8 000	9 000

Dentro de este sistema puede escribirse fácilmente cualquier número menor que 10 000 con solo cuatro símbolos; por ejemplo, el número 8 888 vendría escrito como , η ω π η, o bien simplemente como η ω π η, ya que el acento a veces se omitía cuando el contexto no admitía duda. El uso de las mismas letras para los miles que para las unidades debería haber sugerido a los griegos el principio posicional completamente desarrollado para la aritmética decimal, pero el hecho es que parecieron apreciar las ventajas de este paso.

Que tenían este principio más o menos en la cabeza es evidente no solo por el uso repetido de las letras α a θ para las unidades y los millares, sino también por el hecho de que los símbolos se acomodan por orden de magnitud, desde el menor a la derecha al mayor a la izquierda. Al llegar al número 10 000, que para los griegos señalaba el comienzo de una nueva manera de contar o categoría numérica, en un sentido parecido a como hacemos nosotros al separar los miles de las potencias menores por un punto o un espacio, el sistema de notación jónico griego adoptaba un principio multiplicativo.

Una expresión que representa a un número de 1 a 9 999, si aparece escrita encima o a continuación de ella la letra M, separada del resto del número por un punto, expresa el producto de dicho número por 10 000, la miríada griega. Así, el número $88_1888.888$ vendría escrito como $\mathrm{M}, \eta\omega\pi\eta \cdot \eta\omega\pi\eta$. Si se necesitan números aún más grandes podía aplicarse el mismo método a la doble miríada, $100_1000.000$ o 10^8.

El sistema de notación griego antiguo para los enteros no era excesivamente incómodo y servía eficazmente para los fines a que estaba destinado, pero donde el sistema mostraba sus puntos débiles era en el tratamiento de las fracciones. Los griegos se vieron tentados a usar principalmente las fracciones unitarias, como los egipcios, y tenían un sistema sencillo para representarlas; escribían meramente el denominador y le colocaban a su derecha un acento o señal diacrítica para distinguirlo del entero correspondiente.

Así, por ejemplo, $\frac{1}{34}$ aparecería λδ', expresión que podría confundirse, desde luego, con la representación del número $30\frac{1}{4}$, pero el contexto o el uso de palabras adicionales podía ayudar a clarificar la situación sin ambigüedades.

En los siglos posteriores se generalizó el uso de las fracciones ordinarias y de las sexagesimales, pero esto lo estudiaremos más adelante en conexión con la obra de Arquímedes, de Ptolomeo y de Diofanto, pues ahí nos encontraremos ya con documentos que, aunque en realidad no provengan directamente de la época de estos hombres, son copias de obras escritas por ellos, situación completamente diferente de la que se refiere a los matemáticos del período helénico.

Aritmética y logística

Según el *Diccionario de la lengua española* de la Real Academia, la palabra "logística" viene

"Del lat. mediev. *logisticus*, y este del gr. λογιστικός *logistikós*.

1. adj. Perteneciente o relativo a la logística.
2. Lógica que emplea el método y el simbolismo de las matemáticas.
3. Parte de la organización militar que atiende al movimiento y mantenimiento de las tropas en campaña.
4. Conjunto de medios y métodos necesarios para llevar a cabo la organización de una empresa o de un servicio, especialmente de distribución.

Sinónimos o afines de 'logístico, logística': organización, estrategia.".

La logística, en nuestra vida cotidiana, es la actividad que planifica, gestiona, controla el almacenamiento y envío de bienes en una cadena de suministro. Su objetivo principal es gestionar todas las operaciones relacionadas con el movimiento de materias primas o productos de la forma más eficiente posible.

Ahora usaremos este término en su segunda acepción del diccionario y ligado a la aritmética y sus métodos.

La historia de la matemática durante la época de Tales y de los pitagóricos depende necesariamente en alto grado de conjeturas e inferencias, puesto que los documentos originales se han perdido todos. A este respecto, nuestros conocimientos de la matemática griega del 600 al 450 a. C. son muchos e inseguros, y de los que tenemos sobre el álgebra babilónica o la geometría egipcia hacia el 1700 a. C. no han sobrevivido ni siquiera aparatos o tablas de operaciones matemáticas de la Grecia arcaica. Es evidente que debió utilizarse algún tipo de mesa

para cálculos con ábaco para efectuar las operaciones aritméticas, pero la forma del aparato y su funcionamiento tenemos que inferirlos del ábaco romano y de algunas referencias dispersas por los autores griegos.

Heródoto (Heródoto de Halicarnaso fue un historiador y geógrafo griego, tradicionalmente considerado como el padre de la historia en el mundo occidental y el primero en componer un relato razonado y estructurado de las acciones), que escribía en la primera mitad del siglo v a. C., nos dice que al calcular con piedrecillas, lo mismo que al escribir, los griegos movían la mano de izquierda a derecha, mientras que los egipcios lo hacían de derecha a izquierda.

Un vaso cerámico un poco posterior nos muestra a un cobrador de tributos con un tablero para cuentas que se utilizaba no solo para los múltiplos decimales enteros de un dracma, sino también para subdivisiones fraccionarias no decimales. Comenzando por la izquierda, las sucesivas columnas representan las miríadas, los miles, cientos y decenas de dracmas, respectivamente, con los símbolos utilizados en notación herodiánica; a continuación, siguiendo a la columna de las unidades para dracmas, aparecen las columnas para los óbolos (seis óbolos son iguales a un dracma), para medios óbolos y para los cuartos de óbolo.

Aquí podemos ver la hábil manera en cómo evitaban las civilizaciones antiguas el uso excesivo de fracciones: simplemente subdividían las unidades de longitud, peso y moneda de un modo tan eficaz que podían calcular en términos de múltiplos enteros de las subdivisiones. Esta es sin duda la explicación de la gran popularidad de que gozaron en la Antigüedad las subdivisiones duodecimales y sexagesimales, puesto que en este campo el sistema decimal presenta notables desventajas; las fracciones decimales se usaron raramente, ya fuera por los griegos o por otros pueblos occidentales, hasta el período del Renacimiento.

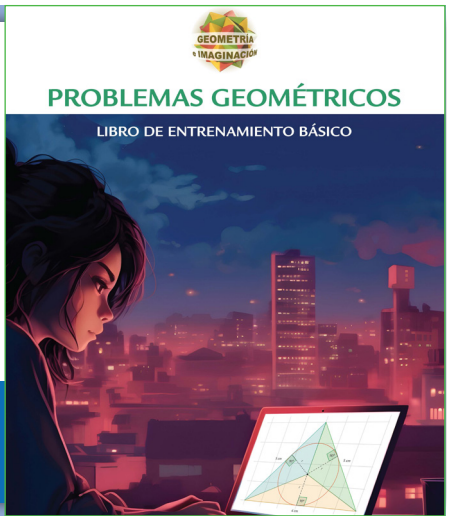
El ábaco se puede adaptar con facilidad a cualquier sistema de numeración o a cualquier combinación de sistemas; es probable que su uso extendido se deba, al menos en parte, al desarrollo sorprendentemente tardío de un sistema de notación posicional coherente para los enteros y las fracciones.

Al respecto, la época pitagórica contribuyó poco o nada al progreso: el punto de vista de los pitagóricos parece haber sido tan decididamente filosófico y abstracto que los detalles técnicos del cálculo apenas les interesaron. Estas técnicas fueron relegadas a una disciplina independiente llamada "logística", que trataba de la numeración y el cálculo aplicados a las cosas y no de la esencia y las propiedades de los números en sí, que eran las cuestiones de las que se ocupaba la aritmética.

Es decir que los antiguos griegos hicieron una distinción clara entre el mero cálculo, por un lado, y lo que se conoce hoy en América como teoría de números (y en Inglaterra como aritmética superior), por el otro. La cuestión de si una separación tan marcada fue una desventaja o no para el desarrollo histórico de la matemática puede ser discutible, pero lo que no es fácil negarles a los matemáticos jónicos y pitagóricos primitivos es el papel principal en la construcción de la matemática como disciplina racional y liberal. Por esta razón a Tales se le llama a veces el primer matemático y a Pitágoras se le suele conocer como el padre de la matemática.

Hasta qué punto podemos aceptar tales estimaciones de una manera literal, en vista de la ausencia de evidencia documental que las apoye, dependerá de nuestro grado de confianza en la tradición. Es evidente que la tradición puede ser bastante engañosa, pero es raro que esté completamente equivocada.

Un libro para imaginar, jugar y construir figuras; para comprender el pensamiento y el para qué de la geometría moderna.



red olímpica

fenchu@oma.org.ar

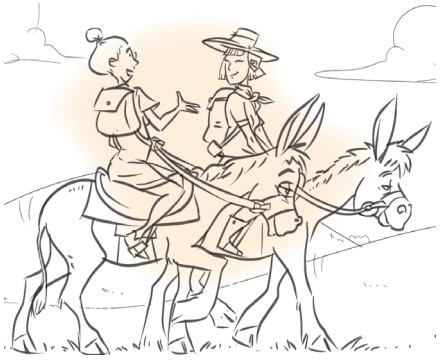
11 4826 8976 **+54 9 11 5035 7537**

¡Hacé tu pedido!

En la Red Olímpica realizamos envíos de todos nuestros títulos a todo el país bajo el sistema contra reembolso o delivery.

III. Dialogando con los estudiantes sobre la probabilidad y la programación lineal

¿Qué es la realidad?



Empecemos por la teoría de números

INTRODUCCIÓN

Los enteros fueron poco a poco perdiendo su relación con supersticiones y misticismos, pero su interés, para los matemáticos, no disminuyó nunca. Euclides (hacia el año 300 a. C.), cuya fama está ligada a la parte de sus *Elementos* que forma la base de la geometría elemental, parece haber obtenido resultados originales en la teoría de números, mientras que su geometría es, en su mayor medida, una compilación de resultados anteriores. Diofanto de Alejandría (hacia el año 275), uno de los primeros algebristas, dejó una huella importante en la teoría de números. Pierre de Fermat (1601-1665), jurista en Toulouse (Francia) y uno de los más grandes matemáticos de su tiempo, inició las investigaciones modernas en este campo.

Leonhard Euler (1707-1783), el más prolífico de los matemáticos, obtuvo una gran cantidad de resultados en la teoría de números entre sus investigaciones matemáticas. Otros nombres preeminentes en los anales de la matemática –Adrien-Marie Legendre, Peter Gustav Lejeune Dirichlet, Bernhard Riemann– deben añadirse a la lista anterior a Gauss (1777-1855), el más célebre matemático de los tiempos modernos, dedicado asimismo a distintas ramas de la matemática, quien resumió su opinión sobre la teoría de números en la frase: "La matemática es la reina de las ciencias y la teoría de números es la reina de la matemática".

LOS NÚMEROS PRIMOS

1. Hechos fundamentales

La mayor parte de las proposiciones de la teoría de números, como en general de la matemática, no se refieren a un objeto particular, el número 5 o el número 32, sino a una clase completa de objetos que tienen alguna propiedad común; por ejemplo, la clase de todos los números pares:

$$2, 4, 6, 8, \ldots,$$

o la clase de los enteros divisibles por 3:

$$3, 6, 9, 12, \ldots,$$

o bien la clase de los cuadrados de los números enteros:

$$1, 4, 9, 16, \ldots,$$

y así sucesivamente.

De fundamental importancia en la teoría de números es la clase de los números *primos*. Casi todos los enteros se pueden descomponer en producto de factores más pequeños:

$$10 = 2 \times 5,\ 111 = 3 \times 37,\ 144 = 3 \times 3 \times 2 \times 2 \times 2 \times 2, \text{ etcétera.}$$

Los números que no pueden descomponerse de este modo se llaman *números primos* o simplemente *primos*.

Con más precisión, **un número primo es un entero *p*, mayor que uno, que no admite más factores que él mismo y la unidad. (Se dice que un entero *a* es factor o divisor de otro entero *b* si existe otro entero *c* tal que *b* = *ac*.)** Los números 2, 3, 5, 7, 11, 13, 17, … son primos, mientras que 12, por ejemplo, no lo es, ya que se tiene 12 = 3 × 4. La importancia de la clase de los números primos se debe al hecho de que cualquier

entero puede expresarse como producto de números primos: si un número no es primo, se puede descomponer sucesivamente hasta que todos sus factores sean primos; por ejemplo:

$$360 = 3 \times 120 = 3 \times 30 \times 4 = 3 \times 3 \times 10 \times 2 \times 2 = 3 \times 3 \times 5 \times 2 \times 2 \times 2 = 2^3 \times 3^2 \times 5.$$

Un entero (distinto de 0 y 1) que no sea primo se llama *compuesto*. Una de las primeras cuestiones que se presentan en la teoría de los números primos es la de saber si hay solamente un número finito de estos números o si, por el contrario, la clase de los números primos tiene infinitos elementos distintos, como ocurre con la clase de los números enteros de la cual forma parte. La respuesta es: existen infinitos números primos.

La prueba de la infinitud de la clase de los números primos dada por Euclides ha quedado como modelo de razonamiento matemático. Procede por "reducción al absurdo" y parte de la hipótesis de que el teorema es falso. Esto significa que existiría únicamente un número finito de números primos, quizá muchos (por ejemplo, un millón) o, dicho de un modo general, n. Usando subíndices, podríamos indicar dichos números primos por $p_1, p_2, \ldots, p_n$. Cualquier otro entero sería compuesto y debería ser divisible por uno al menos de los $p_1, p_2, \ldots, p_n$.

Vamos a ver que dicha hipótesis nos lleva a una contradicción; para ello, construyamos un número A que será distinto de los primos $p_1, p_2, \ldots, p_n$ por ser mayor que ellos y que, sin embargo, no será divisible por ninguno de los p. Tal número es el

$$A = p_1 \times p_2 \times \ldots \times p_n + 1.$$

Es decir, se obtiene añadiendo 1 al producto de todos los números primos que suponíamos existentes. A es distinto de los p y, por tanto, debe ser compuesto.

Pero dividiendo A por p_1, o por p_2, etc., se obtiene siempre de resto 1; en consecuencia, A no admite ningún p como divisor. Puesto que nuestra hipótesis inicial de que había solo un número finito de números primos nos conduce a una contradicción, dicha hipótesis es absurda y, entonces, la contraria debe ser cierta; esto prueba el teorema.

Aunque la demostración es indirecta, puede modificarse fácilmente para dar un método constructivo, al menos teóricamente, de una sucesión infinita de números primos. Partiendo de un número primo cualquiera, por ejemplo, $p_1 = 2$, supongamos que hemos encontrado n primos $p_1, p_2, p_3, \ldots, p_n$; observemos entonces que el número $p_1 \times p_2 \times \ldots \times p_n + 1$, o bien es primo o bien contiene factores primos que han de ser distintos de los n hallados previamente.

Puesto que estos factores pueden hallarse por ensayos directos, estamos seguros de que, en todo caso, hay al menos un nuevo factor primo p_{n+1}; procediendo de este modo se ve que la sucesión de los números primos construibles no tiene fin.

Ejercicio para entrenarse. Llévese a efecto dicha construcción a partir de $p_1 = 2$, $p_2 = 3$ y obténganse 5 números primos más.

Si un número ha sido expresado como producto de números primos, podemos disponer dichos factores primos en un orden cualquiera. La experiencia demostraría que, salvo la arbitrariedad en la ordenación, la descomposición de un número N en factores primos es única:

Todo entero N, mayor que 1, puede descomponerse en producto de números primos, y solamente de una forma.

Esta proposición parece a simple vista tan evidente que un profano podría inclinarse a admitirla sin prueba. Sin embargo, no es una trivialidad y la demostración, aunque elemental, requiere algunos razonamientos sutiles.

La demostración clásica, dada por Euclides, de este "teorema fundamental de la aritmética" está basada en un método o "algoritmo" para el cálculo del máximo común divisor de dos números. Este método será considerado más adelante. En vez de dicha demostración daremos aquí otra, de cosecha más reciente; más breve, pero quizá más artificiosa que la de Euclides.

Será un ejemplo típico de demostración indirecta. Supondremos la existencia de un entero susceptible de dos descomposiciones básicamente diferentes, y de esta hipótesis resultará una contradicción. Esta contradicción demostrará que la hipótesis de que existe un entero con dos descomposiciones esencialmente diferentes en factores primos es absurda y, como consecuencia, resultará que la descomposición en factores primos de un entero cualquiera es única.

Si existe un entero positivo capaz de descomponerse en dos productos esencialmente diferentes de primos, habrá uno menor que todos los demás para el que se verifique tal propiedad,

$$m = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s, \qquad (1)$$

donde los p y los q son primos. Ordenando de nuevo, si es preciso, los p y los q, podemos suponer que se tiene

$$p_1 < p_2 < \dots < p_r, \quad q_1 < q_2 < \dots < q_s.$$

Ahora bien: p_1 no puede ser igual a q_1 ya que, en caso contrario, dividiendo los dos últimos miembros de (1) por $p_1 = q_1$ se obtendrían dos descomposiciones esencialmente diferentes para un entero menor que m, en contradicción con la elección hecha de m como el entero más pequeño para el cual ese hecho es posible. Por tanto, o bien es $p_1 < q_1$ o se tiene $q_1 < p_1$.

Supongamos $p_1 < q_1$ (Si fuera $q_1 < p_1$ bastaría con cambiar las letras p y q en lo que sigue). Formemos el entero

$$m = m' - (p_1 q_2 q_3 \dots q_s). \qquad (2)$$

Sustituyendo m por las dos expresiones dadas por (1), podríamos escribir el entero m' en una de las dos formas

$$m' = (p_1 p_2 \dots p_r) - (p_1 q_2 \dots q_s) = p_1 (p_2 p_3 \dots p_r - q_2 q_3 \dots q_s) \qquad (3)$$

$$m' = (q_1 q_2 \dots q_s) - (p_1 q_2 \dots q_s) = (q_1 - p_1)(q_2 q_3 \dots q_s). \qquad (4)$$

Puesto que es $p_1 < q_1$, de (4) se sigue que m' es un entero positivo, mientras que de (2) resulta que m' es menor que m. De donde se deduce que, salvo el orden de los factores, la descomposición de m' debe ser única.

Pero de (3) resulta que p_1 es un factor de m'; por tanto, de (4) se concluye que p_1 debe aparecer como factor o de $(q_1 - p_1)$ o de $(q_2 q_3 \dots q_s)$. Esto resulta de suponer la descomposición única para m' (véase el razonamiento del párrafo siguiente). La última hipótesis es imposible, porque p_1 es menor que todas las q. En consecuencia, p_1 debe ser un factor de $q_1 - p_1$ de modo que existirá un h tal que

$$q_1 - p_1 = p_1 \cdot h \quad \text{o} \quad q_1 = p_1(h + 1).$$

Pero esto expresa que p_1 es un factor de q_1 contrariamente al hecho de ser q_1 número primo. Esta contradicción prueba que nuestra hipótesis inicial era absurda y, por tanto, completa la demostración del teorema fundamental de la aritmética.

Un corolario importante de este teorema fundamental es el siguiente: **si un número primo *p* es un divisor del producto *ab*, *p* debe ser factor de *a* o de *b***. Pues si p no fuera divisor de a ni de b, el producto de factores primos que da la descomposición de ab no contendría p. Por otra parte, puesto que se supone que p es un divisor de ab, existirá un entero t tal que

$$ab = pt.$$

En consecuencia, el producto de p por una descomposición en factores primos de t daría una descomposición de ab en factores primos que contendría p, lo que estaría en contradicción con el hecho de que la descomposición en factores primos es única.

Ejemplo. Si se ha comprobado de una parte que 13 es un divisor de 2 652, y, de otra, que es 2 652 = 6 × 442, se puede concluir que 13 es un divisor de 442. Por el contrario, 6 es un factor de 240, y 240 = 15 × 16; sin embargo, 6 no es factor de 15 ni de 16. Esto último prueba que la hipótesis de que p es primo es esencial para el corolario.

Ejercicio para entrenarse. Para hallar todos los divisores de un número cualquiera a es suficiente descomponer a en un producto:

$$a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_r^{\alpha_r}$$

donde las p son los distintos factores primos, cada uno de ellos elevado a una cierta potencia. Todos los divisores de a son los números

$$b = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_r^{\beta_r}$$

donde los β son enteros cualesquiera que satisfacen las desigualdades

$$0 \le \beta_1 \le \alpha_1,\ 0 \le \beta_2 \le \alpha_2,\ \ldots,\ 0 \le \beta_r \le \alpha_r.$$

Demuéstrese esta proposición. Como consecuencia, pruébese que el número de divisores distintos de *a* (incluidos los divisores *a* y 1) viene dado por el producto

$$(\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_r + 1).$$

Por ejemplo,

$$144 = 2^4 \times 3^4$$

tiene 5 × 3 divisores, que son: 1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72 y 144.

2. Distribución de los números primos

Podemos construir una lista de todos los números primos menores que un entero *N* dado escribiendo primero ordenadamente todos los enteros menores que *N*, tachando después todos los que sean múltiplos de 2; luego, todos los restantes que sean múltiplos de 3, y así sucesivamente, hasta que hayan sido eliminados todos los números compuestos (Figura siguiente).

~~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~~	~~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~~

Este proceso, conocido como la *criba de Eratóstenes*, conserva en el tamiz los números primos menores que *N*. Las tablas completas de números primos hasta 10 000 000 han sido calculadas mediante mejoras del método anterior; gracias a ellas se dispone de una masa imponente de datos empíricos referentes a la distribución y otras propiedades de los números primos.

Sobre la base de estas tablas se han adelantado conjeturas plausibles (del mismo modo que si la teoría de números fuese una ciencia experimental), muchas de las cuales resultan de demostración muy difícil.

a) Fórmulas que dan números primos

Se han hecho muchos intentos para obtener fórmulas aritméticas simples que dieran únicamente números primos, aunque no se obtuvieran todos. Fermat hizo la famosa conjetura (no en forma de afirmación definitiva) de que todos los números de la forma

$$F(n) = 2^{2^n} + 1$$

son primos. En efecto, para *n* = 1, 2, 3, 4 se obtiene

$$F(1) = 2^2 + 1 = 5,$$
$$F(2) = 2^{2^2} + 1 = 2^4 + 1 = 17,$$
$$F(3) = 2^{2^3} + 1 = 2^8 + 1 = 257,$$
$$F(4) = 2^{2^4} + 1 = 2^{16} + 1 = 65537,$$

todos los cuales son números primos. Pero en 1732 Euler obtuvo la descomposición

$$2^{2^5} + 1 = 614 \times 6\,700\,417;$$

de donde resulta que $F(5)$ no es primo. Más tarde se comprobó que otros de los números de Fermat eran compuestos, siendo necesarios para dichas comprobaciones métodos difíciles de la teoría de números, a causa de la insuperable dificultad de los ensayos directos. Hasta la fecha, no ha sido probado que sea primo ninguno de los números $F(n)$ para $n > 4$.

Otra sencilla y notable expresión que da varios números primos es

$$f(n) = n^2 - n + 41.$$

Para $n = 1, 2, \ldots, 40$, $f(n)$ es primo; pero para $n = 41$, se tiene $f(n) = 41^2$, que evidentemente no es primo.

La expresión

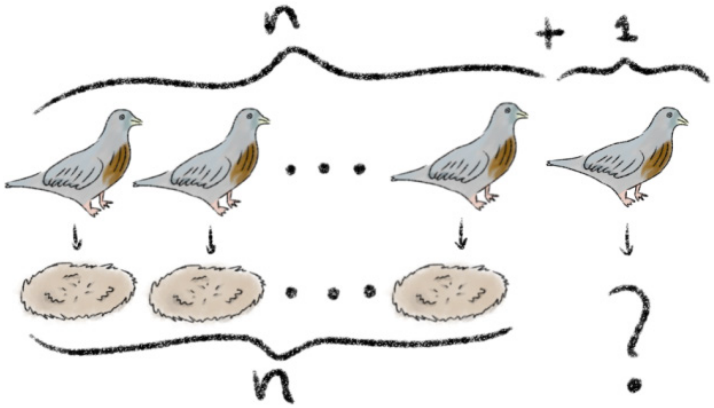
$$n^2 - 79n + 1\,601$$

da primos para n menor que 80, pero falla para $n = 80$. En resumen, puede decirse que la tarea de encontrar expresiones de tipo sencillo que den números primos ha resultado estéril. Ni que decir tiene que la posibilidad de obtener una fórmula algébrica simple que diera todos los números primos aparece como irrealizable.

b) Números primos en una progresión aritmética

Mientras que es muy sencillo demostrar que existen infinitos números primos en la sucesión de enteros 1, 2, 3, …, la extensión de un resultado análogo para sucesiones tales como la 1, 4, 7, 10, 13, … o la 3, 7, 11, 15, 19,… o, más en general, para toda progresión aritmética, $a, a + d, a + 2d, \ldots, a + nd, \ldots$, donde a y d no tienen factores comunes, es bastante más complicada.

Todas las observaciones parecen indicar el hecho de que en toda progresión de dicho tipo existen infinitos números primos, como ocurre para la progresión más simple: 1, 2, 3, … Probar este teorema general requirió un gran esfuerzo. Peter Gustav Lejeune Dirichlet (1805-1859), uno de los matemáticos más notables del siglo XIX, obtuvo ese brillante resultado mediante la aplicación de los métodos más avanzados del análisis matemático de su tiempo.



Retrato de Peter Gustav Lejeune Dirichlet y una representación gráfica de las series infinitas.

Sus trabajos originales sobre este tema se cuentan aún hoy entre los resultados más destacados y, pasado ya más de un siglo, la demostración no ha sido lo suficientemente simplificada como para ser accesible a quienes no posean una buena preparación en la técnica del cálculo y de la teoría de funciones.

Aunque no intentaremos probar el teorema de Dirichlet en toda su generalidad, es fácil extender la demostración de Euclides sobre la infinitud de la sucesión de números primos para desarrollar algunas progresiones aritméticas especiales, tales como $4n + 3$ y $6n + 5$.

Para tratar la primera, observemos que todo número primo mayor que 2 es impar (ya que en otro caso sería divisible por 2) y, por tanto, será de la forma $4n + 1$ o $4n + 3$, para ciertos enteros n. Por otra parte, el producto de dos números de la forma $4n + 1$ es también de esta forma, ya que

$$(4a + 1)(4b + 1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1.$$

Supongamos ahora que no existiera más que un número finito de números primos $p_1, p_2, p_3, \ldots, p_n$, de la forma $4n + 3$, y consideremos el número

$$N = 4(p_1, p_2, \ldots, p_n) - 1 = 4(p_1, \ldots, p_n - 1) + 3$$

O bien N es primo, o bien puede ser descompuesto en producto de números primos, ninguno de los cuales pudiendo ser $p_1, p_2, \ldots, p_n$, puesto que dividiendo N por cualquiera de estos da de resto –1. Además, no todos los factores de N pueden ser de la forma $4n + 1$, ya que N no es de esta forma y, como acabamos de ver, el producto de números de la forma $4n + 1$ es también de esta forma.

Por tanto, al menos uno de dichos factores debe ser de la forma $4n + 3$, lo cual es imposible, puesto que hemos visto que ninguno puede ser de los p y estos formaban, según nuestra hipótesis, todos los números primos de la forma $4n + 3$. En consecuencia, la hipótesis de que no hay más que un número finito de números primos de la forma $4n + 3$ nos ha llevado a una contradicción, lo que demuestra que dicho número debe ser infinito.

Ejercicio para entrenarse. Pruébese el correspondiente teorema para la progresión $6n + 5$.

c) El teorema de los números primos

En el proceso de la investigación en busca de una ley que gobernase la distribución de los números primos, se dio un paso decisivo cuando los matemáticos, dejando de lado los fútiles intentos para hallar una fórmula simple que diera todos los números primos o el número exacto de estos comprendidos entre los n primeros enteros, buscaron en su lugar información relativa a la distribución media de los números primos dentro del conjunto de los enteros.

Para todo entero n, designemos con A_n el número de primos comprendidos entre los enteros 1, 2, 3, …, n. Si subrayamos los números primos de la sucesión formada por los primeros enteros 1, 2, 3, 4, 5, 6, 7, 8, 9 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, …, podremos calcular los valores iniciales de A_n:

$$A_1 = 0, A_2 = 1, A_3 = A_4 = 2, A_5 = A_6 = 3, A_7 = A_8 = A_9 = A_{10} = 4, A_{11} = A_{12} = 5, A_{13} = A_{14} = A_{15} = A_{16} = 6,$$
$$A_{17} = A_{18} = 7, A_{19} = 8, \text{ etc.}$$

Si tomamos ahora una sucesión de valores para n que crezca ilimitadamente, por ejemplo:

$$n = 10, 10^2, 10^3, 10^4, \ldots,$$

la correspondiente sucesión de valores de A_n crecerá también sin límite (pero menos rápidamente). Puesto que sabemos que existen infinitos números primos, los valores de A_n excederán más pronto o más tarde a cualquier número finito. La densidad de los números primos entre los n primeros enteros vendrá dada por el cociente A_n/n, y a partir de la tabla de números primos los valores de A_n/n pueden ser calculados empíricamente para un gran número de valores de n.

N	A_n/n
$\mathbf{10^3}$	0,168
$\mathbf{10^6}$	0,078498
$\mathbf{10^9}$	0,050847478
…	…

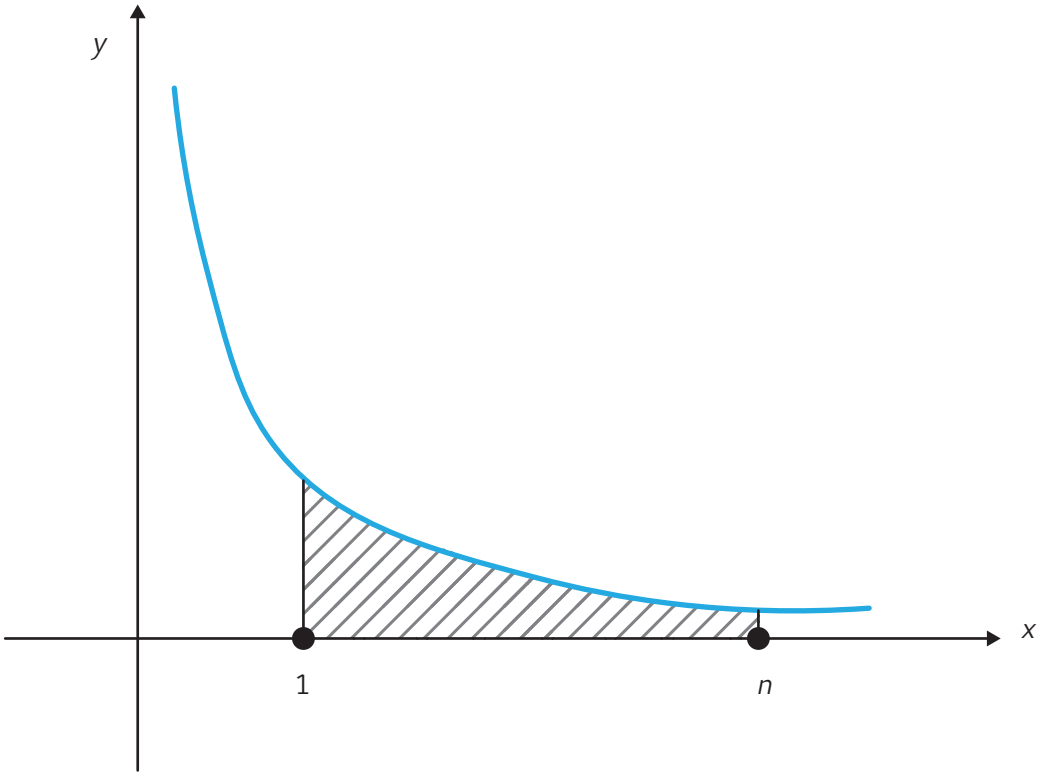
El último número decimal de esta tabla puede considerarse como la probabilidad para que un entero elegido al azar entre los 10^9 primeros enteros sea primo, ya que el número de casos posibles es 10^9, de los cuales A_{10^9} son primos.

La distribución de números primos particulares entre los enteros es muy irregular; pero esta irregularidad en

pequeño desaparece si fijamos nuestra atención en la distribución media de los números primos dada por la razón A_n/n.

La ley sencilla que rige el comportamiento de este cociente es uno de los más notables descubrimientos de toda la matemática. Para establecer el teorema de los números primos, debemos previamente definir el "logaritmo natural" de un entero *n*. Con este objeto, tomemos en el plano dos ejes perpendiculares y consideremos el conjunto de los puntos del plano para los cuales el producto de sus distancias *x*, *y* a estos dos ejes es igual a la unidad.

En función de las coordenadas *x, y*, este lugar, una hipérbola equilátera, queda definido por la ecuación $xy = 1$. El log *n* vendrá definido entonces como el área limitada, en la siguiente figura,



por la hipérbola, el eje *x* y las dos verticales $x = 1$ y $x = n$. (Una exposición más detallada del logaritmo se verá más adelante.)

Del estudio empírico de la tabla de números primos, Gauss dedujo que el cociente A_n/n es aproximadamente igual a $1/\log n$, y que la aproximación mejora al crecer *n*. La bondad de la aproximación viene medida por el cociente $\dfrac{A_n/n}{1/\log n}$, cuyos valores para $n = 1\,000,\ 1\,000\,000,\ 1\,000\,000\,000$ se dan en la tabla siguiente:

n	A_n/n	$1/\log n$	$\dfrac{A_n/n}{1/\log n}$
10^3	0,168	0,145	1,159
10^6	0,078 498	0,072 382	1,084
10^9	0,050 847 478	0,048 254 942	1,053
...	...	...	...

Sobre la base de esta evidencia empírica, Gauss hizo la conjetura de que la razón A_n/n es "asintóticamente igual a $1/\log n$". Lo que quiere decir que si tomamos una sucesión creciente de valores de *n*; por ejemplo, si tomamos para *n*

$$10,\ 10^2,\ 10^3,\ 10^4,\ \ldots$$

como antes hicimos, la razón de A_n/n a $1/\log n$

$$\frac{A_n/n}{1/\log n}$$

calculada para estos valores sucesivos de n se aproximará cada vez más a 1, y que la diferencia entre dicho cociente y 1 será tan pequeña como queramos para valores suficientemente grandes de n. Esta afirmación se expresa simbólicamente, mediante el signo $\sim$ en la forma:

$$A_n/n \sim 1/\log n, \text{ lo que significa que } \frac{A_n/n}{1/\log n} \text{ tiende a 1 al crecer } n.$$

Que el signo $\sim$ no puede ser reemplazado por el signo ordinario de igualdad = resulta evidente si se observa que mientras A_n es siempre entero, $n/\log n$ no lo es.

El hecho de que el comportamiento medio de la distribución de los números primos pueda ser descrito mediante la función logarítmica es un descubrimiento notable, ya que resulta sorprendente que dos conceptos matemáticos que parecen tan inconexos estén en realidad tan íntimamente ligados.

Aunque el enunciado de la conjetura de Gauss es fácil de comprender, una demostración rigurosa de dicha conjetura era inaccesible a los métodos de la ciencia matemática de su época. Para probar el teorema, que se refiere únicamente a conceptos elementales, es necesario emplear los métodos más potentes de la matemática moderna.

Fueron precisos casi cien años antes de que el análisis se desarrollara lo suficiente para que Jacques Hadamard (1896), en París, y Charles-Jean de la Vallée Poussin (1896), en Lovaina, pudieran dar una demostración completa del teorema de los números primos.

Importantes simplificaciones y modificaciones fueron realizadas por Hans Carl Friedrich von Mangoldt (1854-1925), un matemático alemán que contribuyó a la solución del teorema de los números primos. Y Edmund Georg Hermann Landau (1877-1938), otro matemático alemán de origen judío, trabajó en el campo de la teoría de números y el análisis complejo.

Mucho antes del resultado de Hadamard, Riemann (1826-1866) había contribuido al problema con una decisiva labor de exploración en un célebre trabajo en el cual aparecen definidas las direcciones estratégicas del posible ataque. Y hace ya un tiempo que el matemático norteamericano Norbert Wiener fue capaz de modificar la demostración de modo de evitar el uso de números complejos en un paso importante del razonamiento. En todo caso, la demostración del teorema de los números primos continúa siendo una cuestión difícil, incluso para estudiantes avanzados. Volveremos a ocuparnos del tema en su tratamiento más actual.

En 1949, Atle Selberg (1917-2007), un joven matemático noruego, se hizo conocer por sus trabajos sobre la teoría analítica de los números y la hipótesis de Riemann. Siendo estudiante, Selberg fue influenciado por los trabajos y la personalidad del matemático indio Srinivasa Ramanujan (1887-1920). Estudió en la Universidad de Oslo, donde obtuvo el doctorado en 1943. Durante la Segunda Guerra Mundial se dedicó en solitario al estudio de la función zeta de Riemann. En 1948 realizó una demostración elemental del teorema de los números primos. A la vez, el matemático húngaro Paul Erdős realizó su propia demostración, por lo que se inició una disputa entre los dos, sobre quién había demostrado primero el teorema. Por todos sus resultados, Selberg recibió la medalla Fields en 1950. En esos años 50 se marchó a los Estados Unidos, al Instituto de Estudios Avanzados de Princeton, donde consiguió importantes resultados trabajando sobre el operador laplaciano y la superficie de Riemann, y recibió el premio Wolf en 1986.

d) Dos problemas no resueltos referentes a los números primos

Mientras que el problema de la distribución media de los números primos ha sido resuelto favorablemente, quedan otras varias conjeturas que, sostenidas por la evidencia empírica, no han podido hasta ahora ser probadas como ciertas.

Una de ellas es la famosa *conjetura de Goldbach*. Christian Goldbach (1690-1764) aparece en la historia de la matemática únicamente por esa conjetura que propuso como problema en una carta a Euler en 1742. Comprobó que, en todos los casos observados, todo número par (excepto el 2, que es primo) puede ser

representado como suma de dos números primos; por ejemplo: 4 = 2 + 2, 6 = 3 + 3, 8 = 5 + 3, 10 = 5 + 5, 12 = 5 + 7, 14 = 7 + 7, 16 = 13 + 3, 18 = 11 + 7, 20 = 13 + 7, …, 48 = 29 + 19, …, 100 = 97 + 3, etcétera.

Goldbach preguntaba a Euler si era capaz de demostrar que esa propiedad es cierta para todo número par, o si podría encontrar un contraejemplo. Euler no pudo dar una respuesta, ni nadie ha podido darla hasta ahora. La evidencia empírica a favor de la proposición de que todo número par puede ser representado de ese modo es bastante convincente, como puede verificar cualquiera ensayando en algunos ejemplos. El origen de la dificultad reside en el hecho de que los números primos se definen mediante la multiplicación, mientras que el problema se refiere a la adición. En términos generales, resulta difícil establecer conexiones entre las propiedades aditivas y las multiplicativas de los enteros.

Hasta hace poco tiempo, una demostración de la conjetura de Goldbach parecía completamente inaccesible. Hoy, en cambio, no parece estar muy lejos la solución de este problema. Un éxito importante, completamente inesperado y que sorprendió a los expertos, fue alcanzado en 1931 por un joven matemático ruso desconocido hasta entonces, Lev Schnirelmann (1905-1938), quien probó que todo entero positivo puede ser representado como suma de a lo sumo 300 000 números primos.

Aunque este resultado pueda parecer ridículo en comparación con el problema inicial de probar la conjetura de Goldbach, fue sin embargo el primer paso en la dirección justa. La prueba es directa y constructiva, a pesar de no dar un método práctico para encontrar la descomposición en suma de números primos para un entero arbitrario.

Posteriormente, el matemático ruso Iván Vinográdov, usando métodos debidos a Godfrey Hardy, John Edensor Littlewood y a su gran colaborador indio Ramanujan, ha conseguido reducir el número de 300 000 a 4, lo que está mucho más cerca de la solución del problema de Goldbach. Sin embargo, hay una diferencia notable entre los resultados de Schnirelmann y los de Vinográdov, más significativa aún que la diferencia entre 300 000 y 4.

El teorema de Vinográdov ha sido demostrado únicamente para enteros "suficientemente grandes"; con más precisión: Vinográdov ha probado que existe un entero N tal que todo entero $n > N$ puede ser representado como suma de, a lo más, cuatro números primos. Su demostración no permite determinar N: en contraste con el teorema de Schnirelmann, el de Vinográdov es esencialmente indirecto y no constructivo.

Lo que realmente prueba Vinográdov es que la hipótesis de que existen infinitos enteros que no pueden descomponerse en suma de 4 números primos es absurda. Aquí se tiene un buen ejemplo de la profunda diferencia existente entre los dos tipos de demostración, directa e indirecta.

El problema siguiente, más notable aún que el de Goldbach, está todavía muy lejos de ser resuelto. Se ha observado que los números primos se suceden frecuentemente en pares de la forma p y $p + 2$. Así, por ejemplo, 3 y 5, 11 y 13, 29 y 31, etc. Se cree que la proposición que afirma la existencia de infinitos pares de ese tipo es cierta; sin embargo, hasta el presente no se ha podido dar el menor paso aprovechable en el camino de demostrar tal proposición.