Taller de Ciencia para Jóvenes
CIMAT, 20-31 julio, 1998

Introducción a la Teoría de Números

Gil Bor
Centro de Investigación en Matemáticas
Guanajuato, México

Contents

Prefacio

Estas notas las escribí para acompañar los cursos de "Ciencia para Jóvenes" para alumnos de escuelas preparatorias en los años 1997-8, que se llevaron acabo en el Centro de Investigación en Matemáticas (CIMAT) en Guanajuato, México. El material lo redacté en su mayoría del libro de Hardy y Wright, *"An introduction to the Theory of Numbers"* (Oxford University Press, 4th edition, 1971). Otra fuente importante – principalmente de los ejercicios – fue el libro de André Weil, *"Number Theory for Beginners"* (Springer-Verlag, 1979). La mayoría de los ejercicios que aparecen dentro de cada sección son fáciles y el lector se debería asegurar que los puede resolver. Al final de cada sección aparecen ejercicios adicionales (en general más difíciles) para seguir digerir aún más el material de la sección. Libros adicionales que pueden resultar útiles para el lector interesados en el tema son:

- *"The book of Numbers"*, por John Conway y Richard Guy (Springer-Verlag, 1996). Es un libro facinante y poco común (reflejando la personalidad del primer autor), repleto de ideas e ilustraciones maravillosas. He oído que este libro fue traducido al español.

- *"Resolución de Ecuaciones en Números Enteros"* por A. O. Gelfand (Mir, 1979). Traducido al español del ruso. Escrito por uno de los mejores matemáticos rusos.

- *"Modern Elementry Theory of Numbers"*, por L. E. Dickson (The University of Chicago Press, 1947). Un clásico del tema.

  Todos estos libros se encuentran en la biblioteca del CIMAT.

Gil Bor
Julio, 1998
CIMAT, Guanajuato.

1 Conceptos básicos

1.1 Divisibilidad de enteros

Los números

$$\ldots, -3, -2, -1,\ 0,\ 1,\ 2, \ldots$$

se llaman los *enteros*; los números

$$0, 1, 2, 3, \ldots$$

los *enteros no-negativos*; y los números

$$1, 2, 3 \ldots$$

los *enteros positivos*. Los enteros positivos forman la materia prima de la aritmética, pero a veces es esencial considerarlos como una sub-clase de una clase más amplia de números como los enteros.

Se dice que un entero n es *divisible* por otro entero d, distinto de cero, si existe un entero, digamos m, tal que $n = d \cdot m$.

Si n y d son positivos, m también es necesariamente positivo. Expresamos el hecho que n es divisible por d, o que d es un *divisor* de n, por

$$d|n.$$

Así tenemos que

$$1|n \quad \text{y} \quad n|n,$$

para todo n, y $d|0$ para todo $d \neq 0$.

Ejercicio 1 *Encuentra todos los divisores de 4.*

Respuesta: 1, 2, 4, -1, -2, -4.

Ejercicio 2 *Encuentra todos los divisores positivos de 100.*

Respuesta: 1, 2, 4, 5, 10, 20, 25, 50, 100.

Ejercicio 3 *Encuentra todos los enteros positivos divisibles por 10.*

Es bastante fácil demostrar que

$$\begin{aligned} a|b, b|c &\implies a|c, & (1)\\ a|b &\implies ac|bc, & (2)\\ a|b, a|c &\implies a|\,(bm+cn) & (3)\end{aligned}$$

para todo m, n enteros. (La notación "A $\Longrightarrow$ B'' significa "el hecho A implica el hecho B'').

Demostramos (1): Si $a|b$ entonces existe un entero m_1 tal que $b = am_1$; y si $b|c$ existe un entero m_2 tal que $c = bm_2$. Llamamos m al producto m_1m_2; entonces tenemos que $c = bm_2 = (am_1)m_2 = a(m_1m_2) = am$, así que $a|c$, según la definición. Dejamos la demostración de (2) y (3) como un ejercicio.

Ejercicios Adicionales.

Ejercicio 4 *Demuestra que 13 divide a* $4^{2n+1} + 3^{n+2}$ *para todo entero* $n \geq 0$. *(Sugerencia: inducción).*

Ejercicio 5 *Demuestra que para cualquier triple pitagórico* x, y, z *(i.e.* $x^2 + y^2 = z^2$*), 60 divide a* xyz.

1.2 Números primos

Entre los enteros positivos hay una sub-clase de importancia particular, la clase de los primos. Un número entero positivo p se llama *primo* si

(i) $p > 1$,
(ii) p no tiene divisores positivos además de 1 y p.

Por ejemplo, 37 es un primo. Es importante notar que 1 no se considera primo. Normalmente reservamos la letra p para los primos.

Un número entero positivo mayor que 1 y no primo se llama *compuesto*. Aquí está nuestro primer teorema:

Teorema 1 *Todo entero positivo, con excepción del 1, es un producto de primos.*

Demostración. Sea n un entero positivo mayor que 1. Si n es primo, no hay nada que probar. Si n no es primo, o sea compuesto, entonces tiene divisores entre 1 y n. Si m es el más pequeño entre estos divisores, m debe ser primo; porque si no, entonces m tendría un divisor l, $1 < l < m$, que necesariamente sería también un divisor de n. Esto contradice la elección de m como el divisor más pequeño; así que m debe ser primo.

Concluimos entonces que si n no es primo es divisible por un primo, digamos p_1, o sea

$$n = p_1 n_1,$$

donde n_1 es un entero positivo, $1 < n_1 < n$. Si n_1 es primo la demostración está terminada, y si no, continuamos como antes: n_1 es divisible por un primo p_2 menor que n_1, así que

$$n = p_1 n_1 = p_1 p_2 n_2,$$

donde n_2 es un entero positivo, $1 < n_2 < n_1 < n$.

Así seguimos y obtenemos una sucesión decreciente de enteros positivos $n > n_1 > n_2 > n_3 > \ldots > 1$. Tarde o temprano este proceso tiene que parar, o sea obtenemos un $n_k = p_k$ primo, y

$$n = p_1 p_2 p_3 \ldots p_{k-1} p_k. \tag{4}$$

Esto completa la demostración. □

Por ejemplo, si empezamos con 666, obtenemos

$$666 = 2 \cdot 3 \cdot 3 \cdot 37.$$

Ahora una observación que nos ayuda a averiguar si un entero n es compuesto o primo:

Ejercicio 6 *Demuestra que si n no es primo entonces tiene un divisor primo p en el rango $1 < p \leq \sqrt{n}$.*

Por ejemplo, para averiguar si 79 es un primo, es suficiente buscar un divisor primo menor que 9 (notando que $8 < \sqrt{79} < 9$). Como 2,3,5 y 7 no dividen a 79 concluimos que 79 es un primo.

Los primos en la factorización (4) no son necesariamente distintos, o arreglados en un orden particular. Si los arreglamos en orden creciente, agrupando conjuntos de primos idénticos en un único factor, y cambiamos la notación un poco, obtenemos

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}, \tag{5}$$

donde $a_1, a_2, \dots$ son enteros positivos. Decimos entonces que n está expresado en *forma estandar*. Por ejemplo,

$$169400 = 2^3 \cdot 5^2 \cdot 11^2$$

es una expresión de 169400 en forma estandar.

Ejercicio 7 *Cuantos enteros hay entre 1 y 100 en cuya forma estandar participan exactamente 2 primos? 3 primos?*

1.3 El Teorema Fundamental de la Aritmética

No hay nada en la demostración del Teorema 1 que nos asegure que la expresión de n como un producto de primos es única, salvo orden de los factores, o dicho de otra manera, que n tiene una sola forma estandar. Pero si consideramos algunos casos particulares sospechamos que esto es cierto.

Teorema 2 ("El Teorema Fundamental de la Aritmética") *La forma estandar de un entero positivo n es única; en otras palabras, se puede expresar n como un producto de primos en solo una manera, salvo por el orden de los factores.*

El teorema 2, como su nombre implica, es muy básico, e indispensable para el estudio sistemático de los números enteros. Al parecer, el teorema fue anunciado explicitamente por primera vez por el matemático alemán Carl Friedrich Gauss (1777-1855) en su libro *Disquisitiones arithmeticae* (1801), aunque sin duda el resultado ya era conocido antes de Gauss. La demostración del teorema no es muy difícil, pero sí un poco larga. Por el momento la posponemos.

Ahora, debe ser obvio porque insistimos que 1 no sea primo. Si lo fuera, tendríamos que corregir el Teorema 2, pues siempre podría uno añadir cualquier número de 1's en la forma estandar.

Damos ahora algunas ilustraciones de la utilidad de nuestro Teorema Fundamental.

Un entero positivo d que divide a dos enteros a y b simultáneamente, $d|a$ y $d|b$, se llama un *divisor común* de a y b. Obviamente, $d \leq \min\{a, b\}$ (el mínimo entre a y b). Denotamos el *divisor común máximo* de a y b por (a, b). Por ejemplo, $(4, 6) = 2$, y si $a > 0$ entonces $(a, 0) = (-a, 0) = a$.

Si $(a, b) = 1$ decimos que a y b son *primos relativos*, o *coprimos*. Por ejemplo, 9 y 14 son primos relativos. Usando el Teorema Fundamental obtenemos una fórmula sencilla para (a, b).

Teorema 3 *Si*

$$a = \Pi_p p^\alpha \qquad (\alpha \geq 0)$$

y

$$b = \Pi_p p^\beta \qquad (\beta \geq 0),$$

entonces

$$(a, b) = \Pi_p p^{\min\{\alpha,\beta\}}.$$

La notación $a = \Pi_p p^\alpha$ es una notación breve para la factorización de a en primos, y significa que estamos considerando un producto de términos de la forma p^α, para todo los primos p, donde la potencia α depende de p. Por supuesto, los α's son todos ceros excepto para un número finito de primos, así que el producto es realmente finito.

El teorema es una consecuencia inmediata del Teorema Fundamental y dejamos la demostración como un ejercicio.

Por ejemplo, para obetener el divisor común máximo de 79380 y 2142, calculamos primero sus formas estandar,

$$79380 = 2^2 \cdot 3^4 \cdot 5 \cdot 7^2, \qquad 2142 = 2 \cdot 3^2 \cdot 7 \cdot 17,$$

y obtenemos inmediatamente que su divisor común máximo es

$$2 \cdot 3^2 \cdot 7 = 126.$$

El *mínimo común múltiple* de dos números a y b es el positivo mínimo divisible por ambos a y b, y está denotado por $\{a, b\}$. Tenemos entonces que $a|\{a, b\}$, $b|\{a, b\}$.

Teorema 4 *En la notación del Teorema 3,*

$$\{a, b\} = \Pi_p p^{\max\{\alpha,\beta\}}.$$

Por ejemplo, el mínimo común múltiple de $79380 = 2^2 \cdot 3^4 \cdot 5 \cdot 7^2$ y $2142 = 2 \cdot 3^2 \cdot 7 \cdot 17$ es

$$2^2 \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 17 = 1,349,460.$$

Dejamos la demostración de este teorema también como un ejercicio.

Teorema 5

$$\{a, b\} = \frac{ab}{(a, b)}.$$

Demostración. Es una consecuencia de los dos teoremas anteriores y la identidad obvia

$$\min\{\alpha, \beta\} + \max\{\alpha, \beta\} = \alpha + \beta.$$

□

Otro resultado básico que derivamos del Teorema Fundamental es

Teorema 6 *Si p es un primo, y $p|ab$, entonces $p|a$ ó $p|b$.*

La condición de ser primo es claramente esencial; por ejemplo, $6|3 \cdot 4$, pero 6 no divide a 3 ni a 4.

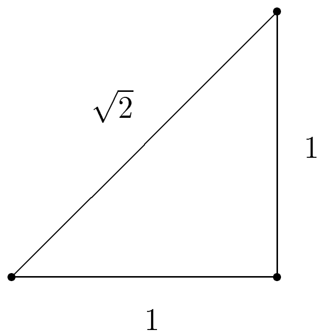
Demostración. Escribimos a y b como productos de primos, $a = p_1 p_2 \ldots$, $b = q_1 q_2 \ldots$, así que $ab = p_1 p_2 \ldots q_1 q_2 \ldots$. Segun el Teorema Fundamental, si $p|ab$ entonces p debe ser uno de los primos en la expresion de ab como producto de primos; o sea p es uno de los p_i's o uno los q_j's. En el primer caso $p|a$, y en el segundo caso $p|b$. □

Presentamos una aplicación interesante de este último teorema. Primero una definición: un número, no necesariamente entero, es *racional*, si se puede expresar como la razón de dos enteros m/n. Por ejemplo $3/4$ es racional y todos los números enteros son racionales. Un número no racional se llama *irracional*.

Si construimos un triángulo rectángulo con dos lados de longitud 1, la longitud l del tercer lado, la *hipotenusa*, satisface, según el teorema de Pitágoras,

$$l^2 = 2,$$

o sea $l = \sqrt{2}$.



Teorema 7 *$\sqrt{2}$ es irracional.*

Demostración. Si lo fuera, entonces podríamos escribir $\sqrt{2} = m/n$, con m y n enteros positivos, y suponer también que son primos relativos, $(m, n) = 1$. Así que $2n^2 = m^2$ y $2|m^2$. Como 2 es un primo, el teorema anterior implica que $2|m$, así que $m = 2k$, donde k es un entero positivo. Obtenemos entonces

$$2n^2 = (2k)^2 = 4k^2 \implies n^2 = 2k^2.$$

Ahora tenemos $2|n^2 \implies 2|n$, así que 2 es un divisor común de m y n, contradiciendo la suposición original. $\square$

Ejercicios Adicionales.

Ejercicio 8 *Demuestra que si un entero es divisible por ambos 2 y 3, entonces es divisible por* $2 \cdot 3 = 6$.

Respuesta: Si n es divisible entre 2 entonces es de la forma $n = 2l$ para un entero l. Si es divisible entre 3 es de la forma $n = 3m$, para un entero m. Así que $n = 2l = 3m$. Pero como 2 y 3 son primos, *ambos deben aparecer en la factorización de n como productos de primos* (según el Teorema Funadamental de la Aritmética). Así que $n = 2 \cdot 3 \cdot k$, para un entero k, así que n es divisible por 6.

Ejercicio 9 *Encuentra un par de enteros* a *y* b *y un entero divisible por* a *y* b *pero no por* $a \cdot b$.

Ejercicio 10 *Para cuales pares de enteros* a *y* b*, los enteros divisibles por ambos* a *y* b *son divisibles por* $a \cdot b$.

(Sugerencia: usar el Teorema Fundamental de la Aritmética).

Ejercicio 11 *Sean* a, b *dos enteros.*

a) Suponte que existen dos enteros x, y *tal que* $ax + by = 1$*. Demuestra que* $(a, b) = 1$.

b) Ahora suponte que $(a, b) = 1$*. Demuestra que existen 2 enteros* x, y *tal que* $ax + by = 1$.

Ejercicio 12 *Para un entero positivo* n *denotamos por* $n!$ *("n factorial") el producto* $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ *. Demuestra que para todos enteros positivos* a, b*, el número* $a!b!$ *divide al número* $(a+b)!$.

(Sugerencia: hay varias maneras de demostar este hecho. Una es por inducción; por ejemplo inducción sobre $a + b$*. Otra manera, mas interesante, es demostrar que la expresión* $(a+b)!/(a!b!)$ *es el número de sub-grupos distintos de* a *niños que se puede formar de una clase de* $a + b$ *niños. Como este número es claramente un número enteros,* $a!b!$ *tiene que dividir a* $(a + b)!$ *para que* $(a + b)!/(a!b!)$ *salga un número entero.)*

Ejercicio 13 *a) Demuestra que si* a, b *son dos enteros que dividen a un tercer entero* c*, entonces* $(a, b) = 1$ *implica que* ab *divide a* c *también.*

b) Encuentra un contra-ejemplo al inciso de a) en el caso de $(a, b) \neq 1$.

Ejercicio 14 *Demuestra que* $\sqrt{3}$ *es irracional.*

Ejercicio 15 *Demuestra que* $\sqrt{6}$ *es irracional.*

Ejercicio 16 *Demuestra que para todo entero* n*, si* $\sqrt{n}$ *no es entero, entonces es irracional.*

1.4 El algoritmo de Euclides

En la última sección vimos un método para encontrar el divisor común máximo (a,b) de dos enteros a y b, usando la forma estandar de estos enteros (su factorización en primos). Pero existe otro método (o “algoritmo”), mucho más eficiente, descrito por el matemático griego Euclides (365-300 BC, aproximadamente) en su libro “Elementos”. El algoritmo está basado en el siguiente hecho.

Ejercicio 17 *Sean a y b dos enteros positivos y distintos, digamos $a > b$. Dividimos a entre b con resíduo r, $0 \le r < b$. Demuestra que $(a,b) = (b,r)$.*
(Sugerencia: investigar la relación $a = bq + r$).

Ahora debe ser claro como seguir. Si $r = 0$, es decir $b|a$, entonces $(a,b) = b$, y sino, dividimos a b entre r con resíduo, digamos r_1. Así segimos con $b > r_1 > r_2 > ....$, tal que $(a,b) = (b,r_1) = (r_1,r_2) = ...$ hasta que en algun momento tenemos residuo 0, digamos $r_{n+1} = 0$, así que $(a,b) = r_n$.

Ejercicio 18 *Aplica el algoritmo para encontrar el divisor común máximo de* 1998 *y* 2998.

Ejercicio 19 *Demuestra que en la “sucesión de Fibonacci”, 1,2,3,5,8,13, ..., en donde cada termino, empezando con el tercero, es la suma de los dos anteriores, cada dos elemntos consecutivos son primos relativos.*

1.5 La sucesión de los primos

Los primeros primos son

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, \ldots$$

Es fácil construir una tabla de primos, hasta un límite N no muy grande, por una técnica conocida como la ”criba de Eratostenes”. Ya hemos visto (Ejercisio 6 que si $n \le N$, y n no es primo, o sea n es compuesto, entonces n debe ser divisible por un primo no más grande que $\sqrt{N}$. Ahora escribimos una lista de los números

$$2, 3, 4, 5, \ldots, N$$

y eliminamos sucesivamente

(i) $4, 6, 8, 10, \ldots,$ o sea 2^2 y luego cada número par,

(ii) $9, 15, 21, 27, \ldots,$ o sea 3^2, y luego todos los múltiplos de 3 no eliminados todavía,

(iii) $25, 35, 55, 65, \ldots,$ o sea 5^2, el cuadrado del siguiente número que queda, y luego todos los múltiplos de 5 no eliminados todavia,...

Así continuamos el proceso hasta que el siguiente número que queda, despues del último número cuyos múltiplos fueron eliminados, es mayor que $\sqrt{N}$. Los números que quedaron, los que no fueron eliminados por la criba, son todos los primos entre 1 y N. Prácticamente todas las tablas de primos están construidas por este método.

Las tablas indican que la sucesión de los primos es infinita. El número total de primos menores que 10 millones es 664,579, y el número de primos que hay entre 9,900,000 y 10,000,000 es 6,134. El número total de primos menores que 1,000,000,000 es 50,847,478. Se conocen también unos primos muy grandes, la mayoría de la forma $2^m - 1$. Los más grandes conocidos tienen miles de dígitos y se siguen encontrando más y más grandes todo el tiempo.

Todo esto sugiere el siguiente teorema de Euclides.

Teorema 8 *El número de primos es infinito.*

Demostración. Existen varias demostraciones del teorema. Presentamos la demostración original de Euclides.

Sean $2, 3, 5, \ldots, p$ todos los primos entre 2 y un primo p, y vamos a demostrar la existencia de un primo nuevo, mayor que p. Sea

$$N = (2 \cdot 3 \cdot 5 \cdot \ldots \cdot p) + 1.$$

Si N no es primo es divisible por un primo. Pero N no es divisible por ninguno de los primos $2, 3, 5, \ldots, p$ (dividiendo a N por cualquiera de estos números da residuo 1), así que si N no es primo es divisible por un primo entre p y N. De cualquier modo obtenemos un primo mayor que p. $\square$

Por ejemplo, empezando con el primo 2, obtenemos por el método de esta demostración una sucesión de primos

$$2, 3, 7, 43, 1907, \ldots$$

Este método no es muy efectivo – hay maneras mucho mejores de encontrar primos – pero tiene la virtud de convertir a la demostración de Euclides en una demostración *constructiva*: el argumento de Euclides no solo muestra que el número de primos es infinito, sino también nos construye, paso por paso, una sucesión infinita de primos.

Ejercicio 20 *Aquí vemos una demostración alternativa para la existencia de una infinidad de primos.*

a) Demuestra que para a par y $m \neq n$, $a^{2^m} + 1$ *y* $a^{2^n} + 1$ *son primos relativos.*

(Sugerencia: si $m < n$, *demuestra que* $a^{2^m} - 1$ *divide a* $a^{2^n} + 1$. *Usa el algoritmo de Euclides).*

b) Dedudce de a) que hay una infinidad de primos.

(Sugerencia: considera, para un a par, la sucesión infinita $a^2 + 1, a^{2^2} + 1, a^{2^3} + 1, a^{2^4} + 1, \ldots$. *Según a), los factores primos de cada uno de estos numeros no aparecen en ninguno de los otros.)*

Ejercicio 21 *Demuestra que la sucesión* $3, 7, 11, 15, 19, \ldots$ *(i.e. todos los números de la forma* $4k + 3$*) contiene una infinidad de primos.*

(Sugerencia: se puede adaptar el método de la demostración de Euclides del teorema 8 para este caso. Dada una lista $3, 7, 11, 19, \ldots, p$ *de tal primos, considera a* $N = (3 \cdot 5 \cdot \ldots \cdot p) + 1$.*)*

1.6 Algunas preguntas acerca de los primos

La distribución de los primos entre los enteros positivos, en "promedio", es muy regular; su densidad muestra una disminución continua pero lenta. El número de primos en los primeros 5 "bloques" de 1000 es

$$168, 135, 127, 120, 119,$$

y los de los últimos 5 bloques menores que 10,000,000 son

$$62, 58, 67, 64, 53.$$

Estos últimos 53 primos estan divididos en grupos de

$$5, 4, 7, 4, 6, 3, 6, 4, 5, 9$$

entre los 10 "bloquecitos" de 100 del último millar.

Por otro lado, la distribución *detallada* de los primos es extremadamente irregular. En primer lugar, las tablas muestran bloques grandes de números compuestos. Después del primo 370,261 hay un bloque de 111 números compuestos. Es bastante fácil ver que estos bloques grandes de compuestos deben ocurrir: tomamos todos los primos

$$2, 3, 5, \ldots, p$$

hasta un primo p. Si definimos

$$N = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p,$$

tenemos que todos los $p - 1$ números

$$N + 2, N + 3, N + 4, \ldots, N + p$$

son compuestos. Esto es cierto porque si tomamos uno de estos números, diagamos $N + m$, $2 \leq m \leq p$, m es divisible por uno de los primos, digamos q, $2 \leq q \leq p$, y este q divide también a N, así que q divide a $N + m$. Según el Teorema 8 hay primos arbitrariamente grandes, así que obtenemos

Teorema 9 *Existen bloques arbitrariamente largos de compuestos consecutivos.*

Examinamos ahora otro fenómeno, la ocurrencia de bloques de primos. Las tablas de primos indican la persistencia indefinida de *pares primos*, como $3, 5$ o $101, 103$, cuya diferencia es 2. Hay 1224 tales pares $(p, p + 2)$ antes de $100, 000$, y 8169 antes de 1,000,000. Esto sugiere la

conjetura: hay un número infinito de pares primos $(p, p + 2)$.

De hecho, es razonable conjeturar más. Si tomamos los tres números $p, p + 2, p + 4$, los tres no pueden ser primos, porque uno de ellos es divisible entre 3 (ejercicio), pero no hay una razón obvia para no tener ternas de primos de la forma $p, p + 2, p + 6$, o $p, p + 4, p + 6$, y la evidencia de las tablas sugiere que estas ternas también persisten indefinitivamente. Llegamos entonces a otra *conjetura: hay un número infinito de ternas de primos de la forma* $(p, p+2, p+6)$ *y* $(p, p+4, p+6)$.

Estas conjeturas, y otras similares, acerca de bloques más grandes de primos, no tienen hasta la fecha demostraciones ni contraejemplos.

¿Que otras preguntas naturales se puede hacer acerca de una sucesión de números como los primos? Aquí consideramos algunas.

(i) ¿Existe una fórmula sencilla general que produce la sucesión de todos los primos?

No se conoce una fórmula tal, y es probable que no exista, porque la distribución de los primos es distinta de la que esperaríamos de la existencia de esa fórmula. Aún así, no podemos excluir la posibilidad de que tal fórmula exista.

Una pregunta similar, con comentarios semajantes, es

(ii) ¿existe una fórmula general que produce a partir de un primo, el primo que le sigue (o sea una fórmula tipo $p_{n+1} = p_n^2 + 1$*)?*

O una pregunta aún más modesta como

(iii) ¿existe una regla sencilla que produce, dado un primo p*, otro primo más grande?*

Como hemos visto antes, la demostración del Teorema 8 nos sugiere una regla de este tipo, pero esta regla está muy lejos de ser sencilla o efectiva, si la examinamos de cerca. El único intento razonable en la dirección de estas preguntas fue una conjetura del matemático francés Pierre de Fermat (1601-1665). Los llamados "números de Fermat" son los números definidos por la fórmula

$$F_n = 2^{2^n} + 1,$$

así que

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65,537.$$

Estos 5 números son primos y Fermat conjeturó que todos son primos. Desafortunadamente, no es cierto.

Ejercicio 22 *Demuestra que* $2^{32}+1$ *no es un primo.*
(Sugerencia: demuestra que 641 es un divisor.)

Esto fue descubierto en 1732, por el matemático suizo Leonhard Euler (1707-1783). Hoy en día conocemos muchos otros números de Fermat compuestos y de hecho no se ha encontrado ningún otro número de Fermat primo, más que los 5 mencionados arriba, así que más razonable será conjeturar que el número de primos entre los F_n es *finito*. Pero los números de Fermat tienen mucho interés en la teoría de números; por ejemplo, Gauss demostró que si F_n es un primo p, entonces es posible construir con compás y regla un polígono regular con p lados. La construcción para el caso de $p = 3$ es muy fácil, la de $p = 5$ un poco menos fácil pero todavía "clásica" (conocida por los griegos antiguos), pero la construcción para el caso de $p = 17$ ya es muy difícil y se necesitaba de alguien como Gauss para encontrarla.

Otra pregunta interesante es

> *(iv) ¿cuantos primos hay menores que un número dado* x*?*

Esta pregunta es mucho más productiva, pero necesita una interpretación cuidadosa. Denotamos por $\pi(x)$ el número de primos menores o iguales a x, así que $\pi(1) = 0$, $\pi(2) = 1$, $\pi(20) = 8$. De hecho, si tuviésemos una fórmula exacta para $\pi(x)$, podríamos usarla para producir una lista de todos los números primos; si denotamos por p_n el n-ésimo primo ($p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$), es claro que $\pi(p_n) = n$, así que la fórmula deseada para p_n se obtiene al invertir (o resolver) la última ecuación, expresando p_n en términos de n. En consecuencia, pedir una fórmula sencilla para $\pi(x)$ es prácticamente repetir la pregunta (i). Tenemos entonces que reinterpretar la pregunta de otra manera, y preguntar

> " *¿Cuantos primos* aproximadamente *hay...?*" *¿será cierto que la "mayoría" de los números son primos, o solo una pequeña fracción? ¿existe una expresión sencilla,* $f(x)$*, que sea una "buena aproximación" a* $\pi(x)$*?*

La pregunta, en esta forma modificada, fue respondida por varios matemáticos, empezando por el matemático ruso Pafnuty Lvovich Chebyshev (1821-1894) alrededor de 1850. Para anunciar la respuesta tenemos que usar la función logarítmica $\log x$.

Teorema 10 ("El teorema de los números primos") *Una "buena aproximación", para x grande, de la función $\pi(x)$ es*

$$\pi(x) \sim \frac{x}{\log x};$$

y más precisamente, si llamamos $f(x)$ al lado derecho de esta aproximación, entonces tenemos que la razón $\pi(x)/f(x)$ tiende a 1 cuando x tiende a infinito.

Para tener idea de lo que dice el teorema notamos que la función $x/\log x$ es una función que tiende a infinito más lento que x, pero más rápido que cualquier raíz $\sqrt[a]{(x)}$, $a > 1$, y que es la función más sencilla con esta propiedad.

Es interesante comparar el Teorema 10 con la evidencia de las tablas. Los valores de $\pi(x)$ para $x = 10^3$, $x = 10^6$, $x = 10^9$, son

$$168, \quad 78{,}498, \quad 50{,}847{,}478;$$

mientras los valores de la aproximación $x/\log x$, al entero más cercano, son

$$145, \quad 72{,}382, \quad 48{,}254{,}942.$$

Las razones de de estos números son

$$1.159\ldots, \quad 1.084\ldots, \quad 1.053\ldots,$$

e indica una convergencia, bastante lenta, a 1.

Existen muchas más conjeturas y preguntas no contestadas acerca de los primos. Aquí están otras.

- ¿Hay un número infinito de primos de la forma n^2+1 (como $5, 17, 37, \ldots$)?
- ¿Es cierto que cada número par, mayor que 4, es la suma de dos primos impares (como $6 = 3+3$, $8 = 5+3$, $78 = 59+19, \ldots$)? Esto se conoce como *la conjetura de Goldbach.*
- ¿Es cierto que cada número impar, mayor que 7, se puede expresar como la suma de 3 primos impares (como $23 = 5 + 5 + 13, \ldots$)?

1.7 La demostración del Teorema Fundamental de la Aritmética

Si el Teorema no fuera cierto, existirán números que son productos de primos de más de una manera. Llamemos temporalmente a tales números *raros*, y sea n el mínimo número raro. Tenemos entonces dos factorizaciones distintas de n en primos,

$$n = p_1 p_2 p_3 \ldots = q_1 q_2 q_3 \ldots,$$

con $p_1 \leq p_2 \leq \ldots$, $q_1 \leq q_2 \leq \ldots$. De hecho, ninguno de los p's puede ser igual a ninguno de los q's, pues si P es un primo que aparece en las dos factorizaciones entonces n/P será un número raro menor que n, contradiciendo el hecho de que n fue escogido como el raro *mínimo*.

Ahora, como p_1 es el primo mínimo en la primera factorización, tenemos que $p_1^2 \leq n$ (ver la observación al final de la sección 1.2), y análogamente $q_1^2 \leq n$. Además, $p_1 \neq q_1$, así que $p_1 q_1 < n$, por lo que $N = n - p_1 q_1$ satisface $0 < N < n$, así que N no es raro.

Como $p_1|n$ y $q_1|n$, tenemos también que $p_1|N$ y $q_1|N$, así que ambos p_1 y q_1 aparecen en la factorización única de N, por lo que $p_1 q_1|N$. De $n = N + p_1 q_1$ tenemos que $p_1 q_1|n$, así que $q_1|(n/p_1)$. Pero $n/p_1 < n$, así que su factorización $p_2 p_3 \ldots$ es única y q_1 no aparece como ninguno de los factores, contradiciendo al hecho de que $q_1|(n/p_1)$. $\square$

En el siguiente capítulo (ejercicios 23- 25) vemos otra demostración a este teorema.

2 Congruencias

2.1 Definición de congruencias

Si un entero positivo m divide a la diferencia $a - b$ de dos números, decimos que "a es *congruente* a b modulo m", y lo escribimos

$$a \equiv b \pmod{m}.$$

Por ejemplo,

$$5 \equiv 9 \pmod{4}, \quad -8 \equiv 1 \pmod{9}, \quad 1997 \equiv 7 \pmod{10}.$$

Esta definición no introduce nada nuevo, porque "$a \equiv b \pmod{m}$" y "$m|(a-b)$" tienen exactamente el mismo significado; pero cada notación tiene su ventaja.

Notamos que en esta definición a y b no tienen que ser números positivos, y de hecho ni enteros, aunque nosotros no lo vamos a usar más que para números enteros.

Si $x \equiv a \pmod{m}$ decimos tambien que "a es un *residuo* de x" $\pmod{m}$. Si $0 \leq a \leq m-1$, llamamos a a el residuo *mínimo* (no-negativo) de x, módulo m. Así que dos números a y b son congruentes $\pmod{m}$ si tienen los mismos residuos $\pmod{m}$.

El residuo mínimo $\pmod{m}$ de un entero no-negativo x se puede determinar así: se divide x entre m, y lo que *sobra* es el residuo mínimo. Por ejemplo, el residuo mínimo de 100 $\pmod{7}$ es 2, porque al dividir 100 entre 7 el resultado es 14 (esto no importa) y sobran 2 (esto sí importa). El residuo mínimo de $-100 \pmod{7}$ es $7 - 2 = 5$. (¿Por qué?)

Una *clase de residuos* $\pmod{m}$ es la clase de todos los números congruentes a un número dado $\pmod{m}$. Por ejemplo, la clase de residuos de $3 \pmod{5}$ consiste de los números

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

y la clase de residuos de $0 \pmod{m}$ consiste de todos los múltiplos de m

$$\ldots, -3m, -2m, -m, \ 0, \ m, \ 2m, \ 3m, \ldots.$$

Cada miembro de una clase de residuos $\pmod m$ se llama un *representante* de la clase. Obviamente hay m clases de residuos $\pmod m$, representados por los residuos mínimos

$$0, 1, 2, 3, \ldots, m-1.$$

Las congruencias son de gran importancia práctica en la vida cotidiana. Por ejemplo, "hoy me levanté a las 6 de la mañana" es una afirmación acerca del número de horas que han pasado, módulo 24, desde algún tiempo fijo. La clase de residuos de este número de horas, o sea la hora del día, es normalmente mucho más importante que el número real de horas que han pasado desde, digamos, la creación del universo. Calendarios y horarios de camión o clases, son tablas de congruencias, módulo 7, 365 y 24.

2.2 Propiedades elementales de congruencias

Es fácil demostrar que congruencias módulo un entero positivo fijo m satisfacen las siguientes propiedades:

$$\begin{array}{lll} (i) & a \equiv b & \Longrightarrow \; b \equiv a, \\ (ii) & a \equiv b, b \equiv c & \Longrightarrow \; a \equiv c, \\ (iii) & a \equiv b & \Longrightarrow \; ka \equiv kb, \text{ para cualquier } k, \\ (iv) & a \equiv a\text{'}, b \equiv b\text{'} & \Longrightarrow \; a + b \equiv a\text{'} + b\text{'} \quad \text{y} \quad ab \equiv a\text{'}b\text{'}. \end{array}$$

Demostramos por ejemplo (iii). Si $a \equiv b$ entonces $m|(a-b)$ así que existe un l tal que $a - b = ml$. Así que $k(a-b) = ka - kb = mlk$, así que $m|ka - kb$, y obtenemos que $ka \equiv kb \pmod m$. Dejamos la demostración de las otras propiedades como un ejercicio.

Las propiedades (i) – (iv) son muy parecidas a las propiedades conocidas de las ecuaciones del álgebra ordinaria, pero de pronto encontramos una diferencia importante. En álgebra, tenemos también un converso a (iii). Es decir,

$$ka = kb \implies a = b, \quad \text{si } k \neq 0. \tag{6}$$

Pero con congruencias no es cierto. Por ejemplo

$$4 \cdot 5 \equiv 4 \cdot 3 \text{ y } 4 \not\equiv 0 \pmod 8, \tag{7}$$

pero

$$5 \not\equiv 3 \pmod 8.$$

Para entender lo que sí es cierto en esta dirección, revisamos primero la justificación usual de (6).

En álgebra ordinaria de números, si $k \neq 0$, entoces k tiene un *inverso*, o sea, existe un número, denotado por $1/k$, tal que $k \cdot (1/k) = 1$. Multiplicando los dos lados de la ecuación $ka = kb$ por $1/k$ (usando una regla tipo (iii)), obtenemos $(1/k) \cdot k \cdot a = (1/k) \cdot k \cdot b$, y por la propiedad del inverso, $k \cdot (1/k) = 1$, obtenemos $a = b$. De este argumento, aplicado a congruencias, obtenemos entonces el siguiente converso a (iii):

Teorema 11 *Si k es invertible $\pmod m$, entonces $ka \equiv kb \pmod m$ implica $a \equiv b$.*

Ahora podemos entender mejor el problema con el ejemplo de (7). El problema surgió del hecho que 4 no tiene inverso modulo 8; o sea, no existe un número x que satisface $4x \equiv 1 \pmod 8$.

La siguiente pregunta, entonces, es fundamental para trabajar con congruencias:

¿Que residuos, modulo m, tienen inverso?

o dicho de otra manera, ¿para cuáles k la congruencia $kx \equiv 1 \pmod m$ tiene una solución x?

La respuesta esta dada por

Teorema 12 *Los residuos invertibles $\pmod m$ son los residuos que son primos relativos a m; o sea los residuos que no tienen un divisor común con m mayor que 1.*

Por ejemplo, segun el teorema, de los 8 residuos mínimos $\pmod 8$, hay 4 que son invertibles (los impares), y 4 que no son invertibles (los pares). En particular, 4 no es invertible, como ya vimos.

Demostración. Suponemos que k es invertible $\pmod m$ y d es un divisor común de m y k. Entonces $k = da$ y $m = db$ para algunos enteros a y b, donde $1 \leq b \leq m$. Ahora $kb = dab = ma \equiv 0 \pmod m$, así que si k es invertible, obtenemos, segun el Teorema 11, que $b \equiv 0$; pero esto es posible, por la condición $1 \leq b \leq m$, solamente si $b = m$, así que $d = 1$.

Para el converso, suponemos que k y m no tienen un divisor común mayor que 1, y consideramos los $m-1$ números

$$k, 2k, 3k, \ldots, (m-1)k.$$

Demostramos que alguno de estos números es congruente a $1 \pmod{m}$. Para eso, es suficiente ver que estos $m-1$ números representan $m-1$ clases de congruencias *distintas.* Si dos de estos números son congruentes, digamos $ka \equiv kb \pmod{m}$, $1 \leq a < b \leq m-1$, tenemos que m divide a la diferencia $kb - ka = k(b-a)$. Ahora como m no tiene factor común con k, $m|k(b-a) \Longrightarrow m|(b-a)$ (usando el Teorema Fundamental). Pero esto es imposible porque $1 \leq b-a \leq m-1$. □

Un caso particular, pero importante, del último teorema es

Teorema 13 *Si p es un primo, entonces a es invertible $(\text{mod } p)$ para todo $a \not\equiv 0$.*

Por este Teorema, y la discución al principio de esta sección, tenemos que la álgebra módulo un primo p se parece, en sus aspectos formal, a la álgebra ordinaria. En la siguiente sección ilustramos el uso de este "principio", en la demostración de un teorema de los más famosos de la teoría de números.

Ejercicios Adicionales.

Ejercicio 23 *Aquí vemos otro método para demostrar el último teorema, y que no depende del Teorema Fundamental del Aritmética (de hecho, como se puede ver en los proximo dos ejercicio, se puede usar este método para* demostrar *el Teorema Fundamental del Aritmética). Además, el método es útil para* encontrar *la inversa de un entero modulo un primo.*

a) Sea p un primo y a un entero, $0 < a < p$. Entre todos los números $2a, 3a, 4a, \ldots$etc (los múltiplos de a) escojemos el primero, digamos ma, que sea mayor que p. Demuestra que $a_1 = m_1 a - p$ satiface $a > a_1 > 0$.

b) Ahora si $a_1 = 1$ acabamos, porque entonces $m_1 a \equiv 1 \pmod{p}$, y si no, seguimos lo mismo con a_1. Es decir, encontramos el primer múltiplo de a_1, digamos $m_1 a_1$, que sea mayor que p, tomamos $a_2 = m_2 a_1 - p$, y tenemos $a > a_1 > a_2 > 0$. Así seguimos hasta que en algun momento llegamos a $a > a_1 > a_2 > \ldots > a_k = 1$. Demuestra que $m = m_1 m_2 m_3 \ldots$ es el inverso $(\text{mod } p)$ de a.

c) Aplica el método para encontrar el inverso de $8 \pmod{101}$.

d) Demuestra que este método también funciona para encontrar el recíproco de un entero a mudulo otro entero n, aún cuando n no es necesariamente un primo, mientras $(a, n) = 1$. De esta manera obtenemos también una demostración alternativa al Teorema 12.

e) Encuentra el inverso de 3 modulo 1000.

g) Consideramos la sucesíon de las potencias positivas de 3, es decir la sucesión de los números $3, 9, 27, 81, \ldots$ etc. ¿Existe entre estos números uno cuyos últimos 3 dígitos son 001?

(Sugerencia: primero demuestra que esto es equivalente al tener un entero x tal que $3^x \equiv 1 \pmod{100}$. Toma 101 números distintos de la lista; por ejemplo, los priemros 101 números: $3, 9, 27, 81, \ldots, 3^{101}$. Los resíduos $\pmod{100}$ es un conjunto de 101 números entre 0 y 99. Concluye que dos de estos números tienen el mismo resíduo, es decir $3^a \equiv 3^b \pmod{100}$, y digamos $a > b$. Multiplica b veces los dos lados de la última congruencia por el inverso de 3 modulo 100 y concluye que el número $x = a - b$ tiene la propiedad que los últimos 3 dígitos de 3^x son 001.)

Ejercicio 24 *Demuestra, usando el ejercicio anterior, que si un primo p divide a un producto de enteros $n = abc...$ entonces tiene que dividir a uno de los factores $a, b, c, ...$ (es el Teorema 6).*

(Sugerencia: si p no divide a ninguno de los factores entonces todos tendrán inversos $\pmod{p}$, digamos $1/a, 1/b, ...$, y el producto $(1/a)(1/b)...$ será un inverso de $n \pmod{p}$, a cual es imposible para un entero divisible por p.)

Ejercicio 25 *Demuestra, usando el ejercicio anterior, el Teorema Fundamental del Aritmética.*

Ejercicio 26 *¿Existe un entero k tal que $k^2 = 111111111111111998$?*

(Sugerencia: demuestra que el cuadrado de cualquier entero es congruente a 0,1, o 4 modulo 8).

Ejercicio 27 *Demuestra que cualquier primo p divide a $(p-1)! + 1$.*

2.3 El pequeño teorema de Fermat

Teorema 14 *Si p es un primo, entonces $a^p \equiv a \pmod{p}$, para todo entero a.*

Este teorema fue anunciado por Fermat en 1640 y demostrado por primera vez por Euler en 1736. El "gran" teorema de Fermat (o "último" teorema) afirma que la ecuación $x^n + y^n = z^n$ no tiene soluciones con enteros positivos para $n > 2$. Su demostración se llevó acabo, despues de grandes esfuerzos de muchos matemáticos, por el matemático inglés Andrew Wiles (1954–) en 1994.

Demostración. Para $a \equiv 0 \pmod p$ el teorema es obvio. Suponemos entonces que $a \not\equiv 0$. En este caso, usando que p es primo, sabemos que a es invertible $\pmod p$, así que los residuos mínimos de sus $p-1$ múltiplos

$$a, 2a, 3a, \ldots, (p-1)a$$

son todos distintos, y distintos de cero, así que deben constituir a *todos* los $p-1$ residuos mínimos $1, 2, \ldots, p-1$. Así obtenemos

$$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod p,$$

así que

$$a^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod p;$$

pero $1 \cdot 2 \cdot \ldots \cdot (p-1) \not\equiv 0 \pmod p$, así que

$$a^{p-1} \equiv 1 \pmod p.$$

□

El principio combinatorio usado en la última demostración se llama el "principio de la palomera": si N palomas se instalan en una palomera con N sitios, y en cada sitio no cabe más que una paloma, entonces todos los sitios tienen que estar ocupados (a veces se afirma esto en una forma equivalente: si N palomas se instalan en una palomera con n sitios, y $n < N$, entonces hay por lo menos un sitio ocupado por más de una paloma). Este principio, tan "obvio" al parecer, es de gran utilidad en nuestra teoría. En la última demostración las "palomas" eran los números $a, 2a, 3a, \ldots, (p-1)a$ y la "palomera" el sistema de residuos mínimos distintos de cero $\pmod p$. Otro lugar en donde hemos usado este principio fue en la demostración del Teorema 12.

Ejercicios Adicionales.

Ejercicio 28 *En este ejercicio vemos una aplicación geométrica para la resolución de un problema muy clásico, el problema de la determinación de todos los tríples pitagóricos (todos los triángulos rectangulos con lados enteros). En otras palabras, estamos buscando a todas los triples de enteros* (a, b, c) *que satisfacen* $a^2 + b^2 = c^2$ *(es cómodo admitir tambíen enteros no positivos, pero excluir el tríple* $(0, 0, 0)$*). Por ejemplo 3,4,5 es un tríple pitagórico. El método que usamos se llama "el método de secantes de Diofantus" (un matemático griego del siglo 3 AC).*

a) Demuestra que si (a, b, c) *es un tríple pitagórico entonces* (da, db, dc) *es también un tríple pitagórico, para todo entero d.*

A dos triples relacionados de esta manera llamamos "proporcionales".

b) Demuestra que todo tríple pitagórico (excluyendo a $(0, 0, 0)$*) es proporcional a un solo tríple* (a, b, c) *sin divisor comun mayor que* 1.

c) A cada tríple pitagórico (a, b, c)*, sin divisor comun mayor que* 1 *y* $c > 0$*, asociamos el punto en el plano con coordenadas* $(a/c, b/c)$*. Por ejemplo al tríple 3,4,5 asociamos el punto* $(3/5, 4/5)$*. Demuestra que de esta manera obtenemos una correspondencia biyectiva entre los triples pitagóricos* (a, b, c) *con* $(a, b, c) = 1$ *y* $c > 0$ *y puntos sobre el círculo unitario* $x^2 + y^2 = 1$ *con coordenadas racionales, i.e. puntos* (x, y) *con* x, y *números racionales (fracciones).*

d)Ahora tomamos una linea en el plano con la ecuación $y = mx + b$*. Suponemos que esta linea intersecta al círculo* $x^2 + y^2 = 1$ *en dos puntos (tal linea se llama un secante del círculo) . Además, suponemos que la pendiente m de la linea es un número racional y uno de los puntos de intersección de la linea con el círculo tiene coordenadas racional. Demuestra que entonces el otro punto de interseccion también tiene coordenadas racionales.*

e) Ahora consideramos una linea que pasa por el punto $(-1, 0)$*. Demuestra que cuando el pendiente m de esta linea varía entre todos los números racionales, su segundo punto de intersección (distinto de* $(-1, 0)$*) varía entre todos los puntos del círculo con coordenadas racionales (excepto* $(-1, 0)$*).*

f) Escribe el pendiente $m = r/s$ *y expresa el tríple pitagórico correspondiente* (a, b, c) *en terminos de r y s.*

g) Usa la fórmula obtenida para producir todos los triples pitagóricos distintos (a,b,c), con $0 < a, b, c < 30$.

h) Encuentra todas las soluciones en números enteros de la ecuación $x^2 + xy + 5y^2 + 11yz = z^2$.