Revista

de

Matemáticas Elementales

VOLUMEN I. Octubre de 1952 FASCICULO 2-3

Tarifa Postal Reducida — Licencia Número 1993 del Ministerio de Correos y Telégrafos.

NUMEROS PRIMOS I.

por

J. Horváth.

1. Esta serie de artículos tratará de los números enteros que son: los números enteros positivos:

$$1, 2, 3, 4, 5, 6, \ldots,$$

el número cero: 0,

y los números enteros negativos:

$$-1, -2, -3, -4, -5, -6, \ldots$$

Estos números son conocidos, generalmente, por toda la gente; cada uno tiene una idea intuitiva de ellos y sabe manejarlos con más o menos habilidad. Lo que no se sabe, tan generalmente, es que estos números se pueden definir, sin que intervenga la intuición, con el sistema de cinco axiomas que llevan el nombre del gran matemático italiano Peano. La definición rigurosa de los números enteros será objeto de otro artículo de esta Revista; el lector interesado puede consultar el libro de E. Landau: Foundations of Analysis, Nueva York 1951. Aquí nos limitamos a enumerar las propiedades de los números enteros que utilizaremos en estos artículos. Estas propiedades se pueden demostrar todas rigurosamente a partir de los axiomas de Peano. *En esta serie de artículos denotaremos los enteros con letras minúsculas latinas (eventualmente con subíndice) como* $a, b, c, m, n, x, y, z, a_1, a_k$, *etc.*

Entre números enteros hay una operación, que se llama la **adición**, que hace corresponder a dos números enteros a y b, el número entero $a+b$, llamado la suma de a y de b; a y b se llaman los términos de la suma $a+b$. Esta operación tiene las propiedades siguientes:

$$(a+b)+c=a+(b+c) \qquad \text{(propiedad asociativa)},$$
$$a+b=b+a \qquad \text{(propiedad conmutativa)},$$
$$0+a=a, \qquad a+(-a)=0,$$
$$\text{si } a+b=a+c, \text{ entonces } b=c.$$

Por la propiedad asociativa se pueden quitar los paréntesis en una expresión de la forma $(((8+5)+3)+7)+2$ y se puede escribir la suma de más de dos términos $8+5+3+7+2$. La propiedad conmutativa subsiste para sumas de varios términos, por ejemplo:

$$8+5+3+7+2=5+7+8+2+3=3+8+2+7+5 = \text{etc.}$$

La operación de la adición tiene una operación inversa, la **sustracción**. Se dice que x es la diferencia de a y de b, y se escribe $x=a-b$, si $x+b=a$. Valen las reglas siguientes:

$$a+(-b)=a-b \quad \text{y} \quad a+(-a)=a-a=0.$$

La otra operación definida entre números enteros es la **multiplicación**, que hace corresponder a dos números enteros a y b, el número entero ab (o $a.b$ o $a\times b$), llamado el producto de a y de b; a y b se llaman los factores del producto ab. La multiplicación tiene las propiedades siguientes:

$$(ab)c=a(bc) \qquad \text{(propiedad asociativa)},$$
$$ab=ba \qquad \text{(propiedad conmutativa)},$$
$$1.a=a, \quad 0.a=0, \quad (-1).a=-a,$$
$$\text{si } ab=ac \text{ y } a\neq 0, \text{ entonces } b=c.$$

Por la propiedad asociativa se pueden quitar los paréntesis en una expresión de la forma $(((8\times 5)\times 3)\times 7)\times 2$ y se puede escribir el producto de más de dos factores $8\times 5\times 3\times 7\times 2$. La propiedad conmutativa subsiste para productos de varios factores, por ejemplo: $8\times 5\times 3\times 7\times 2 = 5\times 7\times 8\times 2\times 3 = 3\times 8\times 2\times 7\times 5 = \text{etc.}$

La adición y la multiplicación están vinculadas por la propiedad distributiva:

$$a(b + c) = ab + ac.$$

El **orden** entre números enteros se define de la manera siguiente: *a es menor que b, si existe un número* positivo *x tal que* $a + x = b$; *en este caso se escribe* $a < b$. Si $a < b$, entonces b es mayor que a, lo que escribiremos así: $b > a$. Si a es menor o igual a b, escribiremos $a \leqslant b$ o $b \geqslant a$ (el segundo se lee: b es mayor o igual a a). Los números positivos son los números mayores que cero y los números negativos son los números menores que cero. El orden tiene las propiedades siguientes:

si $a \leqslant b$ y $b \leqslant a$, entonces $a = b$;
si $a \leqslant b$ y $b \leqslant c$, entonces $a \leqslant c$;
si $a \leqslant b$, entonces $a < b + 1$ y $a - 1 < b$;
si $a \leqslant b$ y $b < c$, entonces $a < c$;
si $a < b$ y $b \leqslant c$, entonces $a < c$;
si $a \leqslant b$ y $c \leqslant d$, entonces $a + c \leqslant b + d$;
si $a < b$ y $c \leqslant d$, entonces $a + c < b + d$;
si $a \leqslant b$ y $c \geqslant 0$, entonces $ac \leqslant bc$;
si $a < b$ y $c > 0$, entonces $ac < bc$;
si $a \leqslant b$ y $c \leqslant 0$, entonces $ac \geqslant bc$;
si $ac \leqslant bc$ y $c > 0$, entonces $a \leqslant b$;
si $ac \leqslant bc$ y $c < 0$, entonces $a \geqslant b$.

El **valor absoluto** $|a|$ de un número a se define de la manera siguiente:

$$|a| = a, \text{ si } a \geqslant 0,$$

$$|a| = -a, \text{ si } a < 0.$$

Por ejemplo $|-6| = 6$, $|3| = 3$, $|0| = 0$. Siempre $|a + b| \leqslant |a| + |b|$ y $|ab| = |a| \cdot |b|$. Se dice que a es inferior a b en valor absoluto, si $|a| < |b|$.

Si tenemos una colección, o como se llama en las matemáticas avanzadas, un *"conjunto"* de números enteros, diremos que este conjunto es acotado por debajo, si existe un número entero que es menor que todos los números del conjunto. Por ejemplo, un conjunto cualquiera de números positivos es acotado por debajo, puesto

que cero es menor que cada número positivo; es claro que cada conjunto finito de números enteros es acotado por debajo; el conjunto de los números negativos *no* es acotado por debajo.

PROPIEDAD A. *En cada conjunto de números enteros, acotado por debajo, existe un número que es menor que todos los otros números del conjunto.*

Esta propiedad de los números enteros, tan sencilla, tiene un papel importantísimo en la demostración de teoremas sobre números enteros, como lo veremos más adelante. En oposición piense (y demuestre!) el lector que los números racionales y los números reales no tienen esta propiedad, pues no existe, por ejemplo, un número racional (o real) positivo inferior a todos los otros números racionales (o reales) positivos.

De manera análoga un conjunto de números enteros se llama acotado por encima si existe un número entero que es mayor que todos los números del conjunto.

PROPIEDAD B. *En cada conjunto de números enteros, acotado por encima, existe un número que es mayor que todos los otros números del conjunto.*

Finalmente hay que explicar el **"principio de la inducción completa"** que también es un instrumento importante para demostrar teoremas sobre números enteros. *Supongamos que* P_n *sea una afirmación que depende del número entero positivo* n.

1. *Si* P_1 *es cierto;*

2. *si suponiendo que* P_n *es cierto para valores* $1 \leqslant n \leqslant m$ *se puede demostrar que* P_{m+1} *es cierto;*

entonces P_n *es cierto para cada valor entero positivo de* n.

Demos inmediatamente un ejemplo. Sea P_n la afirmación: "La suma S_n de la progresión geométrica $1 + q + q^2 + \ldots + q^n$ es igual a $\dfrac{q^{n+1} - 1}{q - 1}$".

1. $S_1 = 1 + q = \dfrac{(1+q)\,(q-1)}{q-1} = \dfrac{q^2 - 1}{q - 1}$

2. Supongamos que para $1 \leqslant n \leqslant m$ sea

$$S_n = 1 + q + q^2 + \ldots + q^n = \frac{q^{n+1} - 1}{q - 1}$$

(en realidad utilizaremos la relación sólo para $n = m$). Entonces

$$S_{m+1} = 1 + q + q^2 + \ldots + q^{m+1} = S_m + q^{m+1}$$

$$= \frac{q^{m+1} - 1}{q-1} + q^{m+1} = \frac{q^{m+1} - 1 + q^{m+1}(q-1)}{q-1}$$

$$= \frac{q^{m+1} - 1 + q^{m+2} - q^{m+1}}{q-1} = \frac{q^{m+2} - 1}{q-1}$$

es decir la afirmación es válida para $m + 1$. Entonces tenemos

$$S_n = 1 + q + q^2 + \ldots + q^n = \frac{q^{n+1} - 1}{q-1},$$

para cada n entero positivo.

Observemos que el principio de inducción completa, en una forma ligeramente diferente de la dada aquí, es uno de los cinco axiomas de PEANO.

Ejercicio: Demostrar, por inducción completa, que la suma de la progresión aritmética $a + (a + d) + (a + 2d) + \ldots + (a + nd)$ es igual a $\frac{n+1}{2}(2a + nd)$.

2. Fijadas estas nociones preliminares, vamos a definir el concepto básico de este artículo: la **divisibilidad.** *Se dice que el número entero* a *es divisible por el número entero* b, *si existe un número entero* q *tal que* $a = bq$. Por ejemplo 15 es divisible por 3, puesto que $15 = 3 \times 5$; -60 es divisible por 12, puesto que $-60 = 12 \times (-5)$. Si a es divisible por b, diremos también que b divide a a (sin residuo), que b es divisor de a, o que a es un múltiplo de b. Con otras palabras, se puede decir que a es divisible por b, si el número $q = \frac{a}{b}$ es entero. Es cómodo introducir la notación siguiente: si b divide a, escribimos $b|a$. Así por ejemplo $2|6$, $5|15$, $2|-8$, $-3|9$, $-5|-20$.

Demos ahora algunas proposiciones sencillas sobre la divisibilidad:

1. Para cada número entero a se tiene que $a|a$. (Cada número entero es divisor de sí mismo).

Demostración. $a = a.1$.

2. Para cada número entero b se tiene que $b|0$. (Cero es divisible por cada número entero).

Demostración. $0 = b.0$.

Las demostraciones de las siguientes proposiciones, igualmente fáciles, las dejamos al lector como ejercicios, rogándole enviarlas a esta Revista. En una entrega siguiente daremos la lista de los lectores que han presentado demostraciones correctas.

3. El único número entero divisible por cero es cero.
4. Cada número entero es divisible por $+1$ y por -1.
5. Los únicos divisores de $+1$ (y de -1) son $+1$ y -1.
6. Si $c|b$ y $b|a$, entonces $c|a$.
7. Si $b|a$, entonces para cada número entero c se tiene que $cb|ca$.
8. Si $cb|ca$ y si c es diferente de cero, entonces $b|a$.
9. Si $b_1|a_1$ y $b_2|a_2$, entonces $b_1b_2|a_1a_2$.
10. Si $b|a_1$ y $b|a_2$, entonces $b|a_1 + a_2$ y $b|a_1 - a_2$.
11. Si $b|a$, entonces para cada número entero c se tiene que $b|ac$.
12. Si $b|a_1$ y $b|a_2$, entonces $b|c_1a_1 + c_2a_2$, para números enteros c_1 y c_2 cualesquiera.
13. Si $b|a$ y $a|b$, entonces $b = \pm a$.
14. Si $b|a$, entonces $-b|a$, $b|-a$, $-b|-a$, $|b|\,||a|$.
15. Si a es diferente de cero ($a \neq 0$) y $b|a$, entonces $|b| \leqslant |a|$.

Demostración. De $a = bq$ se sigue, siendo $|q| \geqslant 1$, que $|a| = |b| \,.\, |q| \geqslant |b| \,.\, 1 = |b|$.

El teorema siguiente expresa una de las propiedades más fundamentales de los números enteros.

TEOREMA DE LA DIVISIÓN CON RESIDUO. *Si* a *es un número entero cualquiera y* b *es un número entero positivo, siempre existe un número entero* q *y un número entero* r *que verifican las relaciones*

$$a = bq + r, \qquad 0 \leqslant r < b.$$

Estas relaciones determinan q *y* r *unívocamente*, es decir si $a = bq' + r'$ y $0 \leqslant r' < b$, entonces necesariamente $q' = q$ y $r' = r$. El número q se llama el cociente (incompleto) y el número r se llama el residuo de la división de a por b. Así por ejemplo si $a = -17$ y $b = 5$, $q = -4$ y $r = 3$, puesto que $-17 = 5 \times (-4) + 3$ y $0 \leqslant 3 < 5$. Con esta terminología se puede decir que a es divisible por b si el residuo es cero.

La demostración de este teorema es basada sobre la propiedad A. de los números enteros y es tan fundamental como el teorema mismo, pues la idea que utiliza se encuentra en muchas partes de las

matemáticas (por ejemplo en la Teoría de los Números), y es sumamente importante que el lector se familiarice con ella y que la comprenda a fondo.

Consideremos todos los números de la forma $a - bu$, donde u es un número entero cualquiera, es decir, donde u toma los valores $u = 0, \pm 1, \pm 2, \ldots$ Con otras palabras, consideramos el conjunto de números de la forma $a - bu$, donde $u = 0, \pm 1, \pm 2, \ldots$ En este conjunto hay números positivos, por ejemplo cuando u es un número negativo de valor absoluto muy grande, y hay también números negativos, por ejemplo para valores muy grandes de u. Por **A.** hay entre los números no negativos de la forma $a - bu$ uno que es inferior a todos los otros, sea este $a - bq$. Con otras palabras, la expresión $a - bu$ toma su valor no negativo más pequeño para $u = q$. Pongamos entonces $r = a - bq$, o $a = bq + r$. Por la definición de $r = a - bq$ (como el número más pequeño *no negativo* de la forma $a - bu$) es cierto que $r \geqslant 0$. Por otra parte, como $a - b(q + 1) < a - bq$, se sigue de la definición de $a - bq$ que $r - b = a - b(q + 1) < 0$. Entonces $0 \leqslant r < b$.

Queda para demostrar la unicidad. Como r es definida por $r = a - bq$, es suficiente demostrar que el único número de la forma $a - bu$ que satisface a $0 \leqslant a - bu < b$ es precisamente $a - bq$. En efecto si $u < q$, es decir si $u \leqslant q - 1$, entonces

$$a - bu \geqslant a - b(q-1) = a - bq + b = r + b \geqslant b.$$

Si $u > q$, es decir si $u \geqslant q + 1$, entonces

$$a - bu \leqslant a - b(q + 1) = a - bq - b = r - b < 0.$$

El teorema queda pues completamente demostrado.

Sean a y b dos números enteros y supongamos que no sean ambos iguales a cero. Es cierto que hay por lo menos un número positivo que es divisor común de a y de b, que es el número 1 (por la propiedad 4.). Por otro lado, como supusimos que uno de los números es diferente de cero, por ejemplo que $a \neq 0$, cada divisor de a, y por lo tanto cada divisor común de a y de b, es inferior en valor absoluto a $|a|$ (cf. teorema 15.). Así, por la propiedad **B.** de los números enteros, existe un divisor común de a y de b, que es más grande que todos los otros. Este divisor común, que es necesariamente positivo porque ya es superior o igual a 1, se llama el **máximo común divisor** de los números enteros a y b. Vamos a emplear la notación (a,b)

para el máximo común divisor de los números enteros a, b, donde, repetimos, uno de los dos tiene que ser diferente de cero (por qué?). Ejemplos: $(8, 12) = 4$, $(-27, 15) = 3$, $(-77, -44) = 11$. El máximo común divisor tiene las dos propiedades evidentes:

$$(a, b) = (b, a), \text{ y para } a \neq 0, (a, 0) = |a|.$$

Sean ahora a y b dos números enteros, ambos diferentes de cero ($a \neq 0$, $b \neq 0$). Se puede afirmar que existen números positivos que son múltiplos de ambos, por ejemplo el número $|a| \cdot |b|$. Por la propiedad **A.** de los números enteros, existe pues un múltiplo común positivo de a y de b que es inferior a todos los otros. Este múltiplo común (que es positivo por la definición misma) se llama el **mínimo común múltiplo** de los números enteros a, b. Vamos a emplear la notación $[a, b]$ para el mínimo común múltiplo de los números enteros a, b ($a \neq 0$, $b \neq 0$). Ejemplos $[4, 6] = 12$, $[-21, 28] = 84$, $[-10, -15] = 30$. El mínimo común múltiplo tiene las dos propiedades evidentes: $[a, b] = [b, a]$, y para cada $a \neq 0$, $[a, \pm 1] = 1$.

Los lemas (teoremas auxiliares) siguientes expresan propiedades del máximo común divisor y del mínimo común múltiplo.

LEMA 1. *Sean* a *y* b *dos números enteros diferentes de* cero *y sea* m = [a, b]. *Si* n *es un múltiplo de* a *y de* b, *entonces* n *es también múltiplo de* m.

Demostración. Por el teorema de la división con residuo existen números enteros q y r tales que $n = mq + r$, $0 \leqslant r < m$. Por otro lado como $r = n - qm$ y como $a|n$, $a|m$, $b|n$, $b|m$, resulta por la regla 12. de la divisibilidad que $a|r$ y $b|r$ es decir que r es múltiplo común de a y de b. Como $0 \leqslant r < m$, la definición de m implica que $r = 0$, luego que $n = mq$ y $m|n$.

LEMA 2. *Sean* a *y* b *dos números enteros diferentes de* cero, *sea* d = (a, b) *y* m = [a, b]. *Entonces* (i) dm = |ab|, (ii) *cada divisor común* f *de* a *y de* b *divide* d (*es decir de* f|a, f|b *sigue* f|d).

Demostración. Como ab es múltiplo común de a y de b, por el lema 1, el número $g = \frac{|ab|}{m}$ es entero. De manera evidente basta demostrar que:

$$(\alpha) \text{ si } f|a, f|b, \text{ entonces } f|g,$$

$$(\beta)\ g = d.$$

Si $f|a$ y $f|b$, entonces por las proposiciones 1., 11. y 14. $a|\,|a|\,\frac{|b|}{f}$ y $b|\,|b|\frac{|a|}{f}$, es decir $\frac{|ab|}{f}$ es múltiplo común de los números a y b. Entonces por el lema 1. $m|\frac{|ab|}{f}$, es decir $\frac{|ab|}{g}\,\Big|\,\frac{|ab|}{f}$. Así el cociente $\frac{|ab|}{f} : \frac{|ab|}{g} = \frac{g}{f}$ es un número entero, o sea $f|g$. Esto demuestra (α).

Como los números $\frac{|a|}{g} = \frac{m}{|b|}$ y $\frac{|b|}{g} = \frac{m}{|a|}$ son enteros (porque $b|m$ y $a|m$), $g|a$ y $g|b$. Por (α) cada divisor común f de a y de b divide también a g, entonces por la proposición 15. $|f| \leqslant g$; es decir g es igual al máximo común divisor $d = (a, b)$. Este demuestra completamente el teorema.

Observemos que las fracciones escritas en esta demostración son en realidad números enteros. Los hemos escrito en forma de fracciones para que no sea necesario introducir demasiadas letras. Esta observación es también válida para los lemas siguientes.

Si $(a, b) = 1$, es decir si 1 es el único divisor común positivo de a y de b, se dice que a y b son primos relativos. Por ejemplo 14 y 15 son primos relativos, ya que los divisores positivos de 14 son 1, 2, 7, 14 y los de 15 son 1, 3, 5, 15.

LEMA 3. *Si* $(a, b) = d$, *entonces* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demostración. Si $f > 0$, $f|\,\frac{a}{d}$ y $f|\,\frac{b}{d}$ entonces por la proposición 7. $fd|a$ y $fd|b$. Por la afirmación (ii) del lema precedente $fd|d$, entonces por las proposiciones 8. y 5. y puesto que $f > 0$, resulta $f = 1$. Entonces el máximo (y único) divisor común positivo de $\frac{a}{d}$ y de $\frac{b}{d}$ es 1.

LEMA 4. *Si* $c > 0$, $c|a$, $c|b$, $\left(\frac{a}{c}, \frac{b}{c}\right) = 1$, *entonces* $(a, b) = c$.

Demostración. Sea $d = (a, b)$. (Como $\frac{a}{c}$ y $\frac{b}{c}$ no son ambos iguales a cero, a y b tampoco no son ambos iguales a cero. Así te-

nemos el derecho de hablar de (a, b) .) Por *Lema* 2, (ii) $c|d$, es decir $\frac{d}{c}$ es un número entero. De $\frac{d}{c} \cdot \frac{a}{d} = \frac{a}{c}$ y de $\frac{d}{c} \cdot \frac{b}{d} = \frac{b}{c}$ sigue que $\frac{d}{c} \left| \frac{a}{c} \right.$ y $\frac{d}{c} \left| \frac{b}{c} \right.$, y como $\left(\frac{a}{c}, \frac{b}{c}\right) = 1, c > 0,$ $d > 0$, sigue que $\frac{d}{c} = 1$ o sea que $d = c$. Esto muestra que en efecto $c = (a, b)$.

El teorema siguiente es de una importancia capital.

LEMA DE EUCLIDES. *Sea* $a \neq 0$. *Si* $(a, b) = 1$ *y* $a|bc$, *entonces* $a|c$.

Demostración. Si $b = 0$, entonces $|a| = (a, 0) = 1$, $a = \pm 1$ y $a|c$.

Si $b \neq 0$, sea $m = [|a|, |b|]$, por $(a, b) = 1$ y el lema 2, (i) $|a| \cdot |b| = m$. Como bc es múltiplo común de a y de b, por el lema 1. $|a| \cdot |b| \mid bc$. Por la proposición 14. $ab|bc$, y finalmente por la proposición 8. $a|c$.

La hipótesis que a y b sean primos relativos es esencial en este último lema. Por ejemplo 6 divide a $9 \times 4 = 36$, pero 6 no es divisor ni de 9, ni de 4.

3. Un número entero p superior a 1 que no tiene otros divisores positivos que 1 y p se llama **número primo.** Los primeros números primos son 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, ...

Un número n que tiene otros divisores a más de ± 1 y $\pm n$, se llama un número **compuesto.** Por ejemplo los números $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, ... son todos compuestos. Vemos que hay un número infinito de números compuestos. El problema de determinar si hay también un número infinito de números primos y ver cómo se reparten los números primos entre los números enteros positivos, será el tema de otros artículos de esta serie; ahora nos ocupamos de investigar cómo se pueden descomponer los números compuestos en números primos, los cuáles son, en un sentido, los ladrillos con que son edificados todos los números positivos. Hasta nueva indicación vamos a considerar únicamente números enteros *positivos.*

Cada número entero compuesto es un producto de números primos. Por ejemplo $14.490 = 2 \times 3 \times 3 \times 5 \times 7 \times 23$. La demostración de este teorema se hace por inducción completa. Es claro que el teorema se puede enunciar de la manera siguiente: Un número entero $n > 1$ o es un número primo, o es un producto de números primos. El teorema es válido para $n = 1$, como para este caso no hay ninguna afirmación; se dice que para $n = 1$ el teorema se cumple "trivialmente". Supongamos ahora que el teorema sea válido para $n = 1, 2, \ldots, m - 1$. Si m es un número primo no hay nada que demostrar. Si m no es primo, entonces tiene un divisor $m_1, 1 < m_1 < m$ y luego $m = m_1 m_2$, donde también $1 < m_2 < m$. Por la hipótesis de inducción, según la cuál cada entero entre 1 y $m - 1$ es primo o producto de primos, $m_1 = p_1 p_2 \ldots p_k$, $m_2 = p_{k+1} p_{k+2} \ldots p_l$, donde los números $p_1, \ldots, p_l$ son todos primos $(1 \leqslant k < l)$. Así $m = p_1 p_2 \ldots p_l$, lo que demuestra completamente el teorema.

Sea p un número primo y a un número entero positivo. Si $p|a$ entonces $(p, a) = p$. Si p no divide a a, entonces $(p, a) = 1$, como es imposible que p tenga divisor positivo diferente de 1 y de p. El lema de EUCLIDES tiene pues el corolario siguiente: Si el número primo p divide al producto bc donde b y c son números enteros, y si p no divide a b (con otras palabras, si $(p, b) = 1$) entonces $p|c$. Más generalmente demostraremos el teorema siguiente:

Si el número primo p *divide al producto* $a_1 a_2 \ldots a_n$, *donde* $a_1, a_2, \ldots, a_n$ *son números positivos, entonces* p *divide por lo menos uno de los números* $a_1, a_2, \ldots, a_n$. Haremos la demostración por inducción completa según el número n de los factores $a_1, a_2, \ldots, a_n$. Si $n = 1$, la proposición se reduce a la tautología: si $p|a$, entonces $p|a$. Supongamos, pues, que el teorema sea válido para $n = 1, 2, \ldots, m - 1$. Si $p|a_1 a_2 \ldots, a_m$, entonces o bien $p|a_1$ en cuyo caso no hay nada que demostrar, o bien p no divide a a_1. En este último caso, por el corolario del lema de EUCLIDES $p|a_2 \ldots a_m$. Como el producto tiene $m - 1$ factores, por la hipótesis de inducción, p divide por lo menos uno de los factores $a_2, \ldots, a_m$, lo que demuestra completamente el teorema.

En particular si $p, p_1, p_2, \ldots, p_n$ son números primos y $p|p_1 p_2 \ldots p_n$, entonces p es igual a uno de los números $p_1, \ldots, p_n$ (porque si un número primo divide a otro número primo, son necesariamente iguales).

Tenemos ahora todo listo para demostrar el teorema que se llama **"el teorema fundamental de la aritmética"**. Este teorema dice

que *la descomposición de un número entero* $n > 1$ *en factores primos* $n = p_1 p_2 \dots p_k$ *es única.* Es decir que si tenemos $n = p_1 p_2 \dots p_k$ y $n = q_1 q_2 \dots q_l$, donde $p_1, p_2, \dots, p_k, q_1, q_2, \dots q_l$ son todos números primos, entonces $k = l$ y los $p_1, p_2, \dots, p_k$ son los mismos que los $q_1, q_2, \dots, q_l$ sólo quizás en otro orden de escritura. Por ejemplo $1540 = 2 \times 2 \times 5 \times 7 \times 11 = 11 \times 2 \times 2 \times 7 \times 5 = 2 \times 7 \times 5 \times 2 \times 11 =$ etc.

Haremos la demostración por inducción completa según el número n. Para $n = 1$ no hay nada que demostrar. Supongamos que el teorema sea válido para $n = 1, 2, \dots, m - 1$. Sea

$$m = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l.$$

Como $p_1 | q_1 q_2 \dots q_l$, por el teorema precedente p_1 es igual a uno entre los números $q_1, q_2, \dots, q_l$ y (reordenando eventualmente los $q_1, q_2, \dots, q_l$) podemos suponer que $p_1 = q_1$. Entonces

$$p_2 p_3 \dots p_k = q_2 q_3 \dots q_l$$

y como este número es inferior a m, por la hipótesis de inducción $k - 1 = l - 1$, es decir $k = l$, y los $p_2, \dots, p_k$ son igual a los $q_2, \dots, q_k$.

Es seguro que cada uno de los lectores ya conoce el teorema fundamental de la aritmética, como lo enseñan en la escuela primaria y en los primeros años de bachillerato. A este grado el teorema es explicado "intuitivamente", sin demostración rigurosa, como es muy natural, porque, como acabamos de ver, la demostración exige unos raciocinios, ideas y artificios muy sutiles, que luégo son utilizados hasta en las matemáticas más altas. La desventaja de enseñar el teorema sin demostración es que, como lo observa Hasse en su libro, mucha gente cree que el teorema es evidente y no necesita demostración. El objeto principal de este artículo y de los dos siguientes de esta serie es de convencer al lector del contrario.

Para terminar observemos que si en la descomposición de un número n figura varias veces el mismo número primo, entonces estos se pueden juntar en uno solo escribiéndolo como una potencia. Por ejemplo $1.540 = 2^2 \times 5 \times 7 \times 11$, $1.800 = 2^3 \times 3^2 \times 5^2$. Finalmente si n es un número entero *negativo,* $(-1) \cdot n$ es positivo y así obtenemos la forma siguiente del teorema fundamental de la aritmética:

Cada número entero n *diferente de cero (positivo o negativo) se puede escribir en la forma*

$$n = \pm 1\ p_1^{\alpha_1}\ p_2^{\alpha_2} \ldots p_k^{\alpha_k},$$

donde $p_1, p_2, \ldots, p_k$ *son números primos diferentes y* $\alpha_1, \alpha_2, \ldots, \alpha_k$ *son números enteros positivos. Los números* $p_1, p_2, \ldots, p_k, \alpha_1, \alpha_2, \ldots, \alpha_k$ *son determinados completamente por el número n.*

Bibliografía.

G. H. Hardy — E. M. Wright: An introduction to the theory of numbers, Oxford University Press. 1945.

H. Hasse: Vorlesungen über Zahlentheorie, Springer, Berlín. 1950.

E. Landau: Elementare Zahlentheorie, Chelsea Publishing Co., Nueva York, 1950 (con diccionario alemán-inglés).