NUMEROS PRIMOS II.

Por J. Horváth.

4. En el número anterior dedujimos el teorema fundamental de la aritmética del lema de Euclides. En este número y en el número **7.** daremos otras dos demostraciones de este lema; la razón de esto es que en las demostraciones dadas en el número **2.** (pp. 28-30) utilizamos números fraccionarios (por lo menos en escritura; cf. la observación de la página 29) y es natural exigir que un teorema tan sencillo sobre números *enteros* se demuestre utilizando únicamente números *enteros*. Las ideas sobre las cuales serán basadas estas demostraciones se aplican también en muchas otras cuestiones de la Teoría de Números y del Algebra como por ejemplo en la descomposición de un polinomio en producto de "polinomios primos" (véase p. ej., van der Waerden, Algebra Moderna, §§ 18, 19, 23).

Sean a y b dos números enteros, que no son ambos iguales a cero. Llamemos M al conjunto de todos los números de la forma $ax + by$, en donde x e y son números enteros arbitrarios (positivos, negativos o nulos). El número a pertenece a M, puesto que podemos escribir $a = a.1 + b.0$, es decir a es de la forma $ax + by$ con $x = 1$, $y = 0$. Poniendo $x = 0$, $y = 1$ se ve que b también pertenece a M. De la misma manera se puede ver que $-a$, $-b$ y por lo tanto $|a|$ y $|b|$ pertenecen también a M.

Si dos números pertenecen a M, entonces su suma y su diferencia también pertenecen a M. En efecto, sean $ax + by$, $ax' + by'$ dos números de M, escribiendo

$$(ax + by) + (ax' + by') = a(x + x') + b(y + y'),$$
$$(ax - by) - (ax' + by') = a(x - x') + b(y - y'),$$

se ve inmediatamente la afirmación, puesto que $x + x'$, $y + y'$, $x - x'$, $y - y'$ son números enteros. *El producto de un número de M por un número entero arbitrario pertenece a M.* Sea en efecto

$ax + by$ un número de M y z un número entero cualquiera. Entonces

$$z\,(ax + by) = a(zx) + b(zy),$$

y es obvio que este último pertenece a M, puesto que zx y zy son números enteros.

El conjunto M contiene números positivos, por ejemplo $|a|$ o $|b|$. Entonces por la propiedad **A.** de los números enteros (p. 24.) *entre los números positivos pertenecientes a M existe uno inferior a todos los demás.* Llamemos este número d_1. Vamos a mostrar, ahora, que *cada número que pertenece a M es un múltiplo de* d_1. Por lo que hemos visto arriba, cada múltiplo de d_1 pertenece a M, entonces resultará que M no es otra cosa que el conjunto de todos los múltiplos de d_1.

Sea, pues, n un elemento de M. Por el teorema de la división con residuo (p. 26.) podemos escribir $n = d_1q + r$, donde $0 \leqslant \leqslant r < d_1$. Por las propiedades de M expuestas arriba vemos que d_1q y $r = n - d_1q$ pertenecen a M. Siendo por definición d_1 el menor número *positivo* de M, resulta que r es necesariamente igual a cero, es decir que $n = d_1q$, n es múltiplo de d_1.

Generalizando el concepto del máximo común divisor de *dos* números (p. 27.), vamos a introducir el concepto del máximo común divisor de un conjunto arbitrario de números enteros. Consideremos entonces un conjunto de números enteros, entre los cuales hay por lo menos un número, llamémoslo c, diferente de cero. El número entero positivo 1 divide a todos los números del conjunto, por el teorema 4 (p. 26.). Por otro lado cada número que divide a todos los números del conjunto, y cual por lo tanto divide a c, debe ser en valor absoluto inferior a $|c|$ por el teorema 15 (p. 26.). Existe entonces por la propiedad **B.** de los números enteros un número entero positivo que divide a todos los números del conjunto y es más grande que cualquier otro número entero con la misma propiedad. Este número se llamará el **máximo común divisor** de los números del conjunto.

De acuerdo con esta definición, se ve que d_1 es el máximo común divisor de los números del conjunto M. En efecto vimos que d_1 es divisor de cada número de M, y es claro que no hay número más grande con esta propiedad, ya que no hay número superior a d_1 que divida a d_1, en virtud del teorema 15 (p. 26.) puesto que d_1 es positivo.

Sea ahora $d = (a, b)$ el máximo común divisor de los números enteros a y b . d es también el máximo común divisor de los números de M. En efecto d divide a todos los números de la forma $ax + by$ por el teorema 12. (p. 26.) y no hay número más grande que haga esto, ya que no hay número más grande que d que divida a a y a b (por la definición de d; se recuerda aquí que a y b pertenecen a M).

Así, d y d_1 son ambos el máximo común divisor de M, luego $d = d_1$. Como d_1 pertenece a M (fué definido como el número positivo más pequeño que pertenece a M) es de la forma $ax + by$. Hemos obtenido, pues, el resultado importante de que *si* d = (a, b), *siempre existen dos números enteros* x *e* y, *tales que* d = ax + by. En particular *si* a *y* b *son primos relativos, es decir si* (a, b) = 1, *existen dos números enteros* x *e* y, *tales que* 1 = ax + by.

De este último se deduce fácilmente el

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

En virtud de la hipótesis $(a, b) = 1$ existen dos números enteros con los cuales $1 = ax + by$ o sea $(ac)x + (bc)y = c$. Como evidentemente $a|ac$ y por hipótesis $a|bc$, resulta, por el teorema 12 (p. 26.), que $a|c$. q. e. d.

5. De la representación de $d = (a, b)$ en la forma $d = ax + by$ se pueden deducir otra vez fácilmente las propiedades del máximo común divisor y del mínimo común múltiplo (cf. pp. 28-29.).

Sean a *y* b *dos números enteros que no son ambos iguales a cero y sea* d = (a, b). *Entonces, cada divisor común* f *de* a *y de* b *divide a* d. (Cf. Lema 2, (ii), p. 28.). Como $d = ax + by$ (x, y números enteros), $f|a$ $f|b$, la proposición resulta del teorema 12 (p. 26.).

Sean a *y* b *dos números enteros que no son ambos iguales a cero y sea* c *un número entero diferente de cero. Entonces* (a, b)|c| = = (ac, bc) (cf. Lemas 3 y 4, p. 29.). Sea $d = (a, b)$, existen dos números enteros x e y tales que $d = ax + by$, luego $c(a, b) = acx + bcy$. Si llamamos M' el conjunto de todos los números de la forma $acu + bcv$, donde u y v son números enteros arbitrarios, las consideraciones del número precedente muestran que los números que pertenecen a M' son precisamente los múltiplos de (ac, bc). Entonces, puesto que $c(a, b)$ pertenece a M', $(ac, bc) \mid c(a, b)$.

Por otro lado como $(a, b) \mid a$ y $(a, b) \mid b$, el teorema 7 (p. 26.) implica que $c(a, b) \mid ac$ y $c(a, b) \mid bc$. Luego por la proposición precedente $c(a, b) \mid (ac, bc)$ y en virtud del teorema 13 (p. 26.) $c(a, b) = \pm (ac, bc)$. Como $(a, b) > 0$, $(ac, bc) > 0$, de la última igualdad sigue $|c|\ (a, b) = (ac, bc)$. q. e. d.

Observemos que de esta última proposición resulta otra vez el lema de EUCLIDES. En efecto si $(a, b) = 1$, entonces $(ac, bc) = |c|$. De $a|ac$ y de $a|bc$ sigue $a|(ac, bc)$ es decir $a|c$.

A pesar de nuestra promesa inicial de no emplear sino números enteros, nos permitimos en la demostración que viene a continuación, usar la escritura de números fraccionarios. El lector podrá, como ejercicio, transformarla en otra en que las fracciones se evitan aun en la escritura.

Sean a *y* b *dos números enteros diferentes de cero. Sea* d = (a, b) *y* m = [a, b]. *Entonces* dm = |ab| (cf. Lema 2, (i), p. 28.). Por la proposición precedente

$$d = (a, b) = \left(\frac{a}{d} \cdot d, \frac{b}{d} \cdot d\right) = \left(\frac{a}{d}, \frac{b}{d}\right) d,$$

es decir $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ y $\left(\frac{am}{d}, \frac{bm}{d}\right) = m$. Como $a|m$ y $b|m$, del teorema 7. (p. 26.) sigue $\frac{ab}{d} \Big| \frac{am}{d}$ y $\frac{ab}{d} \Big| \frac{bm}{d}$ y entonces por la primera proposición de este número $\frac{ab}{d} \Big| m$. Por otro lado $a \Big| \frac{ab}{d}$ y $b \Big| \frac{ab}{d}$ (teorema 11, p. 26.), entonces en virtud del lema 1. (p. 28.) $m \Big| \frac{ab}{d}$. Del teorema 13 (p. 26.) resulta que $m = \pm \frac{ab}{d}$, es decir que $md = |ab|$.

q. e. d.

6. El teorema fundamental de la aritmética nos da un método cómodo para determinar el máximo común divisor y el mínimo común múltiplo de varios números.

Sean a y b dos números enteros. Para encontrar (a, b) podemos suponer que $a \geqslant 1$ y $b \geqslant 1$. De hecho, si por ejemplo $b = 0$, en-

tonces $a \neq 0$ y $(a, b) = |a|$. Además, por la relación evidente $(|a|, |b|) = (a, b)$, si a y b son ambos diferentes de cero, la búsqueda de su máximo común divisor se reduce a la búsqueda del máximo común divisor de dos números superiores o iguales a 1.

Escribamos, ahora, los dos números a y b como productos de potencias de números primos. Admitiendo la convención usual de que un número diferente de cero a la potencia cero es la unidad, se puede lograr que en los dos productos figuren los mismos números primos como bases:

$$
\begin{aligned}
& a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} \qquad (\alpha_1 \geqslant 0, \alpha_2 \geqslant 0, \ldots, \alpha_k \geqslant 0) \\
& b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k} \qquad (\beta_1 \geqslant 0, \beta_2 \geqslant 0, \ldots, \beta_k \geqslant 0)
\end{aligned} \tag{*}
$$

Así por ejemplo

$$1.638 = 2 \times 3^2 \times 7 \times 13 = 2 \times 3^2 \times 5^0 \times 7 \times 13,$$
$$2.100 = 2^2 \times 3 \times 5^2 \times 7 = 2^2 \times 3 \times 5^2 \times 7 \times 13^0.$$

Para que b *divida a* a *es necesario y suficiente que se cumplan las relaciones* $\alpha_1 \geqslant \beta_1, \alpha_2 \geqslant \beta_2, \ldots, \alpha_k \geqslant \beta_k$.

Si estas relaciones se cumplen, entonces

$$q = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \ldots p_k^{\alpha_k - \beta_k}$$

es un número entero y $bq = a$, es decir $b|a$. Inversamente si $b|a$ es decir si $bq = a$ (q entero), por el teorema fundamental de la aritmética cada divisor de b, que es una potencia de un número primo, debe dividir también a a (porque de otra manera obtendríamos dos descomposiciones diferentes de a en números primos). Esto demuestra inmediatamente las desigualdades $\alpha_1 \geqslant \beta_1$, $\alpha_2 \geqslant \beta_2$, ..., $\alpha_k \geqslant \beta_k$.

Siendo u y v dos números enteros, denotaremos por $min\ (u, v)$ el menor de los números u y v. Es evidente que $min\ (u, v) \leqslant u$, $min\ (u, v) \leqslant v$ y que $min\ (u, v)$ es el número entero más grande que tenga esta propiedad.

Siendo siempre a y b dos números enteros, $a \geqslant 1$, $b \geqslant 1$, escritos en la forma (*), sean $\gamma_1 = min\ (\alpha_1, \beta_1)$, $\gamma_2 = min\ (\alpha_2, \beta_2)$, ...,

$\gamma_k = min\ (\alpha_k, \beta_k)$. Entonces *el máximo común divisor de* a *y de* b *es igual a*

* $$d = p_1^{\gamma_1}\ p_2^{\gamma_2} \cdots p_k^{\gamma_k}$$

En efecto por la proposición precedente d divide a a y a b y es claro que no hay número más grande que haga lo mismo. Así por ejemplo

$$(1.638, 2.100) = 2 \times 3 \times 5^0 \times 7 \times 13^0 = 42.$$

De la misma manera se puede determinar el máximo común divisor de varios números; dejaremos los detalles al lector como ejercicio.

Siendo u y v dos números enteros, denotaremos por $max\ (u, v)$ el mayor de los dos números u y v. Es evidente que $u \leqslant max\ (u, v)$, $v \leqslant max\ (u, v)$ y que $max\ (u, v)$ es el número entero más pequeño que tenga esta propiedad. Además tenemos la igualdad obvia

$$max\ (u, v) + min\ (u, v) = u + v.$$

El mínimo común múltiplo $m = [a, b]$ es ahora

$$m = \frac{a\,b}{d} = \frac{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\, p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}}{p_1^{\gamma_1}\, p_2^{\gamma_2} \cdots p_k^{\gamma_k}} =$$

$$= p_1^{\alpha_1+\beta_1-\gamma_1}\ p_2^{\alpha_2+\beta_2-\gamma_2}\ \cdots\ p_k^{\alpha_k+\beta_k-\gamma_k}.$$

Poniendo $\delta_1 = max\ (\alpha_1, \beta_1)$, $\delta_2 = max\ (\alpha_2, \beta_2)$, $\ldots$, $\delta_k = max\ (\alpha_k, \beta_k)$, vemos entonces que

$$m = p_1^{\delta_1}\ p_2^{\delta_2} \cdots p_k^{\delta_k}.$$

Ejemplo:

$$[1.638, 2.100] = 2^2 \times 3^2 \times 5^2 \times 7 \times 13 = 81.900.$$

Ejercicio: ¿Cómo se define el mínimo común múltiplo de un conjunto *finito* de números enteros, diferentes de cero? ¿Por qué no

se puede definir el mínimo común múltiplo de un conjunto infinito de números enteros? Extender el método expuesto en esta sección a la determinación del mínimo común múltiplo de varios números.

7. En el número precedente hemos determinado el máximo común divisor de dos números utilizando sus descomposiciones en números primos. Pero podemos obtener el mismo resultado sin ellas, por un procedimiento que se llama el **algoritmo de Euclides** y que muchas veces da el resultado más rápidamente. Este algoritmo tiene también un interés teórico, pues nos conducirá a una nueva demostración del lema de EUCLIDES.

En este número también podemos suponer que $a \geqslant 1$, $b \geqslant 1$. Sea por ejemplo $a > b$, entonces por el teorema de la división con residuo $a = bq + r$, $0 \leqslant r < b$. Tenemos que $(a, b) = (b, r)$. Esta afirmación será evidente si tenemos en cuenta que cada divisor común de a y de b divide a r, es decir, es divisor común de b y de r, e inversamente cada divisor de b y de r divide a a, es decir es divisor común de a y de b.

Pongamos ahora $a = a_1$, $b = a_2$ y hagamos sucesivamente las divisiones

$$\begin{aligned} a_1 &= q_1 a_2 + a_3 & 0 \leqslant a_3 < a_2 \\ a_2 &= q_2 a_3 + a_4 & 0 \leqslant a_4 < a_3 \\ a_3 &= q_3 a_4 + a_5 & 0 \leqslant a_5 < a_4 \\ &\cdots\cdots\cdots & \cdots\cdots\cdots \end{aligned}$$

Como $a_1 > a_2 > a_3 > a_4 > \ldots$, después de un número finito de pasos debemos llegar a una división que da el residuo cero.

Sea

$$a_{i-1} = q_{i-1} a_i$$

Entonces por la observación precedente

$$\begin{aligned} (a_1, a_2) &= (a_2, a_3) = (a_3, a_4) = \ldots \\ &= (a_{i-1}, a_i) = (a_i, 0) = a_i . \end{aligned}$$

Es decir *el máximo divisor común* (a, b) *es el último residuo diferente de cero en la cadena de divisiones.* Por ejemplo poniendo $a = 2.100$, $b = 1.638$, los residuos sucesivos serán 462, 252, 210, 42, 0. Entonces (2.100, 1.638) = 42.

De las ecuaciones

$$a_1 = q_1 a_2 + a_3$$

. . . . . .

$$a_{i-2} = q_{i-2}\, a_{i-1} + a_i,$$

se pueden eliminar sucesivamente los números a_{i-1}, a_{i-2}, ..., a_4, a_3. En efecto

$$\begin{aligned} a_i &= a_{i-2} - q_{i-2}\, a_{i-1} = a_{i-2} - q_{i-2}\,(a_{i-3} - q_{i-3}\, a_{i-2}) \\ &= a_{i-2}\,(1 + q_{i-2}\, q_{i-3}) - a_{i-3}\, q_{i-2}, \\ a_i &= (a_{i-4} - q_{i-4}\, a_{i-3})\,(1 + q_{i-2}\, q_{i-3}) - a_{i-3}\, q_{i-2} = \\ &= a_{i-4}\,(1 + q_{i-2}\, q_{i-3}) - a_{i-3}\,(q_{i-2} + q_{i-4} + q_{i-2}\, q_{i-3}\, q_{i-4}), \end{aligned}$$

etc. Finalmente llegaremos a una expresión de la forma

$$a_i = a_1 x + a_2 y, \text{ es decir } d = ax + by,$$

en donde x e y son números enteros. El lema de EUCLIDES es consecuencia inmediata de esta representación de d, como lo hemos visto en el número **4.** Esta es la demostración original de EUCLIDES para su lema.

8. Durante 2.000 años la demostración del teorema fundamental de la aritmética, dada en el número **3** y basada esencialmente sobre el lema de EUCLIDES, era la única. Esta demostración es sumamente importante porque, como ya lo hemos observado, se puede aplicar en muchas otras circunstancias. Sin embargo, es interesante ver ahora una demostración que no presupone el conocimiento del lema de EUCLIDES, y que fue dada en el siglo XX. por ERNESTO ZERMELO. Esta demostración conduce quizás más rápidamente al teorema fundamental.

Tenemos que demostrar que, prescindiendo del orden, un número entero $n > 1$ se puede escribir sólo de una manera como producto de números primos (cf. p. 32.). Haremos otra vez la demostración por inducción completa según el número n. Para $n = 1$ no hay nada que demostrar. Supongamos que el teorema sea válido para $n = 1, 2, \ldots, m - 1$. Si m es un número primo no hay nada que demostrar. Si m no es primo, tiene un factor primo p_1 * (cf. p. 31) y se puede escribir $m = p_1 s$, donde $1 \leqq s \leqq m - 1$ y enton-

* p se llama factor primo de n, si p es un número primo que divide a n (porque entonces figura como factor en la descomposición de n).

ces, por la hipótesis de inducción, s se escribe de una manera única en la forma $s = p_2\, p_3 \ldots p_k$, donde $p_2, p_3, \ldots, p_k$ son números primos. Supongamos ahora que m admita otra descomposición en números primos $m = q_1\, q_2 \ldots q_l$. Entonces p_1 es diferente de cada uno de los números $q_1, q_2, \ldots, q_l$. En efecto si fuera $p_1 = q_i$, de $m = p_1 s = q_1\, q_2 \ldots q_l$ obtendríamos que s es igual al producto de los números primos $q_1, q_2, \ldots, q_{i-1}, q_{i+1}, \ldots, q_l$. Pero la descomposición de s es única, entonces estos últimos números primos serían los mismos que $p_2, p_3, \ldots, p_k$. Así la descomposición $m = q_1\, q_2 \ldots q_l$ sería la misma que $m = p_1\, p_2 \ldots p_k$

Como $p_1 \neq q_1$, evidentemente tenemos el derecho de suponer que $p_1 < q_1$. Sea $m = q_1 t$, donde $t = q_2\, q_3 \ldots q_l$. Sea

$$m' = m - p_1 t = \begin{cases} p_1 (s - t) \\ (q_1 - p_1)t. \end{cases}$$

Puesto que $q_1 > p_1$, m' es un número entero positivo y $m' < m$. Los números $s - t$, $q_1 - p_1$, t son también números enteros inferiores a m, y por la hipótesis de inducción tienen entonces descomposiciones únicas en números primos. De la representación $m' = p_1 (s - t)$ se ve que p_1 debe ser factor primo de m' Luego de la representación $m' = (q_1 - p_1)t$ se ve que p_1 debe ser factor primo de $q_1 - p_1$ o de t. Pero ya hemos visto anteriormente que p_1 es diferente de los factores primos $q_2, q_3, \ldots, q_l$ de t. Entonces $p_1 | (q_1 - p_1)$. Como $p_1 | p_1$, vemos que $p_1 | q_1$. Puesto que $1 < p_1 < q_1$ y que q_1 es primo, esto es imposible, entonces la hipótesis de que m se puede descomponer de dos maneras diferentes en números primos, conduce a una contradicción y esta contradicción demuestra el teorema.

La demostración precedente utiliza muy hábilmente el hecho de que el lema de Euclides es, por su parte, consecuencia del teorema fundamental de la aritmética. En efecto $(a, b) = 1$ quiere decir que a y b no tienen factor primo común. Si $a | bc$, todos los factores primos de a lo son también de bc. Pero como no pueden ser de b, lo son de c, es decir $a | c$. Cuando la demostración precedente concluye de $p_1 | (q_1 - p_1)t$ que $p_1 | (q_1 - p_1)$ o $p_1 | t$, utiliza el hecho de que el teorema fundamental ya se supone válido para números enteros positivos inferiores a m, es decir que en realidad el lema de Euclides se considera verdadero para números b y c cuyo producto es inferior a m.