

Revista Digital: Matemática, Educación e

Internet

ISSN: 1659-0643

revistadigitalmatematica@itcr.ac.cr

Instituto Tecnológico de Costa Rica

Costa Rica

Braddock S., George

Una fórmula que relaciona a los números primos con la función parte entera y los
números triangulares

Revista Digital: Matemática, Educación e Internet, vol. 15, núm. 1, agosto-febrero, 2015,
pp. 1-15

Instituto Tecnológico de Costa Rica
Cartago, Costa Rica

Disponible en: <https://www.redalyc.org/articulo.oa?id=607973004001>

- ▶ Cómo citar el artículo
- ▶ Número completo
- ▶ Más información del artículo
- ▶ Página de la revista en redalyc.org



Una fórmula que relaciona a los números primos con la función parte entera y los números triangulares

George Braddock S.
georgebraddock@gmail.com

Recibido: 1 octubre, 2012 Aceptado: 29 abril, 2014

Resumen. El máximo común divisor entre un número primo p y cada uno de los enteros positivos menores que p es igual a 1 y, como el máximo común divisor se relaciona con la función parte entera según una fórmula explícita dada por el matemático brasileño M. Polezzi (1997), entonces se halló una interesante proposición que relaciona los números primos, la función parte entera, los números cuadrados y los números triangulares. Esa proposición sirve como un nuevo test para probar la primalidad de un número.

Palabras clave: Divisibilidad, máximo común divisor, mcd, puntos reticulares, función parte entera, números primos, coprimos, números triangulares, test de primalidad.

Abstract. The greatest common divisor between a prime number p and each of the positive integers less than p is equal to 1 and, as the greatest common divisor is related with the floor function according to a explicit formula given by the brasilian mathematician M. Polezzi (1997), then it was found a interesting proposition relating the prime numbers, the floor function, the square numbers and the triangular numbers. This proposition serves as a new test for testing the primality of a number.

KeyWords: Divisibility, greatest common divisor, gcd, reticular points, lattice points, integer part function, prime numbers, relative primes, triangular numbers, primality test.

1.1 Introducción

Existe una estrecha relación entre el máximo común divisor de dos números n y d , con el número de puntos $(x,y) \in \mathbb{Z} \times \mathbb{Z}$, que están en el segmento que une los puntos $(n,0)$ y $(0,d)$.

Esa relación le permitió al matemático Marcelo Polezzi, del Departamento de Matemática de la Universidad Estatal Paulista (de Brasil), establecer en 1997 una fórmula explícita para el máximo común divisor de dos números.

Aquí se utilizó dicha fórmula y, teniendo en cuenta que un número primo es coprimo con todos los enteros menores que él, se halló una interesante proposición que relaciona a los números primos con la función parte entera y con el polinomio $n^3 - 4n^2 + 5n - 2$.

Esa proposición (dada en el teorema 1.5 de este artículo) y sus corolarios, sirven como un nuevo test para probar la primalidad de un número. En uno de esos corolarios se relacionan los números primos, la función parte entera, los números cuadrados y los números triangulares.

1.2 Relación del máximo común divisor con la función parte entera

Definición 1.1

Un punto P de coordenadas (x,y) se llama punto entero o también punto reticular si tanto x como y son números enteros, es decir si $(x,y) \in \mathbb{Z} \times \mathbb{Z}$.

Teorema 1.1 (Relación del máximo común divisor con los puntos reticulares)

Si n y d son enteros positivos, entonces

$$|H| = 1 + mcd(n,d),$$

donde H es conjunto de puntos reticulares en el segmento que une los puntos $(n,0)$ y $(0,d)$.

Demostración: Se verá primero un ejemplo con $n = 15$, $d = 10$:

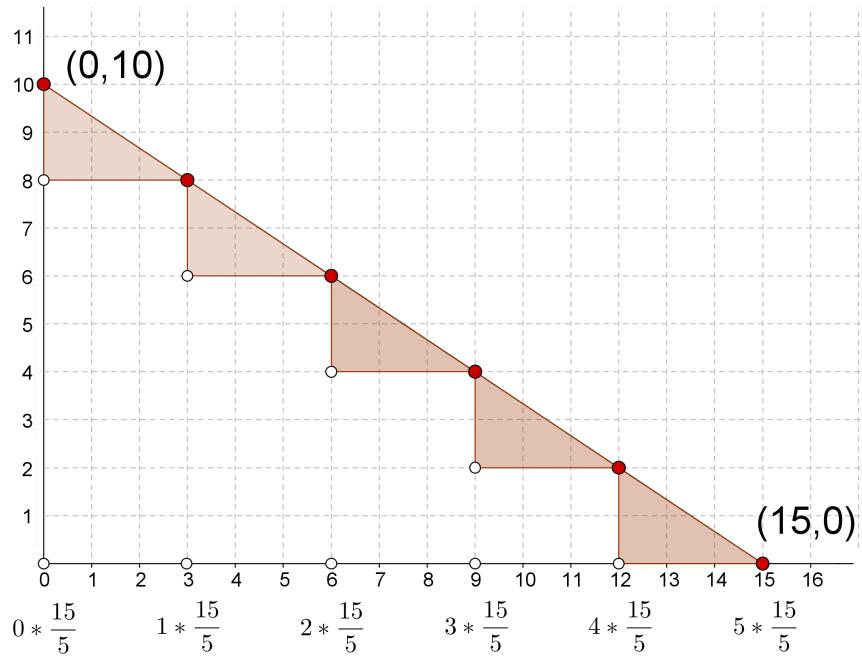


Figura 1.1: Como $\text{mcd}(15, 10) = 5$ y $\frac{10}{15} = \frac{2}{3}$ entonces hay 5 triángulos rectángulos con catetos de medida 2 y 3, cuya hipotenusa está contenida en la hipotenusa del triángulo ABC , como se muestra en las regiones sombreadas. El número de puntos reticulares en la hipotenusa es igual a $1 + \text{mcd}(15, 10) = 1 + 5 = 6$.

Se definen los enteros z , a y b así:

$$z = \text{mcd}(15, 10) = 5, \quad a = \frac{10}{z} = \frac{10}{5} = 2, \quad b = \frac{15}{z} = \frac{15}{5} = 3.$$

Note, en la Figura 1.1, que la ecuación de la recta AB es $y = 10 - \frac{a}{b}x$ y que, a los valores de x que son múltiplos de 3 en $[0, 15]$, les corresponde un valor entero de y que es múltiplo de 2 en $[0, 10]$. El número de puntos reticulares en el segmento AB es

$$1 + \left\lfloor \frac{15}{b} \right\rfloor = 1 + \left\lfloor \frac{10}{a} \right\rfloor = 1 + \text{mcd}(15, 10).$$

Aquí inicia la demostración del teorema: Se le llamará A al punto $(n, 0)$ y B al punto $(0, d)$. Si se definen los enteros z , a , b , w así:

$$z = \text{mcd}(n, d), \quad a = \frac{d}{z}, \quad b = \frac{n}{z}, \quad w = \frac{a}{b}x$$

Note que la recta AB tiene ecuación $y = d - wx$ y que $y \in \mathbb{Z} \iff w \in \mathbb{Z}$.

Por el teorema 1.6, se tiene que $\text{mcd}(a, b) = 1$. Luego, por el corolario 1.11 (del teorema 1.7), se tiene que todas las soluciones de la ecuación diofántica $ax = bw$ están dadas por el conjunto

$$\{(x, w) \in \mathbb{Z} \times \mathbb{Z} / x = bk, w = ak, k \in \mathbb{Z}\}$$

Por el corolario 1.12 (del teorema 1.8), existen $\lfloor \frac{n}{b} \rfloor$ múltiplos de b en el segmento $[1, n]$ y existen $\lfloor \frac{d}{a} \rfloor$ múltiplos de a en el segmento $[1, d]$. Entonces, los únicos valores de x correspondientes a puntos reticulares del segmento AB , son los valores de x que están en el conjunto

$$\mathbb{X} = \left\{ 0 \times b, 1 \times b, 2 \times b, \dots, \left\lfloor \frac{n}{b} \right\rfloor \times b, \right\},$$

y los valores de y correspondientes son los dados por el conjunto

$$\mathbb{Y} = d - \left\{ 0 \times a, 1 \times a, 2 \times a, \dots, \left\lfloor \frac{d}{a} \right\rfloor \times a, \right\}.$$

El total de puntos reticulares en AB es entonces

$$|\mathbb{X}| = 1 + \left\lfloor \frac{n}{b} \right\rfloor = 1 + \left\lfloor \frac{n}{\frac{n}{z}} \right\rfloor = 1 + [z] = 1 + z = 1 + \text{mcd}(n, d)$$

que puede calcularse también así:

$$|\mathbb{Y}| = 1 + \left\lfloor \frac{d}{a} \right\rfloor = 1 + \left\lfloor \frac{d}{\frac{d}{z}} \right\rfloor = 1 + [z] = 1 + z = 1 + \text{mcd}(n, d)$$

Si H es el conjunto de puntos reticulares en el segmento AB , entonces se cumple la igualdad:

$$|H| = 1 + \text{mcd}(n, d) \quad (1.1)$$

■

Corolario 1.1

Si se le llama h al conjunto de puntos reticulares en la hipotenusa del triángulo rectángulo AOB , sin contar a los puntos $(0, d)$ y $(n, 0)$, entonces

$$\text{mcd}(n, d) = 1 + |h| \quad (1.2)$$

Demostración: Por el teorema 1.1, $\text{mcd}(n, d) = |H| - 1$, pero como $|H| = 2 + |h|$, $\text{mcd}(n, d) = 2 + |h| - 1$ entonces $\text{mcd}(n, d) = 1 + |h|$ ■

Corolario 1.2

Si n y d son coprimos, entonces $|h| = 0$, donde h es el conjunto de puntos reticulares en la hipotenusa del triángulo rectángulo AOB , sin incluir los puntos $(n, 0)$ y $(0, d)$.

Teorema 1.2 (La fórmula de Polezzi)

Si n y d son enteros positivos, entonces

$$\text{mcd}(n, d) = n + d - nd + 2 \sum_{k=1}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor \quad (1.3)$$

Demostración: Esta demostración es una adaptación de la prueba dada en [2], pág. 445 (1997), por el matemático Marcelo Polezzi de Brasil.

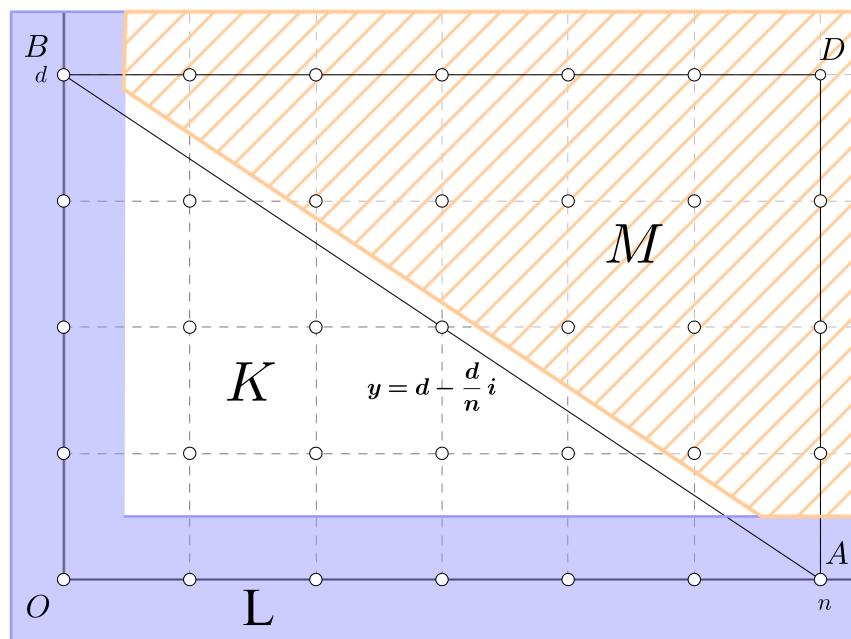


Figura 1.2: El número de puntos reticulares que están dentro y en el borde del rectángulo OADB es igual a la suma del número de puntos reticulares de cada una de las regiones L, K, M

En la Figura 1.2 las coordenadas de los puntos A , D y B son $(n, 0)$, (n, d) y $(0, d)$ respectivamente.

Como la ecuación de la recta AB es $y = d - \frac{d}{n}x$ el número de puntos reticulares en la región K está dado por

$$|K| = \sum_{i=1}^{n-1} \left\lfloor d - \frac{d}{n}i \right\rfloor = \sum_{i=1}^{n-1} \left\lfloor \frac{nd}{n} - \frac{d}{n}i \right\rfloor = \sum_{i=1}^{n-1} \left\lfloor \frac{d}{n}(n-i) \right\rfloor$$

haciendo el cambio de variable $k = n - i$, se puede escribir

$$|K| = \sum_{k=1}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor \quad (1.4)$$

El número de puntos reticulares de la región L es

$$|L| = n + d + 1 \quad (1.5)$$

Debido a la simetría del rectángulo $OADB$ con respecto a la línea AB , se tiene

$$|M| + |H| = |L| + |K|$$

Por la igualdad (1.1) se tiene que

$$|M| + 1 + mcd(n, d) = |L| + |K|$$

de donde se obtiene la igualdad

$$|M| = |L| + |K| - 1 - mcd(n, d) \quad (1.6)$$

Se le llamará N al conjunto de puntos reticulares que hay tanto en el borde como en el interior del rectángulo $OADB$. En la Figura 1.2 resulta evidente la igualdad

$$|N| = |L| + |K| + |M|$$

usando el resultado (1.6) se obtiene la igualdad

$$|N| = |L| + |K| + |L| + |K| - 1 - mcd(n, d)$$

$$|N| = 2|L| + 2|K| - 1 - mcd(n, d) \quad (1.7)$$

Pero, como un lado del rectángulo tiene $(n + 1)$ puntos reticulares y el otro lado tiene $(d + 1)$ puntos, se puede decir también que

$$|N| = (n + 1)(d + 1) = nd + n + d + 1 \quad (1.8)$$

A partir de (1.7) y (1.8) se tiene

$$2|L| + 2|K| - 1 - mcd(n, d) = nd + n + d + 1,$$

usando (1.5) y (1.4) queda

$$2(n + d + 1) + 2 \left(\sum_{k=1}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor \right) - 1 - mcd(n, d) = nd + n + d + 1$$

$$n + d + 1 + 2 \left(\sum_{k=1}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor \right) - 1 - mcd(n, d) = nd$$

$$\text{mcd}(n,d) = n + d - nd + 2 \left(\sum_{k=1}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor \right)$$

■

Esta es una fórmula explícita para el máximo común divisor, que lo relaciona con la función *parte entera*. Como existe una estrecha relación entre el máximo común divisor y los números primos, la fórmula anterior nos permitirá más adelante, establecer una relación entre los números primos y la función *parte entera*.

1.3 Relación de los números primos con los puntos reticulares

Teorema 1.3

Un entero positivo n es primo si y solo si es coprimo con cada uno de los números enteros del conjunto $D = \{1, 2, 3, 4, \dots, n-1\}$.

Demostración:

“ \Rightarrow ”

Si n es primo sus únicos divisores son 1 y n . Entonces ninguno de los elementos del conjunto D , excepto el 1, son divisores de n . Se deduce que el único divisor común con cada uno de ellos es 1 y por lo tanto es coprimo con cada uno de ellos.

“ \Leftarrow ”

Si n es coprimo con todos los números del conjunto D , entonces ninguno de esos números, excepto el 1, divide a n . Se concluye que los únicos divisores de n son 1 y el mismo n , esto es n es un primo. ■

Corolario 1.3

Un entero positivo n es primo si y solo si

$$\sum_{d=1}^{n-1} \text{mcd}(n,d) = n - 1$$

Demostración: n es primo siii $\sum_{d=1}^{n-1} \text{mcd}(n,d) = \sum_{d=1}^{n-1} 1 = n - 1$

■

El teorema 1.3 puede expresarse de la siguiente manera:

Corolario 1.4

Un número entero positivo n es primo si y solo si ninguna de las rectas que unen el punto $(n, 0)$ con los puntos $(0, d)$ con $d \in \{1, 2, 3, 4, \dots, n - 1\}$ contiene algún punto reticular, distinto de ellos.

La demostración se deja como ejercicio para el lector.

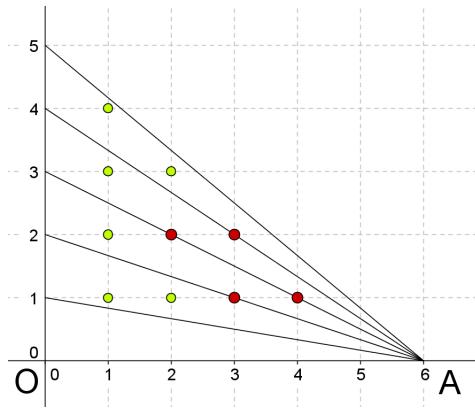


Figura 1.3: Como el número 6 es compuesto, hay puntos reticulares en al menos una de las líneas que unen el punto $(6, 0)$ con los puntos $(0, d)$, con $0 < d < 6$.

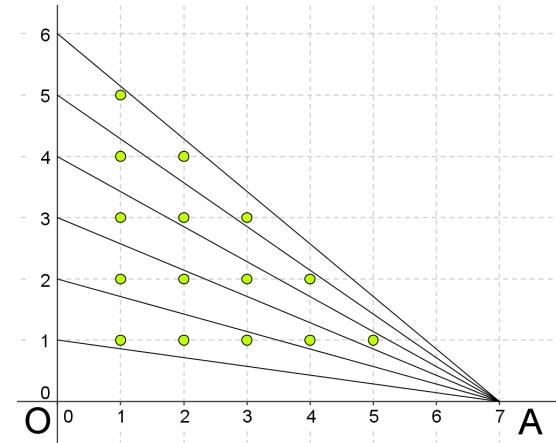


Figura 1.4: Como el número 7 es primo, no hay puntos reticulares en ninguna de las líneas que unen el punto $(7, 0)$ con los puntos $(0, d)$, con $0 < d < 7$.

En la Figura 1.3 se observa que, si $k = \text{mcd}(n, d)$ y n es un número compuesto, habrá $k - 1$ puntos reticulares en la línea que une el punto $(n, 0)$ con el punto $(0, d)$ (sin incluir esos puntos).

En la Figura 1.4 se observa que, si n es un número primo, no hay puntos reticulares en las líneas que unen el punto $(n, 0)$ con el punto $(0, d)$ (sin incluir esos puntos).

Teorema 1.4

El número de puntos reticulares de la región K de la Figura 1.2 está dado por

$$|K| = \frac{(n-1)(d-1)}{2} \quad (1.9)$$

si y solo si n y d son coprimos.

Demostración: Por la fórmula de Polezzi (1.3) se tiene

$$\text{mcd}(n, d) = n + d - nd + 2 \sum_{k=1}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor,$$

que, por la fórmula (1.4), puede escribirse

$$\text{mcd}(n, d) = n + d - nd + 2|K|.$$

Como $\text{mcd}(n, d) = 1$ si y solo si n y d son coprimos, entonces

$$1 = n + d - nd + 2|K|$$

$$d(1-n) + 2|K| = 1 - n$$

$$2|K| = (1-n) - d(1-n)$$

$$|K| = \frac{(n-1)(d-1)}{2}$$

se cumple si y solo si n y d son coprimos ■

1.4 Relación de los números primos con la función parte entera

Teorema 1.5

Un entero positivo n es primo si y solo si

$$\sum_{d=2}^{n-1} \sum_{k=2}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor = \frac{n^3 - 4n^2 + 5n - 2}{4} \quad (1.10)$$

Demostración: Teniendo en cuenta la fórmula (1.4), el teorema 1.3 y el teorema 1.4, podemos decir que un entero positivo n es primo si y solo si

$$\sum_{d=1}^{n-1} \sum_{k=1}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor = \sum_{d=1}^{n-1} \frac{(n-1)(d-1)}{2}$$

$$\sum_{d=1}^{n-1} \left(\left\lfloor \frac{d}{n} \right\rfloor + \sum_{k=2}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor \right) = \sum_{d=2}^{n-1} \frac{(n-1)(d-1)}{2}$$

pero como $\left\lfloor \frac{d}{n} \right\rfloor = 0 \forall d < n$

$$\sum_{d=1}^{n-1} \left(0 + \sum_{k=2}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor \right) = \sum_{d=2}^{n-1} \frac{(n-1)(d-1)}{2}$$

$$\sum_{d=1}^{n-1} \sum_{k=2}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor = \frac{(n-1)}{2} \left[\sum_{d=2}^{n-1} d - \sum_{d=2}^{n-1} 1 \right]$$

$$\sum_{d=1}^{n-1} \sum_{k=2}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor = \frac{(n-1)}{2} \left[\frac{(n-1)n}{2} - 1 - (n-2) \right]$$

$$\sum_{k=2}^{n-1} \left\lfloor \frac{k}{n} \right\rfloor + \sum_{d=2}^{n-1} \sum_{k=2}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor = \frac{(n-1)}{2} \left[\frac{n^2 - n - 2n + 2}{2} \right]$$

pero como $\left\lfloor \frac{k}{n} \right\rfloor = 0 \forall k < n$

$$\sum_{k=2}^{n-1} 0 + \sum_{d=2}^{n-1} \sum_{k=2}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor = \frac{(n-1)}{2} \left[\frac{n^2 - n - 2n + 2}{2} \right]$$

$$\sum_{d=2}^{n-1} \sum_{k=2}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor = \frac{(n-1)}{2} \left[\frac{n^2 - n - 2n + 2}{2} \right]$$

$$\sum_{d=2}^{n-1} \sum_{k=2}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor = \frac{n^3 - 4n^2 + 5n - 2}{4}$$

■

Corolario 1.5

Un entero positivo n es primo si y solo si

$$\sum_{d=2}^{n-1} \sum_{k=2}^{n-1} n \left\lfloor \frac{dk}{n} \right\rfloor = t_{n-2} t_{n-1} \quad (1.11)$$

donde $(t_n)_{n \in \mathbb{N} + \{0\}}$ es la secuencia de números triangulares.

Demostración: El teorema 1.5 puede expresarse como se enuncia aquí en este corolario, debido a la identidad

$$\frac{n^3 - 4n^2 + 5n - 2}{4} = \frac{(n-1)(n-1)(n-2)}{4} = \frac{(n-1)n}{2n} \frac{(n-2)(n-1)}{2} = \frac{1}{n} t_{n-1} t_{n-2}$$

Note que, por el teorema 1.8 de la sección 1.5, el término $n \left\lfloor \frac{dk}{n} \right\rfloor$ es el mayor múltiplo de n menor o igual que dk .

Corolario 1.6

Un entero positivo n es primo si y solo si

$$\sum_{d=2}^{n-1} \sum_{k=2}^{n-1} n \left\lfloor \frac{dk}{n} \right\rfloor = \binom{n-1}{2} \binom{n}{2} \quad (1.12)$$

Demostración: El corolario 1.5 puede expresarse como se enuncia aquí en este corolario, debido a las identidades:

$$t_{n-1} = \frac{(n-1)n}{2} = \frac{(n-2)!(n-1)n}{2(n-2)!} = \frac{n!}{2(n-2)!} = \binom{n}{2}$$

$$t_{n-2} = \frac{(n-2)(n-1)}{2} = \frac{(n-3)!(n-2)(n-1)}{2(n-3)!} = \frac{(n-1)!}{2((n-1)-2)!} = \binom{n-1}{2}$$

Corolario 1.7

Un entero positivo n es primo si y solo si

$$2n \sum_{d=2}^{n-1} \sum_{k=2}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor = t_{(C_{n-1}-1)} \quad (1.13)$$

donde $(C_n)_{n \in \mathbb{N}}$ es la secuencia de números cuadrados y $(t_n)_{n \in \mathbb{N} + \{0\}}$ la de números triangulares.

Demostración: El corolario 1.5, puede expresarse como se enuncia en este corolario, debido a las identidades:

$$\begin{aligned} t_{n-2} t_{n-1} &= \frac{(n-2)(n-1)}{2} \frac{(n-1)n}{2} \\ t_{n-2} t_{n-1} &= \frac{(n-1)^2[(n-1)-1][(n-1)+1]}{2^2} \\ t_{n-2} t_{n-1} &= \frac{(n-1)^2[(n-1)^2-1]}{2^2} \\ 2t_{n-2} t_{n-1} &= \frac{C_{n-1}(C_{n-1}-1)}{2} \\ 2t_{n-2} t_{n-1} &= t_{(C_{n-1}-1)} \end{aligned}$$

El teorema 1.5 y sus corolarios, proporcionan un nuevo test de primalidad para un número n , que requiere que se realicen $(n-2)^2$ sumas, cuyos términos son todos menores o iguales a $n-2$.

Se verificará a continuación que la fórmula (1.13) se cumple para $n = 7$, pues 7 es primo.

Para $n = 7$ la parte derecha de la fórmula (1.13) es

$$t_{(C_6-1)} = t_{35} = \frac{35 \cdot 36}{2} = 35 \cdot 18 = 630$$

La parte izquierda

$$2 \cdot 7 \sum_{d=2}^6 \sum_{k=2}^6 \left\lfloor \frac{dk}{7} \right\rfloor$$

es igual a

$$\begin{aligned} &14 \cdot \left(\left\lfloor \frac{2 \cdot 2}{7} \right\rfloor + \left\lfloor \frac{2 \cdot 3}{7} \right\rfloor + \left\lfloor \frac{2 \cdot 4}{7} \right\rfloor + \left\lfloor \frac{2 \cdot 5}{7} \right\rfloor + \left\lfloor \frac{2 \cdot 6}{7} \right\rfloor + \left\lfloor \frac{3 \cdot 2}{7} \right\rfloor + \left\lfloor \frac{3 \cdot 3}{7} \right\rfloor + \left\lfloor \frac{3 \cdot 4}{7} \right\rfloor + \left\lfloor \frac{3 \cdot 5}{7} \right\rfloor + \left\lfloor \frac{3 \cdot 6}{7} \right\rfloor + \left\lfloor \frac{4 \cdot 2}{7} \right\rfloor + \left\lfloor \frac{4 \cdot 3}{7} \right\rfloor \right. \\ &\quad \left. + \left\lfloor \frac{4 \cdot 4}{7} \right\rfloor + \left\lfloor \frac{4 \cdot 5}{7} \right\rfloor + \left\lfloor \frac{4 \cdot 6}{7} \right\rfloor + \left\lfloor \frac{5 \cdot 2}{7} \right\rfloor + \left\lfloor \frac{5 \cdot 3}{7} \right\rfloor + \left\lfloor \frac{5 \cdot 4}{7} \right\rfloor + \left\lfloor \frac{5 \cdot 5}{7} \right\rfloor + \left\lfloor \frac{5 \cdot 6}{7} \right\rfloor + \left\lfloor \frac{6 \cdot 2}{7} \right\rfloor + \left\lfloor \frac{6 \cdot 3}{7} \right\rfloor + \left\lfloor \frac{6 \cdot 4}{7} \right\rfloor + \left\lfloor \frac{6 \cdot 5}{7} \right\rfloor + \left\lfloor \frac{6 \cdot 6}{7} \right\rfloor \right) \\ &= 14 \cdot ((0+0+1+1+1) + (0+1+1+2+2) + (1+1+2+2+3) + (1+2+2+3+4) + (1+2+3+4+5)) = 14 \cdot (3+6+9+12+15) = 14 \cdot 45 = 630 \end{aligned}$$

Entonces sí se cumple que la parte izquierda es igual a la parte derecha, cuando $n = 7$.

Se verificará a continuación que la fórmula (1.13) no se cumple para $n = 6$, pues 6 es compuesto.

Para $n = 6$ la parte derecha de la fórmula (1.13) es

$$t_{(C_5-1)} = t_{24} = \frac{24 \cdot 25}{2} = 12 \cdot 25 = 300$$

La parte izquierda

$$2 \cdot 6 \sum_{d=2}^5 \sum_{k=2}^5 \left\lfloor \frac{dk}{6} \right\rfloor$$

es igual a

$$\begin{aligned} & 12 \cdot \left(\left\lfloor \frac{2 \cdot 2}{6} \right\rfloor + \left\lfloor \frac{2 \cdot 3}{6} \right\rfloor + \left\lfloor \frac{2 \cdot 4}{6} \right\rfloor + \left\lfloor \frac{2 \cdot 5}{6} \right\rfloor + \left\lfloor \frac{3 \cdot 2}{6} \right\rfloor + \left\lfloor \frac{3 \cdot 3}{6} \right\rfloor + \left\lfloor \frac{3 \cdot 4}{6} \right\rfloor + \left\lfloor \frac{3 \cdot 5}{6} \right\rfloor \right. \\ & \quad \left. + \left\lfloor \frac{4 \cdot 2}{6} \right\rfloor + \left\lfloor \frac{4 \cdot 3}{6} \right\rfloor + \left\lfloor \frac{4 \cdot 4}{6} \right\rfloor + \left\lfloor \frac{4 \cdot 5}{6} \right\rfloor + \left\lfloor \frac{5 \cdot 2}{6} \right\rfloor + \left\lfloor \frac{5 \cdot 3}{6} \right\rfloor + \left\lfloor \frac{5 \cdot 4}{6} \right\rfloor + \left\lfloor \frac{5 \cdot 5}{6} \right\rfloor \right) \\ & = 12 \cdot ((0+1+1+1) + (1+1+2+2) + (1+2+2+3) + (1+2+3+4)) \\ & = 12 \cdot (3+6+8+10) = 12 \cdot 27 = 324 \end{aligned}$$

Entonces no se cumple que la parte izquierda sea igual a la parte derecha, cuando $n = 6$.

Se ha verificado así el corolario 1.7 para los casos $n = 7$ y $n = 6$. El lector puede ahora verificar dicho corolario para otros valores de n .

Corolario 1.8

Si n es primo, entonces el número triangular $t_{(C_{n-1}-1)}$ es divisible por $2n$.

Demostración: Se definirá así al número z :

$$z = \sum_{d=2}^{n-1} \sum_{k=2}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor$$

que es un número entero pues es suma de enteros.

Por el corolario 1.7, si n es un primo entonces se cumple la igualdad

$$2nz = t_{(C_{n-1}-1)}$$

esto es

$$z = \frac{1}{2n} t_{(C_{n-1}-1)}$$

y como z es entero, esto implica que $t_{(C_{n-1}-1)}$ es divisible por $2n$

■

Ejemplo 1.1

Según el corolario 1.8, como el número 13 es primo, debe cumplirse que el número triangular $t_{(C_{12}-1)}$ es divisible por 26. Veamos:

$$t_{(C_{12}-1)} = t_{12^2-1} = t_{143} = \frac{143 \cdot 144}{2} = 143 \times 72 = 10296$$

que es un número divisible por 26 pues $10296 = 26 \times 396$.

La proposición recíproca del corolario 1.8 no es cierta. Un contraejemplo ocurre para $n = 6$, pues se vió antes que $t_{(C_5-1)} = 300$, que sí es divisible por $2 \cdot 6 = 12$, pero 6 no es primo.

Corolario 1.9

Si el número triangular $t_{(C_{n-1}-1)}$ no es divisible por $2n$ entonces n es compuesto.

Demostración: Esta proposición es la contrapositiva de la demostrada en el corolario 1.8 ■

Ejemplo 1.2

Para $n = 12$ se tiene que

$$t_{(C_{11}-1)} = t_{11^2-1} = t_{120} = \frac{120 \cdot 121}{2} = 60 * 121 = 7260$$

que no es divisible por $2n = 2 \cdot 12 = 24$ pues $7260 = 24 \cdot 302 + 12$.

Se concluye entonces que 12 es un número compuesto.

Corolario 1.10

Si n es primo entonces $n^3 + n - 2$ es divisible por 4.

Demostración: Se deja como ejercicio para el lector. Sugerencia: Use el teorema 1.5 y las propiedades de la relación de divisibilidad. ■

1.5 Algunos teoremas utilizados

Teorema 1.6

Si $a, b \in \mathbb{Z}$ y $\text{mcd}(a, b) = z$ entonces $\text{mcd}(\frac{a}{z}, \frac{b}{z}) = 1$.

Demostración: Se puede ver la prueba en la solución del ejercicio 4 de la sección 3 · 2 de [1], pág. 372 ■

Teorema 1.7

Si $a, b \in \mathbb{Z}$, $\text{mcd}(a, b) = 1$ y (x_0, y_0) es una solución de la ecuación diofántica lineal

$$ax + by = c$$

entonces, para $k \in \mathbb{Z}$, todas las soluciones de esta ecuación son de la forma

$$x = x_0 - bk \quad y = y_0 + ak$$

Demostración:

Se puede ver la prueba en la demostración del teorema 13 de [1], pág. 136 ■

Corolario 1.11

Si $a, b \in \mathbb{Z}$, $\text{mcd}(a, b) = 1$ entonces todas las soluciones de la ecuación diofántica lineal

$$ax - by = 0$$

son, para $k \in \mathbb{Z}$, de la forma

$$x = bk \quad y = ak$$

Teorema 1.8

Sean n y p enteros positivos y $p \leq n$, entonces el mayor número del conjunto $\{1, 2, 3, \dots, n\}$ que es múltiplo de p es $\left\lfloor \frac{n}{p} \right\rfloor p$.

Demostración: Se puede ver la prueba en la demostración del teorema 3 de [1], pág. 200 ■

Corolario 1.12

Sean n y p son enteros positivos y $p \leq n$, entonces el número de múltiplos de p menores o iguales a n es $\left\lfloor \frac{n}{p} \right\rfloor$.

Demostración: Los múltiplos de p en el conjunto $\{1, 2, 3, \dots, n\}$ son los elementos del conjunto

$$M = \left\{ p, 2p, 3p, \dots, \left\lfloor \frac{n}{p} \right\rfloor p \right\}$$

conjunto cuya cardinalidad es $\left\lfloor \frac{n}{p} \right\rfloor$ ■

1.6 Conclusiones

La interpretación geométrica del máximo común divisor que se vió y la fórmula de Polezzi, no era muy conocida en nuestro medio. La relación de los puntos reticulares y los números primos ha quedado claramente establecida. Esta información será de mucha utilidad para docentes de secundaria y para matemáticos en general.

Se han dado a conocer algunos aspectos fundamentales de la interpretación geométrica de la teoría de la divisibilidad y se han encontrado unas fórmulas, de una extraordinaria belleza, que relacionan a los números primos con la función parte entera y con la secuencia de números triangulares, incluyendo un nuevo test para probar la primalidad de un número.

Bibliografía

- [1] Murillo, M; González, J. (2012), *Teoría de Números*. Editorial Tecnológica de Costa Rica. Segunda edición. Cartago, Costa Rica.
- [2] Polezzi, M. A Geometrical Method for Finding an Explicit Formula for the Greatest Common Divisor. American Mathematical Monthly 104, 445-446, 1997.