Relación del máximo común divisor con los puntos reticulares y algunas de sus consecuencias

BRADDOCK, GEORGE[I]

Costa Rica

Resumen

Existe una estrecha relación entre el máximo común divisor de dos números n y d, con el número de puntos reticulares que están en el segmento que une los puntos $(n, 0)$ y $(0, d)$; cuando representamos esos números en un sistema de coordenadas cartesiano. Usando esa relación, el matemático Marcelo Polezzi, de la Universidad Estatal Paulista (Brasil), establecido en 1997 una fórmula explícita para el máximo común divisor de dos números. Teniendo en cuenta que un número primo es coprimo con todos los enteros menores que él, y usando la fórmula de Polezzi, se demostró un teorema que relaciona a los números primos con la función parte entera y con el polinomio n^3-4n^2+5n-2. En uno de sus corolarios se relacionan los números primos, la función parte entera, los números cuadrados y los triangulares. Ese teorema y sus corolarios servirán como test de primalidad para un número n.

Palabras clave: Máximo común divisor, puntos reticulares, función parte entera, números primos, test de primalidad, números triangulares, números cuadrados, fórmula de Polezzi.

A. Introducción

Los “puntos reticulares”son los puntos con coordenadas $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

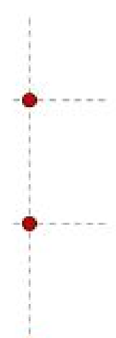

Figure 7: Los puntos reticulares del plano cartesiano.

[I]CUC , Costa Rica

Existe una estrecha relación entre el máximo común divisor de dos números n y d, con el número de puntos reticulares que estánn en el segmento que une los puntos $(n, 0)$ y $(0, d)$ cuando representamos esos números en un sistema de coordenadas cartesiano.

Usando esa relación, el matemático Marcelo Polezzi, de la Universidad Estatal Paulista (Brasil), estableció en 1997 una fórmula explícita para el máximo común divisor de dos números.

Teniendo en cuenta que un número primo es coprimo con todos los enteros menores que él, y usando la fórmula de Polezzi, se demostró un teorema que relaciona a los números primos con la función parte entera y con el polinomio $n^3 - 4n^2 + 5n - 2$.

En uno de sus corolarios se relacionan los números primos, la función parte entera, los números cuadrados y los triangulares.

El teorema se expresa de la siguiente manera: Un número n es primo si y solo si

Ese teorema y sus corolarios servirán como test de primalidad para un número n.

B. Relación MCD-Función parte entera

Relación del mcd con los puntos reticulares

Ejemplo para $n = 15$ y $d = 10$, donde $mcd(15, 10) = 5$

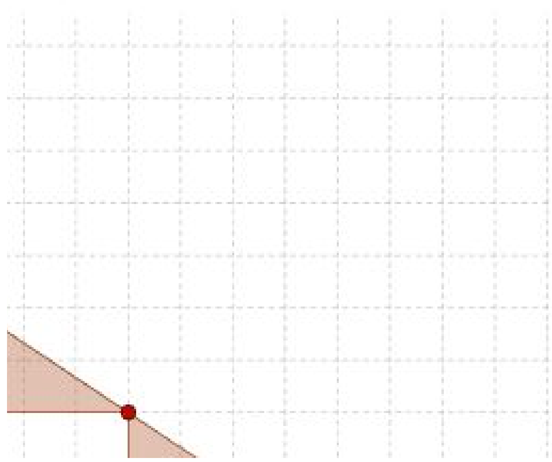

Figure 8: Representación de puntos reticulares.

De acuerdo con la figura anterior, dado que $mcd(15, 10) = 5$ y $\frac{10}{15} = \frac{2}{3}$ hay 5 triángulos rectángulos con catetos de medida 2 y 3, cuya hipotenusa está en la hipotenusa del triángulo ABC, como se muestra en las regiones sombreadas. El número de puntos reticulares en la hipotenusa es igual a $1 + mcd(15, 10) = 1 + 5 = 6$.

En general, si el cateto inferior mide n y el otro cateto mide d, tendremos que la ecuación de la línea que une los puntos $A(n, 0)$ y $B(0, d)$ es:

$$y = d - \frac{a}{b}x \quad \text{donde} \quad a = \frac{d}{mcd(n, d)}, \;\; b = \frac{n}{mcd(n, d)}$$

como puede observarse en la siguiente figura:

Figure 9: Triángulo rectángulo.

La cantidad $\frac{a}{b}x$ será igual a un entero w si se cumple que

$$x = bw$$

La teoría de las ecuaciones diofánticas nos dice que las soluciones de esta ecuación son

$$x = bz \qquad \text{y} \qquad w = az \qquad \text{con} \quad z \in \mathbb{N}$$

Entonces a un valor de x igual al entero bz, le corresponderá un valor de y igual a $d - w$, que será también entero. Por lo tanto el punto (x, y) será un punto reticular que está en la hipotenusa del triángulo rectángulo AOB.

El siguiente teorema relaciona el mcd con los puntos reticulares:


1 (Relación mcd - puntos reticulares).

teros positivos, entonces

Como consecuencia inmediata se tienen los corolarios siguientes:

La fórmula de Polezzi

Figure 10: 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.

Si llamamos $|L|, |K|, |M|$ número de puntos reticulares en la respectiva región, entonces

$$\begin{array}{cc} |L| = n + d + 1 & |K| = \displaystyle\sum_{k=1}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor \\ |M| + |H| = |L| + |K| & |H| = 1 + mcd(n, d) \end{array}$$

y de aquí se puede deducir la relación

$$|M| = n + d - mcd(n,d) + \sum_{k=1}^{n-1} \left\lfloor \frac{dk}{n} \right\rfloor \quad (*1)$$

Por otro lado, a partir de las relaciones

$$2|M| + |H| = (n+1)(d+1) \qquad |H| = 1 + mcd(n,d)$$

se puede deducir la relación

$$|M| = \frac{nd + n + d - mcd(n,d)}{2} \quad (*2)$$

A partir de (*1) y (*2) Polezzi pudo deducir el teorema que sigue.

Relación primos-puntos reticulares

ición # 1 (Definición alternativa de número primo).

nero n es primo si y solo si es coprimo con todos los naturales menores que él.

En la Figura 11 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).

En la Figura 12 se observa que, si $k = mcd(n,d)$ 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).

Figure 11: 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 $0 < d < 7$.

Figure 12: 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 $0 < d < 7$.

Relación primos-función parte entera

Los resultados anteriores permiten establecer la siguiente proposición:

Un entero positivo n es primo si y solo si

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

Simplificando esa fórmula se llega al siguiente teorema:

El teorema anterior puede expresarse de varias formas alternativas, que se muestran en los corolarios que siguen.

Demostración del corolario 5.

El corolario 4, puede expresarse así, debido a las identidades:

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

$$t_{n-2}t_{n-1} == \frac{(n-1)^2[(n-1)-1][(n-1)+1]}{2^2}$$

$$t_{n-2}t_{n-1} = \frac{(n-1)^2[(n-1)^2-1]}{2^2}$$

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

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

Referencias

[1] Polezzi, M. A Geometrical Method for Finding an Explicit Formula for the Greatest Common Divisor. American Mathematical Monthly 104, 445-446, 1997.