Ciencias de la Computación I

Tópicos de Teoría de Números II

Eduardo Contrera Schneider

Universidad de la Frontera

18 de octubre de 2016

Divisor Común

Para $a, b \in Z$, un entero positivo c es un divisor común de a y b si $c|a$ y $c|b$.

Máximo Comun Divisor

Sean $a, b \in \mathbb{Z}$, donde $a \neq 0$ o $b \neq 0$. Entonces $c \in \mathbb{Z}^+$ es el *máximo común divisor* de a, b si

- $c|a$ y $c|b$, y
- para cualquier divisor común d de a y b, tenemos que $d|c$.

Para enteros pequeños no hay dificultad de encontrar el máximo común divisor. Sin embargo, ¿Cómo podemos hacerlo para números más grandes?

Teorema

Para cualesquiera $a, b \in \mathbb{Z}^+$, existe un único $c \in \mathbb{Z}^+$ que es el máximo común divisor de a, b.

De la demostración del teorema anterior podemos ver que el máximo común divir es el entero positivo más pequeño que se puede escribir como combinación lineal de a y b.

Primos Relativos

Los enteros a y b son primos relativos si $mcd(a, b) = 1$.

Como ejemplo, busque las soluciones de la ecuación $42x + 70y = 14$.

Algoritmo de Euclides

Si $a, b \in \mathbb{Z}^+$, el algoritmo de la división se aplica como sigue:

- $a = q_1 b + r_1, \quad con \;\; 0 < r_1 < b$
- $b = q_2 r_1 + r_2, \quad con \;\; 0 < r_2 < r_1$
- $r_1 = q_3 r_2 + r_3, \quad con \;\; 0 < r_3 < r_2$

$\vdots$

- $r_{k-2} = q_k r_{k-1} + r_k, \quad con \;\; 0 < r_k < r_{k-1}$
- $r_{k-1} = q_{k+1} r_k$

entonces el $mcd(a, b) = r_k$, es decir, el último resto distinto de cero.

Ejemplo

- Determine el máximo común divisor entre 250 y 111. Exprese el resultado como combinación de estos enteros.
- Para cualesquiera $n \in \mathbb{Z}^+$, demuestre que los enteros positivos $8n + 3$ y $5n + 2$ son primos relativos.

Ecuaciones Diofánticas

Una ecuación diofántica es una ecuación lineal que requiere soluciones enteras. Para determinar cuándo estas ecuaciones tienen solución, tenemos el siguiente teorema:

Teorema

Si $a, b, c \in \mathbb{Z}^+$, la ecuación diofántica $ax + by = c$ tiene una solución entera $x = x_0$ y $y = y_0$ si y sólo si $mcd(a, b)$ divide a c.

En general, $mcd(a, b) = d$, entonces $mcd(\frac{a}{d}, \frac{b}{d}) = 1$. Si $\frac{a}{d}x_0 + \frac{b}{d}y_0 = 1$, entonces $\frac{a}{d}(x_0 - \frac{b}{d}k) + \frac{b}{d}(y_0 + \frac{a}{d}k) = 1$, para todo $k \in \mathbb{Z}$.

Mínimo Común Múltiplo

Mínimo Común Múltiplo

Si $a, b, c \in \mathbb{Z}^+$, c es un múltiplo común de a, b si c es un múltiplo de a y de b. Además, c es el mínimo común múltiplo de a, b si es el más pequeño de los enteros positivos que son múltiplos comunes de a, b. Denotamos c con $mcm(a, b)$.

Propiedades

- Para cualquier $n \in \mathbb{Z}^+$, tenemos que $mcm(1, n) = mcm(n, 1) = n$.
- Si $a, n \in \mathbb{Z}^+$, tenemos que $mcm(a, na) = na$.
- Si $a, m, n \in \mathbb{Z}^+$ con $m \leq n$, entonces $mcm(a^m, a^n) = a^n$.
- Sean $a, b, c \in \mathbb{Z}^+$, con $c = mcm(a, b)$. Si d es un múltiplo común de a y b, entonces $c|d$.