Ampliación de Matemáticas
Teoría de Números

José Luis Bravo Trinidad

La teoría de números estudia los números naturales o enteros y sus relaciones

Agunos problemas que trata:

1. Calcular las soluciones enteras de una ecuación.
2. Determinar si un número es primo o no y su factorización.
3. Obtener algoritmos que permitan realizar eficientemente operaciones con números naturales.
4. ...

La Teoría de Números surgió en las antiguas civilizaciones al tener que resolver problemas con números enteros. Perdió importancia práctica debido al desarrollo del análisis moderno. Con la computación recuperó su dimensión práctica, pues en última instancia las computadoras sólo trabajan con números enteros.

Aplicaciones:

- Criptografía
- Códigos correctores y detectores de errores
- Tablas hash
- Procesado de señales digitales.

División entera

Teorema (Algoritmo de la División)

Sean $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $b \neq 0$.
Existen $c, r \in \mathbb{Z}$ únicos tales que $a = bc + r$ y $0 \leq r < |b|$.

Demostración.

Consideraremos el caso $a, b > 0$.
En primer lugar, siempre existen $c \geq 0$ y $r \geq 0$ (e.g. $c = 0, r = a$).
Si $r \geq b$, entonces definimos $\bar{r} = r - b \geq 0$ y $\bar{c} = c + 1$ y tenemos

$$a = \bar{b}c + \bar{r}$$

Como $r > \bar{r}$, este proceso lo podemos repetir un número finito de veces. Si no podemos repetirlo, entonces

$$a = bc + r \quad \text{y} \quad 0 \leq r < b.$$

$\square$

Los números a, b, q, r dados por el teorema anterior se denominan **dividendo**, **divisor**, **cociente** y **resto**, respectivamente.

Dados $a, b \in \mathbb{Z}$, $a \neq 0$, decimos que a **divide** a b si el resto al dividir b entre a es cero. También diremos en ese caso que b es **múltiplo** de a. Lo denotamos $a|b$

Ejemplos:

1. 13 divide a 169 ($13|169$), luego 169 es un múltiplo de 13.
2. Los divisores de 91 son 1, 7, 13 y 91.
3. Si n es un número impar, entonces $n^2 = 4k + 1$ para algún k.

Decimos que un número natural $n > 1$ es **primo** si sólo es divisible entre él y la unidad.

Dados, $a, b \in \mathbb{Z}$, $c \in \mathbb{Z}$ es un **divisor común** si c divide a a y a b.
Dados $a, b \in \mathbb{Z}$, el **máximo común divisor** de a y b, $\text{mcd}(a, b)$, es el mayor de los divisores comunes de a y b.
Ejemplo: $\text{mcd}(6, 15) = 3$.

Dados, $a, b \in \mathbb{Z}$, $c \in \mathbb{Z}$ es un **múltiplo común** si c es múltiplo de a y a b.
Dados $a, b \in \mathbb{Z}$, el **mínimo común múltiplo** de a y b, $\text{mcm}(a, b)$, es el menor de los múltiplos comunes positivos de a y b.

Se dice que $a, b \neq 0$ son **primos entre sí** si $\text{mcd}(a, b) = 1$.
Ejemplo: 6 y 35 son primos entre sí, pero 7 y 154 no.

Proposición

Sean $a, b, c \in \mathbb{Z}$ tales que $c|a$ y $c|b$. Entonces $c|ax + by$ para todo $x, y \in \mathbb{Z}$.

Demostración.

Si $c|a$, entonces $a = cd$.

Si $c|b$, entonces $b = ce$.

Para todo $x, y \in \mathbb{Z}$, tenemos

$$ax + by = (cd)x + (ce)y = c(dx + ey).$$

Luego $c|ax + by$. □

En particular, $\mathrm{mcd}(a, b)|ax + by$ para todo $x, y \in \mathbb{Z}$.

Teorema (Identidad de Bézout)

Sean $a, b \in \mathbb{Z}$, $a, b \neq 0$. El máximo común divisor de a y b es el entero positivo d más pequeño que puede expresarse en la forma $d = ax + by$ para algún $x, y \in \mathbb{Z}$.

Demostración.

Para probarlo, veremos que si D es el máximo común divisor de a y b, entonces $D \leq d$ y que también $d \leq D$.

En primer lugar, $D | ax + by = d$, luego $D \leq d$

Por otra parte, definimos

$$\mathcal{S} = \{n \colon n \text{ se puede expresar como } n = ax + by\}.$$

Nótese que $a, b \in \mathcal{S}$.

$\square$

Demostración. (Cont.)

Vamos a probar que $d|n$ para todo $n \in \mathcal{S}$, en particular $d|a$, $d|b$, luego $d \leq D$.

Por reducción al absurdo:

Si $d \not| n$, entonces, $n = cd + r$, con $0 < r < d$. Pero entonces

$$r = n - cd = a\bar{x} + b\bar{y} - c(ax + by) = a(\bar{x} - cx) + b(\bar{y} - cy) \in \mathcal{S},$$

en contradicción con que d es el menor entero positivo de $\mathcal{S}$. □

Corolario

a, b son primos entre sí, si y sólo si existen $x, y \in \mathbb{Z}$ tales que $ax + by = 1$.

Teorema (Algoritmo de Euclides)

Sean $a, b \neq 0$ números enteros. Sea r tal que $a = bc + r$. Entonces

- *Si $r = 0$, entonces $\operatorname{mcd}(a, b) = b$.*
- *Si $r \neq 0$, entonces $\operatorname{mcd}(a, b) = \operatorname{mcd}(b, r)$.*

Para calcular el máximo común divisor de dos números enteros, a, b, utilizaremos el siguiente algoritmo:

1. Dividimos a entre b: $a = bc + r$.
2. Si $r = 0$, entonces devolvemos $\operatorname{mcd}(a, b) = b$.
3. Si $r \neq 0$, entonces $a = b$, $b = r$ y volvemos a 1.

Ejemplo: Calcular el máximo común divisor de 124 y 650.

Teorema (Lemma de Euclides)

Si $c|ab$ y c es primo con a, entonces $c|b$.

Demostración.

Como c es primo con a,

$$\mathrm{mcd}(c, a) = 1.$$

Por la identidad de Bezout existen x e y tales que

$$cx + ay = 1$$

Multiplicando por b,

$$b = cxb + aby.$$

Como c y ab son múltiplos de c, b también. □

Ecuaciones diofánticas

Una **ecuación diofántica** es una ecuación de la forma

$$p(n_1, \ldots, n_m) = 0,$$

donde $p(n_1, \ldots, n_m)$ es un polinomio en las variables $n_1, \ldots, n_m$ y lo que se busca son $n_1, \ldots, n_m \in \mathbb{Z}$ que satisfagan la ecuación.

La ecuación diofántica más sencilla es la lineal con dos variables: Dados $a, b, n \in \mathbb{Z}$, se trata de encontrar todos los $x, y \in \mathbb{Z}$ tales que

$$ax + by = n.$$

En este caso es fácil caracterizar la existencia de soluciones.

Teorema

Sean $a, b, n \in \mathbb{Z}$. La ecuación $ax + by = n$ tiene solución entera si y solo si $mcd(a, b) | n$.

Demostración.

En primer lugar, si la ecuación tiene una solución, es decir, existen x, y tales que $ax + by = n$, entonces, como $d|a$ y $d|b$, $d|ax + by = n$. $\square$

Demostración (Cont.).

Supongamos que $mcd(a,b)|n$. Por la Identidad de Bezout, existen $\bar{x}$ e $\bar{y}$ tales que $a\bar{x}+b\bar{y}=mcd(a,b)$. Entonces, una solución x_0, y_0 de la ecuación lineal será

$$x_0 = \frac{n\bar{x}}{mcd(a,b)}, \quad y_0 = \frac{n\bar{y}}{mcd(a,b)}.$$

□

Ejemplo: Calcular una solución de $6x+10y=8$.
Por el Algoritmo de Euclides calculamos el máximo común divisor y los números que satisfacen la Identidad de Bezout.

$$2 = 2*6 - 1*10$$

Entonces, una solución es:

$$x = 8, \quad y = -4.$$

Teorema

Sean $a, b, n \neq 0$*, si* x_0, y_0 *es una solución de la ecuación* $ax + by = n$*, entonces todas las soluciones son*

$$\{x_0 + k\frac{b}{mcd(a,b)}, y_0 - k\frac{a}{mcd(a,b)} : k \in \mathbb{Z}\}.$$

Demostración.

Sustituyendo, obtenemos las soluciones propuestas cumplen la ecuación. Veamos que no hay más:
Si x_0, y_0 y x_1, y_1 son soluciones y $a = \bar{a}d$, $b = \bar{b}d$, con $d = \mathrm{mcd}(a, b)$, entonces

$$\bar{a}(x_1 - x_0) + \bar{b}(y_1 - y_0) = 0, \quad \text{luego} \quad \bar{a}(x_1 - x_0) = -\bar{b}(y_1 - y_0).$$

Como $\bar{a}, \bar{b}$ son primos entre sí, por el Lema de Euclides, tenemos que $\bar{b}|(x_1 - x_0)$. Luego $x_1 = x_0 - k\bar{b}$ y despejando, $y_1 = y_0 + k\bar{a}$.

Congruencias

Fijado $m \in \mathbb{N}$, diremos que $a, b \in \mathbb{Z}$ son congruentes módulo m si $m|(a-b)$ y lo denotaremos $a \equiv_m b$ ó $a \equiv b \bmod m$.

Teorema

$a \equiv_m b$ si y sólo si a y b tienen el mismo resto al dividir por m.

Teorema

Fijado $m \in \mathbb{N}$, la relación $\equiv_m$ es una relación de equivalencia. Es más, si denotamos como $[n]$ la clase de equivalencia de $n \in \mathbb{N}$, entonces para todo $a \in \mathbb{Z}$ se verifica que

$$a \in [0] \text{ o } a \in [1] \text{ o } \dots \text{ o } a \in [m-1].$$

Fijado $m \in \mathbb{N}$, al conjunto de clases de equivalencia lo denotaremos $\mathbb{Z}/m\mathbb{Z}$.

Teorema

En $\mathbb{Z}/m\mathbb{Z}$ podemos definir las operaciones

$$[a]+[b]=[a+b], \quad [a][b]=[ab].$$

Con las operaciones anteriores $\mathbb{Z}/m\mathbb{Z}$ tiene estructura de anillo (se puede sumar y multiplicar con las propiedades usuales).

Además, si $mcd(a,m)=1$, entonces existe $[b]\in\mathbb{Z}/m\mathbb{Z}$ tal que $[a][b]=1$ ($[b]$ es el inverso de $[a]$).

No se verifica que si $[a][b]=[0]$, entonces $[a]=[0]$ o $[b]=[0]$.

Teorema

Sea $b \geq 2$ un número natural (llamado base), entonces todo número $n \in \mathbb{N}$ puede escribirse de modo único en base b en la forma

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0 b^0,$$

para algún $k \geq 0$, $0 \leq a_i < b$, $i = 1, \ldots, k$ y $a_k \neq 0$.

Si n está expresado en base b como

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0 b^0,$$

lo denotaremos

$$n = (a_k, a_{k-1}, \ldots, a_2, a_1, a_0)_b.$$

Usualmente, si $b \geq 10$ se utilizan letras mayúsculas para denotar las cifras mayores que 9.

Criterios de divisibilidad

Sea n un número natural. Fijado $b \geq 2$, tenemos

$$n = a_m b^m + a_{m-1} b^{m-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0 b^0.$$

Si consideramos su clase de equivalencia en $\mathbb{Z}/k\mathbb{Z}$, tenemos

$$\begin{aligned}[n] &= [a_m b^m + a_{m-1} b^{m-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0 b^0] \\ &= [a_m r_m + a_{m-1} r_{m-1} + \ldots + a_2 r_2 + a_1 r_1 + a_0 r_0],\end{aligned}$$

donde $r_i \equiv_k b^i$ y $0 \leq r_i < k$, $i = 1, \ldots, m$. En particular, n será divisible entre k si y solo si

$$a_m r_m + a_{m-1} r_{m-1} + \ldots + a_2 r_2 + a_1 r_1 + a_0 r_0 \equiv_m 0.$$

Introducción

Teorema

La ecuación $ax \equiv_m b$ tiene solución si y solo si $d = mcd(a, m) | b$.
Si tiene solución, tiene d soluciones, que son

$$x \equiv_m x_0 + (m/d)k, \quad k = 0, 1, \ldots, d-1, (\textit{equiv. } x \equiv_{m/d} x_0),$$

donde $x_0 = (a/d)^{-1}(b/d)$ (nótese que $(a/d)^{-1}$ es el inverso de a/d).

Corolario

Si $mcd(a, m) = 1$, entonces para todo $b \in \mathbb{Z}$ la ecuación $ax \equiv_m b$ tiene solución única en $\mathbb{Z}/m\mathbb{Z}$, $x \equiv_m a^{-1}b$.

Teorema (Teorema Chino del Resto)

Sean m_1 y m_2 primos entre sí. Entonces la ecuación

$$x \equiv_{m_1} b_1, \quad x \equiv_{m_2} b_2$$

tiene solución única en $\mathbb{Z}/m_1 m_2\mathbb{Z}$,

$$x \equiv_{m_1 m_2} b_1 y_1 m_2 + b_2 y_2 m_1,$$

donde y_1 es el inverso de m_2 en $\mathbb{Z}/m_1\mathbb{Z}$ e y_2 es el inverso de m_1 en $\mathbb{Z}/m_2\mathbb{Z}$.

Corolario (Teorema Chino del Resto)

El sistema de congruencias

$$a_i x \equiv_{m_i} b_i, \quad i = 1, \dots, n,$$

donde m_i, m_j *son primos entre sí,* $1 \leq i \neq j \leq n$ *y* a_i, m_i *son primos entres sí,* $i = 1, \dots, n$*, tiene una única solución en* $\mathbb{Z}/m_1 m_2 \dots m_n\mathbb{Z}$*,*

$$x \equiv_{m_1 m_2 \dots m_n} \sum a_i^{-1} b_i y_i M_i,$$

donde y_i *es el inverso de* $M_i = m_1 m_2 \dots m_n / m_i$ *en* $\mathbb{Z}/m_i\mathbb{Z}$*.*

Teorema

Sean m_1 y m_2 números naturales y $d = \operatorname{mcd}(m_1, m_2)$. Si $d|(b_2 - b_1)$ entonces la ecuación

$$x \equiv_{m_1} b_1, \quad x \equiv_{m_2} b_2$$

tiene solución única en $\mathbb{Z}/(m_1 m_2/d)\mathbb{Z}$,

$$x \equiv_{m_1 m_2/d} b_1 + \bar{b}\bar{m}_1^{-1} m_1,$$

donde $\bar{b} = ((b_2 - b_1)/d)$ y $\bar{m}_1^{-1}$ es el inverso de m_1/d en $\mathbb{Z}/m_2\mathbb{Z}$.

Si $n \in \mathbb{N}$ es no nulo, se define el **indicador de Euler** de m y se denota $\phi(m)$, como el número de enteros positivos entre 1 y m que son primos con m.

Para calcular $\phi(m)$ se emplean las siguientes reglas:

1. Si $mcd(a, b) = 1$, entonces $\phi(ab) = \phi(a)\phi(b)$.
2. Si p es un número primo, entonces $\phi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right)$.

Teorema (Teorema de Euler)

Sean a, m enteros con $m \geq 1$. Si $mcd(a, m) = 1$, entonces

$$a^{\phi(m)} \equiv_m 1.$$

Ejemplo: $\phi(8) = \phi(2^3) = 8(1 - 1/2)$ y
$\phi(36) = \phi(2^2 3^2) = 36(1 - 1/2)(1 - 1/3) = 12.$
Comprueba que $a^4 \equiv_8$ para todo número impar en $a\mathbb{Z}/8\mathbb{Z}$.

Corolario (Congruencia de Fermat)

Sea p un número primo. Si un número entero a no es múltiplo de p, entonces

$$a^{p-1} \equiv_p 1.$$

Proposición (Criterio de primalidad)

Un número p es primo si y sólo si para todo $0 < a < p$ se verifica que

$$a^{p-1} \equiv_p 1.$$