Ampliación de Matemáticas
Teoría de Números

La teoría de números estudia los números naturales o enteros y las relaciones entre ellos.

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

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

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

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

□

Los números a, b, c, r se denominan **dividendo**, **divisor**, **cociente** y **resto**, respectivamente.

Dados $a, b \in \mathbb{Z}$, $b \neq 0$, decimos que b **divide** a a (o equivalentemente que b es **divisor** de a) si el resto al dividir a entre b es cero. Lo denotamos $a|b$. En ese caso, también diremos que a es **múltiplo** de b. Denotado como $b = \dot{a}$.

Ejemplos:

1. 13 divide a 169 $(169|13)$, luego 169 es un múltiplo de 13.
2. Los divisores de 91 son 1, 7, 13 y 91.
3. ¿Cuáles son los múltiplos de 3? ¿Y de 9? ¿Y de 11?
4. Si n es un número impar, entonces $n^2 = 4k + 1$ para algún k.

Máximo común divisor

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.

Mínimo común múltiplo

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.

Número primo

Se dice que un número natural $n > 1$ es **primo** si solo tiene como divisores a él y a la unidad.
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 $a|c$ y $b|c$. Entonces $ax + by|c$ para todo $x, y \in \mathbb{Z}$.

Demostración.

Si $a|c$, entonces $a = cd$. Si $b|c$, entonces $b = ce$.
Para todo $x, y \in \mathbb{Z}$, tenemos

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

Luego $ax + by|c$. □

En particular: $ax + by|\operatorname{mcd}(a, b)$ 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 más pequeño que puede expresarse en la forma $d = ax + by$ para algún $x, y \in \mathbb{Z}$.

En particular: a, b son primos entre sí, si y solo 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 $\text{mcd}(a, b) = b$.*
- *Si $r \neq 0$, entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$.*

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 $\text{mcd}(a, b) = b$.
   - Si $r \neq 0$, entonces calculamos $\text{mcd}(b, r)$, que es igual a $\text{mcd}(a, b)$.
3. Repetimos hasta que el resto sea 0.

Ejemplo:

Calcular el máximo común divisor de 312 y 120.

- $312 = 120 * 2 + 72 \Rightarrow mcd(312, 120) = mcd(120, 72)$
- $120 = 72 * 1 + 48 \Rightarrow mcd(120, 72) = mcd(72, 48)$
- $72 = 48 * 1 + 24 \Rightarrow mcd(72, 48) = mcd(48, 24)$
- Finalmente, $mcd(48, 24) = 24 = mcd(312, 120)$.

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

Teorema (Lema de Euclides)

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

Demostración.

Como c es primo con a, entonces $\text{mcd}(c, a) = 1$. 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, entonces b también. □

Ecuaciones diofánticas

Ecuaciones diofánticas

Una **ecuación diofántica** es una ecuación algebraica para la cual buscamos soluciones enteras.
La ecuación diofántica más sencilla es la lineal con dos variables.

Ecuación diofántica lineal

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 $n|mcd(a, b)$.

Demostración.

- En primer lugar, si la ecuación tiene una solución, es decir, existen x, y tales que $ax + by = n$, entonces sabemos que $n|\,\mathrm{mcd}(a, b)$, pues divide a $ax + by$.
- Supongamos que $n|mcd(a, b)$. Entonces, para cierto $\lambda \in \mathbb{Z}$, $n = \lambda\,\mathrm{mcd}(a, b)$. Además, existen $\bar{x}$ e $\bar{y}$ tales que $a\bar{x} + b\bar{y} = \mathrm{mcd}(a, b)$. Entonces, una solución de la ecuación lineal será

$$x = \lambda\bar{x}, \quad y = \lambda\bar{y}$$

Algoritmo de Euclides Extendido

Este algoritmo nos permite calcular los valores (x, y) de la Identidad de Bézout. Consiste en aplicar el algoritmo de Euclides, y sustituir sucesivamente el resto en las ecuaciones que se obtienen.

Ejemplo

Calcular x, y tales que $312x + 120y = \text{mcd}(312, 120)$

- $312 = 120 * 2 + 72 \Rightarrow 72 = 312 + (-2) * 120$
- $120 = 72 * 1 + 48 \Rightarrow 48 = 120 + (-1) * 72$
- $72 = 48 * 1 + 24 \Rightarrow 24 = 72 + (-1) * 48$
- $mcd(48, 24) = 24$, con lo que $312x + 120y = 24$

$24 = 72 + (-1) * 48 = 72 + (-1) * (120 + (-1) * 72) = 2 * 72 - 120 =$
$= 2 * (312 - 2 * 120) - 120 = 2 * 312 - 5 * 120$
La solución es: $x = 312, \quad y = -5$

Algoritmo de Euclides Extendido

Calcular una solución de la ecuación diofántica $ax + by = n$

- Paso 1. Comprobar si la ecuación diofántica tiene solución. En caso afirmativo, se puede resolver la ecuación diofántica.
- Paso 2. Aplicar el Algoritmo de Euclides para encontrar una solución de la Identidad de Bézout: $a\bar{x} + b\bar{y} = \mathrm{mcd}(a, b)$
- Paso 3. Sabemos que $n = c\,\mathrm{mcd}(a, b)$, de modo que multiplicando por c la Identidad de Bézout obtenemos la Ecuación diofántica:

$$a(c\bar{x}) + b(c\bar{y}) = c\,\mathrm{mcd}(a, b) \Rightarrow ax + by = n$$

donde una solución de la ecuación diofántica es

$$x = c\bar{x}, \quad y = c\bar{y}$$

Teorema

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

$$x = x_0 + k\frac{b}{mcd(a,b)}, \quad y = y_0 - k\frac{a}{mcd(a,b)}, \quad \text{con } k \in \mathbb{Z}$$

A x_0, y_0 se les llama soluciones particulares, y a x, y soluciones generales de la ecuación diofántica.

Congruencias

Congruencia

Fijado $m \in \mathbb{N}$, diremos que $a, b \in \mathbb{Z}$ son **congruentes módulo** m si $(a-b)|m$, o, equivalentemente, si a y b tienen el mismo resto al dividir por m. Lo denotamos como $a \equiv_m b$ o bien $a \equiv b \bmod m$.

Por ejemplo, $5 \equiv_4 1$, $6 \equiv_4 2$, $7 \equiv_4 3$, $8 \equiv_4 0$.

Relación de equivalencia

Fijado $m \in \mathbb{N}$, la relación $\equiv_m$ es una relación de equivalencia. Denotamos como $[n]$ la clase de equivalencia de $n \in \mathbb{N}$, y el conjunto de clases de equivalencia lo denotaremos $\mathbb{Z}/m\mathbb{Z}$.

Por ejemplo, si $m = 4$,

$$\mathbb{Z}/4\mathbb{Z} = \{[0], [1], [2], [3]\}$$

El número $5 \in [1] = \{1, 5, 9, 13, \ldots, -3, -7, -11, \ldots\}$

Aritmética modular

Para $m \in \mathbb{Z}$, se tiene el conjunto de clases de equivalencia $\mathbb{Z}/m\mathbb{Z}$, de tal forma que para todo $a \in \mathbb{Z}$, se verifica que

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

Suma en $\mathbb{Z}/m\mathbb{Z}$

Dados $[a], [b] \in \mathbb{Z}/m\mathbb{Z}$, se define la suma como:

$$[a] + [b] = [a + b]$$

con las siguientes propiedades:

- $[a] + [b] = [b] + [a], \quad [a] + ([b] + [c]) = ([a] + [b]) + [c]$
- $[a] + [0] = [a], \quad [a] + [-a] = [0]$

Aritmética modular

Producto en $\mathbb{Z}/m\mathbb{Z}$

Dados $[a], [b] \in \mathbb{Z}/m\mathbb{Z}$, se define el producto como:

$$[a] \cdot [b] = [ab]$$

con las siguientes propiedades:

- $[a] \cdot [b] = [b] \cdot [a], \quad [a] \cdot ([b] \cdot [c]) = ([a] \cdot [b]) \cdot [c]$
- $[a] \cdot [1] = [a], \quad [a] \cdot ([b] + [c]) = [a] \cdot [c] + [b] \cdot [c]$

¡Ojo!

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

Aritmética modular

Inverso en $\mathbb{Z}/m\mathbb{Z}$

Si $\text{mcd}(a, m) = 1$, entonces existe el inverso de $[a]$ en $\mathbb{Z}/m\mathbb{Z}$, esto es, existe $[b]$ tal que $[a] \cdot [b] = [1]$.
Si m es primo, entonces existen los inversos de todos los elementos de $\mathbb{Z}/m\mathbb{Z}$

Ejemplos en $\mathbb{Z}/4\mathbb{Z} = \{[0], [1], [2], [3]\}$

- Comprobar que $[2] + [3] = [1]$
- Comprobar que $[1] + [-1] = [0]$
- Comprobar que $[1][3] = [3], \quad [2][3] = [2]$
- Comprobar que $[2][2] = [0]$
- ¿Existe una clase $[x]$ que cumpla que $[3][x] = [1]$?, esto es, ¿existe el inverso de $[3]$?
- ¿Existe una clase $[x]$ que cumpla que $[2][x] = [1]$?, esto es, ¿existe el inverso de $[2]$?
- Escribir las tablas de multiplicar en $\mathbb{Z}/4\mathbb{Z}$

Ejemplos

- Calcular 3^2 módulo 5, 3^4 módulo 5 y 3^8 módulo 5.
- Calcular 12^{26} módulo 23.
- Calcular la letra de tu DNI. Basta calcular el número módulo 23 y usar:

RESTO	0	1	2	3	4	5	6	7	8	9	10	11
LETRA	T	R	W	A	G	M	Y	F	P	D	X	B

RESTO	12	13	14	15	16	17	18	19	20	21	22
LETRA	N	J	Z	S	Q	V	H	L	C	K	E

Ecuaciones en congruencias

Ecuación en congruencias lineal

Dados $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, se define una **ecuación en congruencias lineal** como

$$ax \equiv_m b$$

cuya solución es $x \in \mathbb{Z}/m\mathbb{Z}$.

Ejemplos

- $3x \equiv_4 1$
- $2x \equiv_5 3$
- $2x \equiv_8 2$

Ecuaciones en congruencias

Teorema

La ecuación $ax \equiv_m b$ *tiene solución si y solo si* $b|mcd(a,m) = d$. *Si tiene solución, podemos encontrarla resolviendo:*

$$(a/d)x \equiv_{m/d} b/d$$

y buscando el inverso de a/d *módulo* m/d. *Así,*

$$x_0 = (a/d)^{-1}(b/d)$$

Tiene exactamente d *soluciones, que son*

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

Ecuaciones en congruencias

Corolario

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

$$x \equiv_m a^{-1}b$$

Ejemplo

- $2x \equiv_{10} 6$
- $6x + 3 \equiv_1 01$
- $3x \equiv_{19} 1$

Sistemas de Ecuaciones en Congruencias Lineales

Teorema (Teorema Chino del Resto)

Sean $m_1, m_2, \ldots, m_n$ primos entre sí. Entonces el sistema

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

tiene solución única módulo $m = m_1 m_2 \cdots m_n$,

$$x \equiv_m b_1 M_1 y_1 + b_2 M_2 y_2 + \cdots + b_n M_n y_n$$

donde $y_1, y_2, \ldots, y_n$ son los inversos de $M_1, M_2, \ldots, M_n$ módulo m_k, $M_k = m/m_k$

Sistemas de Ecuaciones en Congruencias Lineales

Ejemplo: Sea el sistema de ecuaciones en congruencias $x \equiv_5 3,\ x \equiv_3 0$

- El Teorema Chino de los Restos permite deducir que tiene solución única módulo 15, tal que

$$x \equiv_{15} 3M_1y_1 + 0M_2y_2 \equiv_{15} 3M_1y_1$$

  donde $M_1 = 15/5 = 3$, e y_1 su inverso en módulo $m_1 = 5$.
- Se debe determinar y_1, para ello basta resolver la ecuación en congruencias $M_1y_1 \equiv_{m_1} 1$, esto es, $3y_1 \equiv_5 1$.
- Para resolverla, utilicemos la Identidad de Bézout: $3y_1 + 5z = 1$.
- $y_1 = 2$
- Luego, la solución es $x \equiv_{15} 3 \cdot 3 \cdot 2 = 18 \equiv_{15} 3$

Corolario (Teorema Chino del Resto)

El sistema de congruencias

$$a_1x \equiv_{m_1} b_1, \quad a_2x \equiv_{m_2} b_2, \cdots \quad a_nx \equiv_{m_n} b_n$$

donde los módulos m_i son primos entre sí, y para cada ecuación, a_i, m_i son primos entre sí, tiene una única solución módulo $m = m_1m_2 \ldots m_n$,

$$x \equiv_m a_1^{-1}b_1M_1y_1 + a_2^{-1}b_2M_2y_2 + \cdots + a_n^{-1}b_nM_ny_n$$

donde y_i , a_i^{-1} son los inversos de M_i y a_i módulo m_i, respectivamente.

Por ejemplo, resolver

$$\begin{aligned} 3x + 9 &\equiv_5 2 \\ 2x - 5 &\equiv_3 1 \end{aligned}$$

Bases

Teorema

Sea $b \geq 2$ un número natural (llamado base). 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 $a_k \neq 0$.

Lo denotaremos

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

donde las comas pueden ser omitidas si no inducen a confusión

Bases

- Los coeficientes a_i se asocian a los elementos de $\mathbb{Z}/b\mathbb{Z} = \{[0], [1], ..., [b-1]\}$.
- Cuando $b > 10$, se utilizan letras mayúsculas para denotar las cifras mayores que 9. Por ejemplo, en base 11, los coeficientes podrán ser $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A\}$, donde A representa el valor 10.
- Si estamos en base 10, los valores $a_0, a_1, \ldots, a_k$ no son más que las cifras del número.

Ejemplos:

- $5_{10} = (101)_2$
- $7_{10} = (12)_5$
- $111_{10} = (A1)_{11}$
- $15342_{10} = (6CA2)_{13}$

Criterios de divisibilidad

Para cualquier número natural n, expresado en cierta base $b \geq 2$, podremos definir los **criterios de divisibilidad** por m.
En primer lugar, tenemos que

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

En $\mathbb{Z}/m\mathbb{Z}$,

$$n \equiv_m a_k r_k + a_{k-1} r_{k-1} + \ldots + a_1 r_1 + a_0 r_0$$

donde $r_i \equiv_m b^i$.
En particular, n será divisible entre m si y solo si

$$a_k r_k + a_{k-1} r_{k-1} + \ldots + a_1 r_1 + a_0 r_0 \equiv_m 0$$

Algunos criterios de divisibilidad

1. Obtener los criterios de divisibilidad por 4 para un número expresado en base 10.
2. Obtener los criterios de divisibilidad por 11 para un número expresado en base 10.
3. Obtener los criterios de divisibilidad por 14 para un número de cuatro cifras expresado en base 10.

Indicador de Euler

Indicador de Euler

Dado un número natural m 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.

Ejemplo: $\phi(8) = 4, \quad \phi(5) = 4.$

Algunas propiedades:

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

De ese modo,

$$\phi(36) = \phi(2^2 3^2) = 36(1 - 1/2)(1 - 1/3) = 12$$

Teorema (Teorema de Euler)

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

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

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

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

Ejemplos

1. Para cualquier número impar a, resulta que $a^4 \equiv_8 1$. ¿Por qué?
2. Para calcular restos de números grandes, como 3^{34291} módulo 5, basta tener en cuenta que, como 3 y 5 son primos entre sí,

$$3^{\phi(5)} = 3^4 \equiv_5 1$$

Pasamos a módulo 4 el número $34291 \equiv_4 3$. Así,

$$3^{34291} = 3^3 3^{4k} \equiv 3^3 \equiv_5 2$$

3. Calcula el resto de dividir 23^{84292} entre 7.