Teoría de Números

Matemática Discreta
Informatika fakultatea
Donostia

Teoría de Números. Números enteros.

- Conjunto de Números enteros: $\mathbb{Z}$
- En el conjunto $\mathbb{Z}$ la suma, la resta y la multiplicación son operaciones internas, es decir, el conjunto $\mathbb{Z}$ es cerrado para esas operaciones. $\forall x, y \in \mathbb{Z} \Rightarrow \; x + y,\; x - y,\; x \cdot y \in \mathbb{Z}$, pero no para la división. Por ejemplo: $2, 3 \in \mathbb{Z}$, pero $\frac{2}{3} \notin \mathbb{Z}$.
- Teoría de Números: Es la rama de las matemáticas que estudia la división entre enteros.
  - Números enteros positivos: $\mathbb{Z}^+ = \{x \in \mathbb{Z} : x > 0\}$
  - Números enteros negativos: $\mathbb{Z}^- = \{x \in \mathbb{Z} : x < 0\}$
  - $\mathbb{Z} = \mathbb{Z}^+ \cup \mathbb{Z}^- \cup \{0\}$
- $\leq$ relación de orden total: El conjunto $\mathbb{Z}$ está totalmente ordenado, $\forall x, y \in \mathbb{Z} \quad x \leq y$ ó $y \leq x$
- Principio de buen orden: Cualquier subconjunto no vacio de $\mathbb{Z}^+$ tiene un elemento mínimo

Divisibilidad. Números primos

Definición (Divisibilidad)

Dados $a, b \in \mathbb{Z}$ con $a \neq 0$, diremos que a divide a b y lo representamos con la notación $a|b$, si $\exists k \in \mathbb{Z}$ que cumple $b = ka$. Diremos que a es divisor de b y b es múultiplo de a.

En consecuencia: Dados $a, b \in \mathbb{Z}^+$, $a|b \Rightarrow a \leq b$

Teorema (Propiedades de la divisibilidad)

Dados $a, b, c \in \mathbb{Z}$,

1. $1 \mid a; \quad a \mid a; \quad a \mid 0.$ $\qquad (a \neq 0)$
2. $(a \mid b) \wedge (b \mid a) \Rightarrow a = b \vee a = -b.$ $\qquad (a \neq 0, b \neq 0)$
3. $(a \mid b) \wedge (b \mid c) \Rightarrow a \mid c.$ $\qquad (a \neq 0, b \neq 0)$
4. $a \mid b \Rightarrow (\forall x \in \mathbb{Z})\ a \mid xb.$ $\qquad (a \neq 0)$
5. $(a \mid b) \wedge (a \mid c) \Rightarrow (\forall x, y \in \mathbb{Z})\ a \mid xb + yc$ $\qquad (a \neq 0)$
   $a \mid b_i \Rightarrow \forall x_i \in \mathbb{Z} \quad a \mid x_1 b_1 + \cdots + x_n b_n, \quad i = 1, \cdots, n$

Divisibilidad. Números primos

Definición (Número primo)

Sea $n \in \mathbb{Z}^+$, $n > 1$. Diremos que n es un número primo si sus únicos divisores positivos son n y 1:
$m \mid n, \quad m \in \mathbb{Z}^+ \implies m = 1 \vee m = n.$
si n no es un número primo diremos que es compuesto:
$\exists m_1, m_2 \in \mathbb{Z}^+$ non $n = m_1 m_2, \quad 1 < m_1 < n,\ 1 < m_2 < n.$

Teorema

Todo número compuesto tiene algún divisor primo.

$$n \in \mathbb{Z}^+, n > 1, n \text{ compuesto } \implies \exists p \in \mathbb{Z}^+,\ p \text{ primo y } p \mid n.$$

Teorema (Euklides, Elementuak, IX, 20)

Hay infinitos números primos.

División Euclidiana

Teorema (División Euclidiana)

Dados $a, b \in \mathbb{Z}$, con $b > 0$,

$$\exists \mid q \in \mathbb{Z} \quad \exists \mid r \in \mathbb{Z} \quad \text{donde} \quad a = qb + r \text{ con }, \ 0 \leq r < b;$$

q es el cociente, r es el resto, a es el dividendo y b es el divisor.

Definición (Divisor común)

Sean $a, b \in \mathbb{Z}$ y sea $c \in \mathbb{Z}^+$. Diremos que el número c es un divisor común de a y b si se cumple que $c \mid a$ y $c \mid b$.

Máximo Común Divisor

Definición (Máximo Común Divisor, $mcd(a,b)$)

Sean $a, b \in \mathbb{Z}$, $a \neq 0$ ó $b \neq 0$, y sea $d \in \mathbb{Z}^+$. Diremos que el número d es el máximo común divisor de a y b, $mcd(a,b)$, si

1. d es un divisor común de a y b:

$$d \mid a \ \text{y} \ d \mid b;$$

2. cualquier otro divisor común de a y b divide a d:

$$(\forall c \in \mathbb{Z}^+) \quad c \mid a, \quad c \mid b \Rightarrow c \mid d.$$

Teorema

Dados $a, b \in \mathbb{Z}^+$, el máximo común divisor de a y b existe y es único.

Máximo Común Divisor

Propiedades.

1. $mcd(b, a) = mcd(a, b)$.
2. $mcd(0, 0)$ no está definido.
3. Siendo $a \in \mathbb{Z}$, $a \neq 0$, $mcd(a, 0) = \mid a \mid$.
4. Dados $a, b \in \mathbb{Z}$, siempre habrá $mcd(a, b)$ (excepto cuando $a = b = 0$). $mcd(a, b) = mcd(\mid a \mid, \mid b \mid)$
5. Identidad de Bezout (lema de Bezout). Dados $a, b \in \mathbb{Z}$, $a \neq 0$ ó $b \neq 0$, $\exists x, y \in \mathbb{Z}$ con $mcd(a, b) = xa + yb$. Además, $mcd(a, b)$ es el número entero positivo más peque no que se puede expresar como combinación lineal de a y b.

$$mcd(a, b) = \text{mín}\{xa + yb \,:\, x, y \in \mathbb{Z} \text{ y } xa + yb > 0\}.$$

6. Los coeficientes de la combinación lineal no son únicos. Si tenemos $mcd(a, b) = xa + yb$,
   $mcd(a, b) = (x + pb)a + (y - pa)b$, $p \in \mathbb{Z}$

Máximo Común Divisor

Definición

Dados $a, b \in \mathbb{Z}$, diremos que los números a, b son números primos relativos si $mcd(a, b) = 1$.

Consecuencia.

$a, b \in \mathbb{Z}$

a, b primos relativos $\iff \exists x, y \in \mathbb{Z}$ de forma que $xa + yb = 1$.

En general, $d = xa + yb, \quad x, y \in \mathbb{Z} \implies d \geq mcd(a, b)$.

Cálculo del máximo común divisor.

$a, b \in \mathbb{Z}^+$, con $b < a$, $b \mid a \implies mcd(a, b) = b$.

En general, necesitamos un método para calcular el $mcd(a, b)$ de los números $a, b \in \mathbb{Z}^+$: algoritmo de Euclides.

Algoritmo de Euclides

- El algoritmo de Euclides se usa para calcular el $mcd(a, b)$ de los números $a, b \in \mathbb{Z}^+$.
- Gracias a la división Euclidiana sabemos que: dados $a, b \in \mathbb{Z}$, con $b > 0$, $\exists \mid q \in \mathbb{Z}$ (cociente) $\exists \mid r \in \mathbb{Z}$ (resto) tales que $a = qb + r$, $0 \leq r < b$.

En consecuencia,

$$\begin{aligned}
a &= q_1 b + r_1, & 0 < r_1 < b \\
b &= q_2 r_1 + r_2, & 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2 \\
&\vdots & \vdots \\
r_i &= q_{i+2} r_{i+1} + r_{i+2}, & 0 < r_{i+2} < r_{i+1} \\
&\vdots & \vdots
\end{aligned}$$

Algoritmo de Euclides

Realizaremos las siguientes divisiones:

$$\begin{array}{r|l} a & \underline{\; b \;} \\ r_1 & q_1 \end{array} \qquad a = q_1 b + r_1, \qquad 0 < r_1 < b;$$

$$\begin{array}{r|l} b & \underline{\; r_1 \;} \\ r_2 & q_2 \end{array} \qquad b = q_2 r_1 + r_2, \qquad 0 < r_2 < r_1;$$

$$\begin{array}{r|l} r_1 & \underline{\; r_2 \;} \\ r_3 & q_3 \end{array} \qquad r_1 = q_3 r_2 + r_3, \qquad 0 < r_3 < r_2;$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\begin{array}{r|l} r_i & \underline{\; r_{i+1} \;} \\ r_{i+2} & q_{i+2} \end{array} \qquad r_i = q_{i+2} r_{i+1} + r_{i+2}, \qquad 0 < r_{i+2} < r_{i+1};$$

$$\vdots \qquad \vdots \qquad \vdots$$

Algoritmo de Euclides

El resto cada vez es menor, en algún momento obtendremos 0 como resto:

$$\begin{array}{r|l} r_{k-1} & \underline{\quad r_k \qquad\qquad} \\ 0 & \; q_{k+1} \end{array} \qquad r_{k-1} = q_{k+1} r_k + 0;$$

Por lo tanto,

$$b > r_1 > r_2 > \cdots > r_{k-1} > r_k > 0 \; (= r_{k+1}).$$

$mcd(a, b)$ de los números $a, b \in \mathbb{Z}^+$: es el último resto que no es 0 en el proceso previo.

$$\boxed{mcd(a, b) = r_k}$$

Nota: gracias al algoritmo de Euclides, el máximo común divisor de los números a y b se puede expresar como combinación lineal de a y b, ya que vamos a calcular los coeficientes de la combinación lineal.

Mínimo Común Múltiplo

Definición (Múltiplo común)

Sean $a, b, c \in \mathbb{Z}^+$, diremos que el número c es un múltiplo común de los números a y b si $a \mid c$ y $b \mid c$.

Definición (Mínimo Común Múltiplo)

Sean $a, b, m \in \mathbb{Z}^+$. diremos que el número m es el mínimo común múltiplo de los números a y b si m es el múltiplo común más pequeño de a y b:

1. el número m es un múltiplo común de los números a y b.

$$a \mid m \text{ y } b \mid m.$$

2. cualquier múltiplo común de los números a y b es mayor o igual a m.

$$(\forall c \in \mathbb{Z}^+) \quad a \mid c, \quad b \mid c \Rightarrow m \leq c.$$

Mínimo Común Múltiplo

Teorema
Dados $a, b, m \in \mathbb{Z}^+$, si $m = mcm(a, b)$, cualquier múltiplo común de a y b es múltiplo de m:

$$(\forall c \in \mathbb{Z}^+) \quad a \mid c, \quad b \mid c \Rightarrow m \mid c.$$

Teorema
Dados $a, b \in \mathbb{Z}^+$,

$$ab = mcm(a, b) \cdot mcd(a, b).$$

Gracias a este teorema podremos calcular $mcm(a, b)$.

Teorema fundamental de la aritmética

Hemos visto que todo número compuesto tiene al menos un divisor primo. Podemos profundizar en dicho resultado; en el libro IX de **Los Elementos** de Euclides aparece el siguiente teorema:

Teorema (Teorema fundamental de la aritmética)

Dado cualquier $n \in \mathbb{Z}^+$, $n > 1$, n es primo ó n puede escribirse como multiplicación de números primos de una única manera, sin tener en cuenta el orden de los factores (si n es primo él mismo es el único factor)

Teorema fundamental de la aritmética

En la demostración del teorema funcamental de la aritmética suelen utilizarse los siguientes lemas:

Lema

Dados $a, b, p \in \mathbb{Z}^+$, siendo p primo,

$$p \mid ab \Longrightarrow (p \mid a) \text{ ó } (p \mid b).$$

Lema

Dados $a_1, \ldots, a_n, p \in \mathbb{Z}^+$, siendo p primo,

$$p \mid a_1 a_2 \cdots a_n \Longrightarrow p \mid a_j \text{ para algún } j \in \{1, \cdots, n\}.$$

Bibliografia

- Wikipedia.
  https://es.wikipedia.org/wiki/Teoría_de_números
  https://es.wikipedia.org/wiki/Teorema_fundamental_de_la_aritmética
  https://es.wikipedia.org/wiki/Números_coprimos
  https://es.wikipedia.org/wiki/Factorización_de_enteros
  https://es.wikipedia.org/wiki/Máximo_común_divisor
  https://es.wikipedia.org/wiki/Mínimo_común_múltiplo
  https://es.wikipedia.org/wiki/División_euclídea
  https://es.wikipedia.org/wiki/Algoritmo_de_Euclides
  https://es.wikipedia.org/wiki/Identidad_de_Bezout
  https://es.wikipedia.org/wiki/División_por_tentativa
  https://es.wikipedia.org/wiki/Test_de_primalidad
  https://es.wikipedia.org/wiki/Criba_de_Eratóstenes
  https://es.wikipedia.org/wiki/Geometría_euclidiana
- Wikipedia: Los Elementos de Euclides.
  https://es.wikipedia.org/wiki/Elementos_de_Euclides