Divisibilidad en $\mathbb{Z}$

Büten Zar
Bruno Szilagyi

Teorema de la división entera: Dados $a \in \mathbb{N}$ y $b \in \mathbb{Z}$. $\boxed{b = aq + r}$ $0 \leq r < a$

Definición: $a, b \in \mathbb{Z}$, $a \neq 0$ $\boxed{b = \dot{a} \iff b = a.q}$ $q \in \mathbb{Z}$

Propiedad: si $a | b$ y $a > 0$ $b \neq 0$ $\Rightarrow \boxed{0 < a \leq |b|}$

Número primo: $p \in \mathbb{N}$, $p \neq 1$ lo és si tiene en $\mathbb{N}$ solo los 2 divisores triviales.

Propiedades:

1. $\left.\begin{matrix} a|b \\ b|c \end{matrix}\right\} \Rightarrow a|c$

2. $\left.\begin{matrix} a|b \\ a|c \end{matrix}\right\} \Rightarrow a|b+c$

3. $\left.\begin{matrix} a|b \\ n \in \mathbb{Z} \\ n \neq 0 \end{matrix}\right\} \Rightarrow a.n | b.n$

4. $a|b \Rightarrow a|b.n$

Teorema (H) $\begin{matrix} a|b \\ a|c \end{matrix}$ $x, y \in \mathbb{Z}$ (T) $a | bx + cy$

MCD: Se llama máximo común divisor de a y b al mayor de los divisores comunes de a y b.

IDentidad de Bezout

Si $a, b \in \mathbb{N}$, $\exists x, y \in \mathbb{Z}$ / $MCD(a,b) = xa + yb$

Números coprimos: a y b son si $MCD(a,b) = 1$

Propiedades de MCD(a,b)

1. $MCD(a,b)$ es único

2. Sea $a' = \frac{a}{MCD(a,b)}$ y $b' = \frac{b}{MCD(a,b)}$ $\Rightarrow MCD(a', b') = 1$

3. $MCD(a,b) = MCD(b, r_0)$

4. si $d|a$ y $d|b$ $\Rightarrow$ $d \mid MCD(a,b)$

5. $\forall n \in \mathbb{N}$ $\quad MCD(a.n, b.n) = n . MCD(a,b)$

6. $\left.\begin{array}{l} a = a'.d \\ b = b'.d \\ a' \text{ y } b' \text{ son coprimos} \end{array}\right\} \Rightarrow d = MCD(a,b)$

Obs:
- $MCD(a,b) = MCD(|a|, |b|)$
- $MCD(0,b) = |b| = MCD(b,0)$
- $MCD(0,0)$ $\nexists$

mcm(a,b): es el menor natural que es $\dot{a}$ y $\dot{b}$.

Teorema: $mcm(a,b)$ $\exists$ y es único.

Obs:
- $mcm(a,b) = mcm(|a|, |b|)$
- $mcm(a,b) = 0$ (si $a=0$ y/o $b=0$)

Propiedades de mcm (a,b)

1. $\boxed{\left.\begin{array}{l} a|c \\ b|c \end{array}\right\} \Rightarrow mcm(a,b) \mid c}$

2. $\boxed{\dfrac{mcm(a,b)}{a} \text{ y } \dfrac{mcm(a,b)}{b} \text{ son coprimos}}$

3. $\boxed{MCD(a,b) . mcm(a,b) = a.b}$

4. $\boxed{mcm(n.a, n.b) = n . mcm(a,b)}$

Algoritmo de Euclides extendido

Todos los restos del algoritmo de Euclides se pueden "despejar" quedando escritos como CL de coeficientes enteros de a y b.

$MCD(765, 60)$: $\quad 765 = 60.15 + 45 \rightarrow 60 = 45.1 + 15 \longrightarrow 45 = 15.3 + 0$

$$MCD(765, 60) = 15 = x\,765 + y\,60$$

Lema de Euclides: sean $a, b \in \mathbb{N}$ Si p es primo y $p | ab \longrightarrow p | a$ o $p | b$

Corolario: Si $n | a.b$ y $MCD(a, n) = 1 \implies n | b$

Ecuaciones diofánticas lineales

$$\boxed{ax + by = c}$$

Pasos: ① Test de incompatibilidad

Hallo $MCD(a,b) = d$

Si $c \neq \dot{d} \implies$ la ecuación es incompatible

si $c = \dot{d} \implies c = d.k$, hallo $k = \frac{c}{d}$

② Identidad Bezout

Por la IB $\exists$ enteros x_0 e y_0 / $d = x_0 a + y_0 b$. Hallo x_0 e y_0 usando el algoritmo de Euclides extendido.

③ Solución particular

$$\underset{\text{paso 1}}{c = d.k} = \underset{\text{paso 2}}{(x_0 a + y_0 b) k} = a\underbrace{(x_0 k)}_{x_1} + b\underbrace{(y_0 k)}_{y_1} \implies a x_1 + b y_1 = c$$ (x_1, y_1) es sol particular

$$\boxed{\begin{array}{l} x_1 = x_0 . k \\ y_1 = y_0 . k \end{array}}$$

④ Solución general

$$\boxed{\begin{array}{l} y = y_1 + h . a' \\ x = x_1 - h . b' \end{array}}$$ $a' = \frac{a}{d}$ $b' = \frac{b}{d}$

Obs: esto es si la diofántica es de la forma $ax + by = c$.
Si fuera $ax - by = c$

$y = y_1 + h a'$

$x = x_1 + h . b'$

Corolario (Lema Euclides): (p y q primos) si $p | q^m$ para algún $m \in \mathbb{N} \implies p = q$

Corolario: ($p, q_1, \dots, q_n$ son primos) ($m_1, \dots, m_h$ son naturales) si $p | q_1^{m_1} . q_2^{m_2} \cdots q_h^{m_h} \implies p$ es igual a algún q_i

Definición: Sea $n \in \mathbb{N}$

$n = 1$ " La factorización en números primos de n es vacía "

$n \geq 2$: n es primo $n = p$ $\boxed{n = p^1}$ La factorización de n en factores primos es p^1

n no es primo $\boxed{n = p_1^{m_1} p_2^{m_2} \dots p_h^{m_h}}$

Teorema fundamental de la aritmética.

Para todo $n \geq 2$ natural, $\exists !$ y es única (a menos del orden de los factores) la factorización de n en números primos.

Teorema: Existen infinitos números primos.

Teorema: Si $n \in \mathbb{N}$, $n \geq 2$ y no es primo $\Rightarrow \exists$ algún divisor primo p de n / $p \leq \sqrt{n}$

Teorema: Sean $a, b \in \mathbb{N}$, $a, b \geq 2$

El $MCD(a,b)$ tiene como factorización en números primos a todos los factores primos comunes a las factorizaciones de a y b, repetido la menor cantidad de veces que aparece en las dos descomposiciones.

Teorema: Sean $a, b \in \mathbb{N}$ $a, b \geq 2$

El $mcm(a,b)$ tiene como factorización en números primos al producto de todos los factores primos de a y b y cada uno de ellos aparece repetido la mayor cantidad de veces que aparece en las factorizaciones de a y de b.

No tiene porqué ser común a ambas factorizaciones.

Propiedades: sea $n \in \mathbb{N}$

$n = p_1^{n_1} \cdot p_2^{n_2} \dots p_h^{n_h} \Rightarrow n^2 = p_1^{2n_1} \dots p_h^{2n_h}$ → Los exponentes son pares

$n^3 = p_1^{3n_1} \dots p_h^{3n_h}$ → Los exponentes son $\dot{3}$

$\#$ divisores $(n) = (n_1+1)(n_2+1)\dots(n_h+1)$

$\boxed{n \text{ es un cuadrado perfecto} \Leftrightarrow \# \text{ divisores}(n) \text{ es impar.}}$

Büten Zar
Bruno Szilagyi

Congruencias

Definición:

$$\boxed{a \equiv b \pmod{n} \iff n \mid a-b}$$

$n \in \mathbb{Z}$ (fijo)
$a, b \in \mathbb{Z}$

Propiedades

1) $\boxed{\text{Si } a = qn + r \Rightarrow a \equiv r \pmod{n}}$

2) $\left.\begin{array}{l} a = q_1 n + r_1 \\ b = q_2 n + r_2 \end{array}\right\} \Rightarrow \boxed{a \equiv b \bmod_n \iff r_1 = r_2}$

3) La congruencia módulo n es una relación de equivalencia

Reflexiva: $\boxed{a \equiv a \pmod{n}}$

Simétrica: $\boxed{a \equiv b \pmod{n} \iff b \equiv a \pmod{n}}$

transitiva: $\boxed{\left.\begin{array}{l} a \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{array}\right\} \Rightarrow a \equiv c \pmod{n}}$

4) $\boxed{\left.\begin{array}{l} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array}\right\} \Rightarrow a + c \equiv b + d \pmod{n} \quad y \quad ac \equiv bd \pmod{n}}$

5) $\boxed{\left.\begin{array}{l} a \equiv b \pmod{n} \\ m \mid n \end{array}\right\} \Rightarrow a \equiv b \pmod{m}}$

6) $\boxed{\left.\begin{array}{l} a \equiv b \pmod{m} \\ n \in \mathbb{N} \end{array}\right\} \Rightarrow a^n \equiv b^n \pmod{m}}$

7) Para "cancelar"

$\boxed{\left.\begin{array}{l} ca \equiv cb \bmod n \\ c \neq 0 \end{array}\right\} \Rightarrow a \equiv b \bmod \left(\frac{n}{d}\right) \quad \text{siendo } d = MCD(n, c)}$

Definición: $c \in \mathbb{Z}$ es invertible módulo n si $\exists\, e \in \mathbb{Z} \,/\, c.e \equiv 1 \pmod n$

↳ no es único.

Propiedad:

$$\left.\begin{array}{l} ce \equiv 1 \pmod n \\ ce' \equiv 1 \pmod n \end{array}\right\} \Longrightarrow e \equiv e' \pmod n \quad \text{es decir} \quad e' = e + kn$$

Teorema: c es invertible módulo $n \iff MCD(c,n) = 1$

Ecuaciones con congruencia

La ecuación $cx \equiv b \pmod n$ tiene solución entera $\iff MCD(c,n) \mid b$

Por el teorema de ec diofánticas, cuando $d = MCD(c,n) \mid b$, si (x_0, k_0) es solución, todas las ecuaciones son:

$$\boxed{\begin{array}{l} x = x_0 + \frac{n}{d}\alpha \\ k = k_0 + \frac{c}{d}\alpha \end{array}} \Longrightarrow \text{todas las soluciones de } cx \equiv b \pmod n \text{ son: } x = x_0 + \frac{n}{d}\alpha$$

Hay exactamente d soluciones

Teorema chino de los restos

Sean $m_1, \dots, m_k \in \mathbb{Z}$ coprimos 2 a 2 y $a_1, \dots, a_k \in \mathbb{Z}$

Entonces el sistema:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

Tiene solución entera.

Además si x y x' son soluciones $\Rightarrow x \equiv x' \pmod{m_1 \dots m_k}$

También la solución es $\boxed{X = a_1\alpha_1 M_1 + \dots + a_k\alpha_k M_k}$

Donde $M_i = \dfrac{m_1 \dots m_k}{m_i} = \prod_{i \neq J} m_J$

$\alpha_i M_i \equiv 1 \pmod{m_i}$

Büten Žar
Bruno Szilagyi

Pequeño teorema de Fermat

Parte 1

Sea $a \in \mathbb{Z}$

Si p es primo $\Longrightarrow a^p \equiv a \pmod{p} \quad \forall a \in \mathbb{Z}$

Parte 2

Sea $a \in \mathbb{Z}$

Si p es primo y $a \not\equiv 0 \pmod{p} \Longrightarrow a^{p-1} \equiv 1 \pmod{p}$

Definición: Un número $p \in \mathbb{N}$ se llama "pseudoprimo" si no es primo pero cumple:

$$a^p \equiv a \pmod{p} \quad \forall a \in \mathbb{Z}$$

Teorema de Euler – Fermat

$$\boxed{\text{Si } n \in \mathbb{N} \text{ y } \underset{a \in \mathbb{Z}}{} \ \mathrm{MCD}(a,n) = 1 \Longrightarrow a^{\varphi(n)} \equiv 1 \pmod{n}}$$

"φ" es la llamada "Función de Euler"

Definición: Función de Euler

$\forall n \in \mathbb{N}$ (fijo)

$$\boxed{\varphi(n) = \#\{ j \in \mathbb{N} : 1 \leq j \leq n, \ \mathrm{MCD}(n,j) = 1 \}}$$

Proposición 1: $\boxed{\text{Si } p \text{ es primo} \Longrightarrow \varphi(p) = p-1}$

Proposición 2: $\boxed{\text{Si } p \text{ es primo}, \ m \in \mathbb{N}, \ p^m = n \Longrightarrow \varphi(n) = \varphi(p^m) = p^{m-1}(p-1)}$

Proposición 3: $\boxed{\text{Si } p \text{ y } q \text{ son primos} \Longrightarrow \varphi(p.q) = (p-1)(q-1)}$

Función multiplicativa: Es una función $f : \mathbb{N} \to \mathbb{N} \ / \ \forall n, m \in \mathbb{N}$ con $\mathrm{MCD}(n.m) = 1$ se cumple

$$\boxed{f(m.n) = f(m).f(n)}$$

Teorema: La función de Euler es "multiplicativa"

$$\boxed{\varphi(n) = \varphi(p_1^{m_1} \dots p_k^{m_k}) = \varphi(p_1^{m_k}) \dots \varphi(p_k^{m_k})}$$

Además $$\boxed{\varphi(n) = n \prod_{\substack{p_i \mid n \\ p_i \text{ es primo}}} \left(1 - \frac{1}{p_i}\right)}$$

Extra!

Sistemas de numeración

agrego el segundo dígito a la izq y cuento los 10 otra vez.

Decimal (10) : $\overbrace{0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9}^{\text{10 DÍGITOS}} \quad 10 \quad 11 \ldots$

Binario (2) : $\overbrace{0 \quad 1}^{\text{2 DÍGITOS}} \quad 10 \quad 11 \quad 100 \quad 101 \quad 110 \quad 111 \quad 1000 \quad 1001 \quad 1010 \quad 1011$

Hexadecimal (16) : $\overbrace{0 \quad 1 \ldots 9 \; A \; B \; C \; D \; E \; F}^{\text{16 dígitos}} \quad 10 \quad 11 \ldots$

Binario → Decimal

$2^7 \; 2^6 \; 2^5 \; 2^4 \; 2^3 \; 2^2 \; 2^1 \; 2^0$

1 0 1 1 0 0 1 0

1 está
0 no está

$10110010 \rightarrow 2^7 + 2^5 + 2^4 + 2$

Decimal → Binario

157 ⌊2 → cantidad dígitos

157	⌊2						
1	78	⌊2					
	0	39	⌊2				
		1	19	⌊2			
			1	9	⌊2		
				1	4	⌊2	
					0	2	⌊2
						0	$\boxed{1}$

$2^0 \quad 2^1 \quad 2^2 \quad 2^3 \quad 2^4 \quad 2^5 \quad 2^6 \quad 2^7$

$\boxed{1}$ 0 0 1 1 1 0 1

Binario → Hexadecimal

Se agrupan de 4

$\underbrace{1\,0\,0\,1}\;\underbrace{1\,1\,0\,1}$

$2^3 + 2^2 + 1 = 13 = \boxed{D}$

$2^3 + 1 = \boxed{9}$

$\Rightarrow \boxed{9D}$

Decimal → Hexadecimal

$167 \,\underline{|\, 16}$ → cantidad de dígitos

$7 \quad \boxed{10}$

$16^0 \quad 16^1$

10 no es un dígito   10 → A

7 si es un dígito

$167 \longrightarrow \boxed{A7}$

10 → A
11 → B
12 → C
13 → D
14 → E
15 → F

Hexadecimal → Decimal

$16^7 \quad 16^6 \quad 16^5 \quad 16^4 \quad 16^3 \quad 16^2 \quad 16^1 \quad 16^0$

A 7 8 B 0 3 9 2

0 no está
otro díg → si está

$\boxed{A} \cdot 16^7 + 7 \cdot 16^6 + 8 \cdot 16^5 + \boxed{B} \cdot 16^4 + 3 \cdot 16^2 + 9 \cdot 16 + 2 \cdot 1$

convertir las $\boxed{}$ a decimal

$\boxed{10} \cdot 16^7 + 7 \cdot 16^6 + 8 \cdot 16^5 + \boxed{11} \cdot 16^4 + 3 \cdot 16^2 + 9 \cdot 16 + 2 \cdot 16^0$