Que no te escriban poemas de amor
cuando terminen la carrera ►►►►►►

(a nosotros por suerte nos pasa)

WUOLAH

No si antes decirte
Lo mucho que te voy a recordar

Pero me voy a graduar.
Mañana mi diploma y título he de pagar

Llegó mi momento de despedirte
Tras años en los que has estado mi lado.

Siempres me has ayudado
Cuando por exámenes me he agobiado

Oh Wuolah wuolitah
Tu que eres tan bonita

MATEMÁTICA DISCRETA

ARITMÉTICA

Jorge Ballesta Cerezo

...

Tema 4 Aritmética

División entera

Sean $p, q \in \mathbb{N}$. Entonces existen únicos $d, r \in \mathbb{N}$ $0 \leq r < q$ de forma que $p = q \cdot d + r$

$p \mid q$
r, d

Propiedades

- Si $a \mid b$, entonces $a \mid b \cdot c$
- Si $a \mid b$ y $b \mid c$, entonces $a \mid c$
- Si $a \mid b$ y $a \mid c$ entonces $a \mid bx + cy$ $\forall x, y \in \mathbb{Z}$
- Si $a, b \in \mathbb{N} \setminus \{0\}$ y $a \mid b$ entonces $a \leq b$
- Si $a \mid b$ y $b \mid a$ entonces $a = b$ o $a = -b$

Máximo común divisor

d es el máximo común divisor de a y b si es el mayor entero positivo que divide a y b es decir $d \mid a$ y $d \mid b$ y si c es tal que $c \mid a$ y $c \mid b$ entonces $c \mid d$

Se denotará por $\gcd(a, b)$ y su resultado es único

Propiedad

Sea $a, b \in \mathbb{N} \setminus \{0\}$, con $b \leq a$ entonces $\gcd(a, b) = \gcd(b, r)$

Teorema de Bezout

Sea $a, b \in \mathbb{Z} \setminus \{0\}$ y $d = \gcd(a, b) \Rightarrow$ d es el menor entero positivo tq $d = a \cdot x + b \cdot y$ $\forall x, y \in \mathbb{Z}$

(x: inverso de a; y: inverso de b y mod n)

Aritmética modular

Dados $m \in \mathbb{N}\setminus\{0,1\}$ (módulo) y $a,b \in \mathbb{Z}$, decimos que a es congruente con b módulo m si $m \mid a-b$ es decir, si existe $d \in \mathbb{Z}$ tq $a-b=m\cdot d$. Se denotará $a=b \pmod m$

Propiedades

$a=b \pmod m \longleftrightarrow$ $a \div m$ y $b \div m$ sus restos son iguales

Sea $a \in \mathbb{Z}_m$:

a) a es invertible $\longleftrightarrow$ $\gcd(a,m)=1$. En particular si m es primo, todos los elementos no nulos de $\mathbb{Z}_m$ son invertibles

b) $\gcd(a,m)\neq 1 \longleftrightarrow \exists\, b \in \mathbb{Z}_m\setminus\{0\}$ tq $a\cdot b=0$

Sea $m \in \mathbb{N}\setminus\{0,1\}$ y $a,b,c \in \mathbb{Z}_m$:

a) Si $a\cdot b=a\cdot c$ y $\gcd(a,m)=1 \Rightarrow b=c$

b) Si $a\cdot b=a\cdot c$ y $\gcd(a,m)=d \Rightarrow b=c \pmod{\frac{m}{d}}$, es decir $b=c\ \mathbb{Z}_{\frac{m}{d}}$

c) Si m es primo y $a\cdot b=a\cdot c \Rightarrow b=c$

Función φ de Euler (cantidad de números antes de el que son coprimos)

Dados $m \in \mathbb{N}\setminus\{0\}$, definimos $\varphi(m)$ como el cardinal del conjunto $\{k \in \{1,2,\dots,m-1\}: \gcd(k,m)=1\} = \{k \in \mathbb{Z}_m : k \text{ es invertible}\}$

Calcular la función de Euler, pero sí cuando conocemos su descomposición en primos a partir del siguiente resultado. Sea $m,n \in \mathbb{N}\setminus\{0\}$:

a) Si m es primo, entonces $\varphi(m)=m-1$
b) Si m es primo, entonces $\varphi(m^k)=m^k-m^{k-1}$
c) Si $\gcd(n,m)=1$, entonces $\varphi(n\cdot m)=\varphi(n)\cdot\varphi(m)$

$n=p_1^{e}\cdot p_2^{e'}\cdot p_3^{e''}\cdot\dots\cdot p_k^{e^k}=n\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\dots$

Que no te escriban poemas de amor cuando terminen la carrera ►►►►►►

(a nosotros por suerte nos pasa)

No si antes decirte
Lo mucho que te voy a recordar

Pero me voy a graduar.
Mañana mi diploma y título he de pagar

Llegó mi momento de despedirte
Tras años en los que has estado mi lado.

Siempres me has ayudado
Cuando por exámenes me he agobiado

Oh Wuolah wuolitah
Tu que eres tan bonita

Teorema de Euler

Sean $a, m \in \mathbb{Z}\setminus\{0\}$ con $m>1$ tq $\gcd(a,m)=1$:

$$a^{\varphi(m)} = 1 \pmod m$$

Calcular inverso $a^{\varphi(m)-1}$

Corolario

Sean $a, m \in \mathbb{Z}\setminus\{0\}$ con m primo tq $\gcd(a,m)=1$:

$$a^{m-1} = 1 \pmod m$$

Para resolver una ecuación lineal $ax=b$ en $\mathbb{Z}_m$, a debe tener inverso ($\gcd(a,m)=1$) siendo la solución $x = a^{-1}\cdot b \Rightarrow x = a^{\varphi(m)-1}\cdot b \pmod m$

Ejemplo: $7x = 2 \pmod{10}$

$$x = 7^{-1}\cdot 2 \Rightarrow x = 7^{\varphi(10)-1}\cdot 2 = 7^3\cdot 2 \pmod{10} = 6 \pmod{10} \quad x=6 \text{ en } \mathbb{Z}_{10}$$

$$7^{\varphi(10)} = 7^{\varphi(5)\varphi(2)} = 7^4$$

Ecuaciones diofánticas

Vamos a resolver ecuaciones de forma

$$a\cdot x + b\cdot y = c \quad \text{tienen solución si } \gcd(a,b)\mid c$$

Nótese que $a\cdot x + b\cdot y = c$ es equivalente a $a\cdot x = c \pmod b$

donde $a, b, c \in \mathbb{Z}$ y sólo buscamos soluciones enteras por lo que $x, y \in \mathbb{Z}$

Por el teorema de Bezout sabemos que $d=\gcd(a,b) \Rightarrow a\cdot x + b\cdot y = d$ tiene sol.entera

$\gcd(a,b)=d$ $\quad d\mid a$ y $d\mid b \Rightarrow d\mid c \Rightarrow c = dK = Kax + Kby \quad K\in\mathbb{Z}$

Solución aislada $ax_0 + by_0 = d$ (inverso por gcd aplicando Bezout)

Solución general $x = x_0 + \frac{b}{d}n$, $y = y_0 - \frac{a}{d}n$

$x_0 = \frac{cx}{d}$ (inver. de a), $y_0 = \frac{cy}{d}$ (inver. de b)

Teorema chino de los restos

$$\begin{cases} M_1 x = r_1 \pmod{m_1} \\ M_2 x = r_2 \pmod{m_2} \\ \quad \cdots\cdots \\ M_K x = r_K \pmod{m_K} \end{cases}$$

$m_1, m_2, \ldots m_K$ son coprimos dos a dos. Por tanto el sistema tiene solución única módulo $M = m_1 \, m_2 \ldots \cdot m_K$

Sea $M_i = M/m_i$ y sean las soluciones de las ecuaciones $s_1, s_2, \ldots s_K$ donde $s_i = M_i^{\varphi(m_i)-1} \pmod{m_i}$

$x_0 = M_1 \cdot r_1 \cdot s_1 + M_2 \cdot r_2 \cdot s_2 + \ldots + M_K \cdot r_K \cdot s_K$ es la solución del sistema

Ejemplo

$$\begin{cases} \boxed{35}\, x = 1 \mod 3 \\ \boxed{21}\, x = 1 \mod \\ 15\, x = 1 \mod 7 \end{cases} \quad (M_1)$$

$\longrightarrow s_1 = 2^{\varphi(3)-1} \mod(3) = 2$

$\longrightarrow s_2 = 1^{\varphi(5)-1} \mod(5) = 1$

$\longrightarrow s_3 = 1^{\varphi(7)-1} \mod(7) = 1$

$$\left.\begin{cases} 2x = 1 \mod(3) \\ x = 1 \mod(15) \\ x = 1 \mod(7) \end{cases}\right\} \quad x_0 = 35 \cdot \boxed{2} \cdot 2 + 21 \cdot \boxed{4} \cdot 1 + 15 \cdot \boxed{6} \cdot 1$$

1. Transformamos el sistema

$$\begin{cases} x = \boxed{5} \pmod 7 \\ x = 3 \pmod 6 \\ x = \boxed{5} \pmod{13} \end{cases} \longrightarrow \begin{cases} 78 = 6 \cdot 13 \; x = 1 \pmod{17} \\ 91 = 7 \cdot 13 \; x = 1 \pmod 6 \\ 42 = 7 \cdot 6 \; x = 1 \pmod{13} \end{cases}$$

(coprimos)

2. Calculamos los módulos

$7 \cdot 11 = 77 + 1 = 78$

$6 \cdot 15 + 1 = 91$

$13 \cdot 3 + 3 = 42$

$$\begin{cases} 1x = 1 \mod(7) \\ 1x = 1 \mod(6) \\ 3x = 1 \mod(13) \end{cases}$$

3. despejamos ecuaciones mediante el inverso, obtenido con gcd(3,13)

$$\begin{pmatrix} 3 & 1 & 0 \\ 13 & 0 & 1 \end{pmatrix} \xrightarrow[f_1 \times r_2]{r_2 - 4r_1} \begin{pmatrix} 1 & \boxed{-4} & 1 \\ 3 & 1 & 0 \end{pmatrix} \quad (13 \,|\, 3 \,|\, 1)$$

$-4 \mod(13) = -4 + 13 = 9$

4 sustituimos $x_0 = M_1 \cdot r_1 \cdot s_1 + M_2 \cdot r_2 \cdot s_2 + \ldots + M_k \cdot r_k \cdot s_k \pmod{M}$

$78 \cdot 5 \cdot 1 + 91 \cdot 3 \cdot 1 + 42 \cdot 5 \cdot 9 = 2553 = 369 \bmod(546)$

Para saber si $a \equiv b \bmod(m)$ es una congruencia se debe cumplir

$a - b \,\vdots\, m \Rightarrow m \mid a-b$

0 //

Para comprobar si 137 es primo

$\sqrt{137} = 11.7 \simeq 11$

Nº primos $\leq 11 = 2, 3, 5, 7, 11$ 137 ⋮ ... si el resto $\neq 0 \Rightarrow$ es primo