Divisibilidad:

Def: divisibilidad $m \mid n \iff \exists k \in \mathbb{Z}$ t.q. $mk = n$

mcd

algoritmo de división $a = bq + r$

(extendido)

Algoritmo de Euclides: ~~$a, b \in \mathbb{Z}_{>0}$, $a > b$. Para~~

lo verán en el práctico, pero

input: $a, b \in \mathbb{Z}$, ambos no cero

output: $u, v \in \mathbb{Z}$ t.q. $au + bv = \text{mcd}(a, b)$.

Aritmética modular (el operador %)

días de la semana: 4 días después del jueves es $4 + 4 = 2$ → martes

domingo lunes martes j ... sábado

0 ... 4 ... 6

$m \geq 1$; $a, b \in \mathbb{Z}$

Def: $a \equiv b \pmod{m}$ ~~si~~ si $a - b$ es divisible por m

↑ congruencia módulo m (bajo $\equiv$)

↑ el módulo (bajo m)

②

~~Prop~~ Ej $6 \equiv 28 \pmod{11}$ Ej: $7 \equiv 37 \pmod 4$

$\Updownarrow$ $\Updownarrow$

$6-28 = -22$ div ✓ por 11 $7-37$ div por 4 X
$= -30$

Ej: $m-1 \equiv -1 \pmod m$.

Prop $m \in \mathbb{Z}_{\geq 1}$

$a_1 \equiv a_2 \pmod m$ y $b_1 \equiv b_2 \pmod m \Rightarrow$

(a) $a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod m$

y

(b) $a_1 b_1 \equiv a_2 b_2 \pmod m$.

Se nota que no mencionamos división (inversos). ¿Porqué?

No se puede ~~siempre~~ dividir por 3 módulo 15.

o sea cuál es el x t.q. $3x \equiv 1 \pmod{15}$

x	$3x \pmod{15}$
1	3
2	6
3	9
4	12
5	0
6	3
⋮	⋮

Nunca llegaremos a $1 \pmod{15}$.

Pero sí tenemos:

(b) $a \in \mathbb{Z}$. Entonces

$a \cdot b \equiv 1 \pmod{m}$ para un entero b sii $mcd(a,m)=1$.

Dem (b): ($\Leftarrow$) $mcd(a,m)=1 \Rightarrow \exists\, u,v \in \mathbb{Z}$ t.q. $au+mv=1$.

Reduciendo módulo m, nos da

$$au \equiv 1 \pmod{m}.$$

Y entonces el b que buscamos es la u.

($\Rightarrow$) $\exists\, b$ t.q. $ab \equiv 1 \pmod{m} \Rightarrow$

$ab-1 = cm \Rightarrow ab-cm=1$

$\Rightarrow \left.\begin{array}{l} mcd(a,m) \mid a \\ mcd(a,m) \mid m \end{array}\right\} \Rightarrow mcd(a,m) \mid ab-cm$

$\Rightarrow mcd(a,m) \mid 1$

$\Rightarrow mcd(a,m)=1.$

Def. $\mathbb{Z}/m\mathbb{Z} = \{0,1,\ldots,m-1\}$ es el anillo de enteros módulo m.

Las operaciones binarias son dadas por tomando el resto después de dividir por m.

$(ab)\%m = a \cdot b \pmod{m} \in \mathbb{Z}/m\mathbb{Z}$ por el algoritmo de división

$(a+b)\%m = a+b \pmod{m} \in \mathbb{Z}/m\mathbb{Z}$

Def $a \in \mathbb{Z}/m\mathbb{Z}$ tiene inverso multiplicativo si $\text{mcd}(a,m)=1$

El conjunto de unidades de $\mathbb{Z}/m\mathbb{Z}$ es

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{ a : \mathbb{Z}/m\mathbb{Z} : \text{mcd}(a,m)=1 \}$$

$\Updownarrow$

tiene inverso módulo m.

Ej Si $a_1, a_2 \in (\mathbb{Z}/m\mathbb{Z})^\times \Rightarrow a_1 a_2 \in (\mathbb{Z}/m\mathbb{Z})^\times$

Dem $\text{mcd}(a_1 a_2, m) = 1$ o $(a_1 a_2)^{-1} = a_1^{-1} a_2^{-1}$.

Def La función φ de Euler es dada por

$$\varphi(m) = \#\left((\mathbb{Z}/m\mathbb{Z})^\times \right).$$

$$= \#\{ 0 \le a < m : \text{mcd}(a,m)=1 \}.$$

Ej Aritmética modular y cifrados de César.

$0 \leftrightarrow A$

$1 \leftrightarrow B$

$\vdots$

$26 \leftrightarrow Z$

$k=3$,

$E_k(m_1 m_2) = m_1 + k \pmod{27}$

$D_k(c_1) = c - k \pmod{27}$.

Ej Cómo calcular rápidamente $3^{218} \pmod{1000}$ y sin usar multiplicaciones de números grandes. Práctico.

¿Qué pasa si n es un primo?

Prop: Sea p primo. Entonces

$$(\mathbb{Z}/p\mathbb{Z})^{\times} = \{1, 2, \ldots, p-1\}.$$

O sea todo elemento no cero tiene un inverso. O sea

$(\mathbb{Z}/p\mathbb{Z})$ es un cuerpo.

Muchas veces se denota $\mathbb{Z}/p\mathbb{Z}$ como $\mathbb{F}_p$ or $GF(p)$

↑ field = cuerpo ↑ Galois field.

Primos:

Un número primo es un entero $p \geq 2$ con exactamente dos divisores

Prop Si p es primo y $p \mid ab$ entonces $p \mid a$ o $p \mid b$.

Dem $g = \text{mcd}(a,p)$ Entonces $g \mid p$

$\Rightarrow \quad g = 1 \quad$ o $\quad g = p$.

Si $g \neq p$, ($\Leftrightarrow g \mid a \Rightarrow p \mid a$) se cumple la demostración. Entonces supongamos que $g = 1$

Entonces $\exists\, u, v \in \mathbb{Z}$ tq $au + pv = 1$

$\Rightarrow abu + pbv = b$

Como $p \mid ab$ por hipótesis, y como $p \mid pb$ se ve que p tiene que dividir ab ∎

Tma fund. de aritmética. $\mathbb{Z} \ni a \geq 2$. Entonces se puede factorizar

$$a = p_1^{e_1} \cdots p_r^{e_r}$$

Y, salvo permutando el orden de los primos, la factorización en potencias de primos es única.

Dem: Usando inducción se puede probar que se factorización. Ahora la unicidad

$$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

donde los p_i y q_j son primos no necesariamente distintos, y no necesariamente $s=t$. Ahora como $p_1 | a$ sabemos que $p_1 | q_1 \cdots q_t$.

Entonces p_1 divide uno de los q_i (por la Prop anterior).

Como p_1 y q_i son primos, $p_1 = q_i$ y los podemos cancelar.

Reordenando el orden $q_1 \rightsquigarrow q_i$, tenemos

$$p_2 p_3 \cdots p_s = q_2 \cdots q_t$$

Repitiendo el proceso s veces más de

$$1 = q_{t-s} q_{t-s+1} \cdots q_t$$

□

Entonces $t=s$.

Def: El orden de un primo p en $a = p_1^{e_1} \cdots p_r^{e_r}$ es la potencia de p en la factorización de a. Se denota $\mathrm{ord}_p(a)$

$$\begin{cases} \text{si } p \nmid a, & \mathrm{ord}_p(a) = 0 \\ \forall p & \mathrm{ord}_p(1) = 0 \end{cases}$$

Obs: $a = \prod_{\text{primos}} p^{\mathrm{ord}_p(a)}$ ← producto infinito

Thm (Pequeño thm de Fermat)

Sea p un primo y $a \in \mathbb{Z} \Rightarrow$

$$a^{p-1} = \begin{cases} 1 \pmod p & p \nmid a \\ 0 \pmod p & p \mid a. \end{cases}$$

Dem Si $p \mid a$, $p \mid a^{p-1} \Rightarrow a^{p-1} \equiv 0 \pmod p$

Si $p \nmid a$, los números

$$a,\ 2a,\ 3a,\ \dots,\ (p-1)a$$ son distintos módulo p

(porque tenemos inverso módulo p.

Si $ka \equiv la \pmod p$

como $p \nmid a$ esto

$\Rightarrow k \equiv l \pmod p$

pero como $k, l < p$

$\Rightarrow k = l$.

Entonces

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$$

$\Rightarrow a^{p-1} \equiv 1 \pmod p$ multiplicando cada lado por el inverso de $2, 3, \dots, p-1$.

Ej 15485863 es primo

$$\Rightarrow 2^{15485862} \equiv 1 \pmod{15485863}.$$

↑ tenemos que 2 millones

ej Obs Se puede si uno quiere calcular a^n módulo p

Se puede reducir el exponente módulo p-1. o sea

$$a^{n \pmod{p-1}} \equiv a^n \pmod{p}.$$

P.q: cada múltiplo de p-1 que está dentro de n no da un

$$a^{p-1} \equiv 1 \pmod{p}.$$

~~443579 mód p~~

$$2^{100} \pmod{11} \equiv (2^{10})^{10} \pmod{11}$$
$$\equiv 1^{10} \pmod{11}$$
$$\equiv 1 \pmod{11}.$$

ej. 7814^{-1} módulo 17449?

$$7814^{-1} \equiv 7814^{17448 - 1} \equiv 1234 \pmod{17449}$$

usando exponenciación rápida.

Def. El orden de a módulo p es la potencia $k \geq 1$ más pequeña t.q

$$a^k \equiv 1 \pmod{p}$$

Prop Sea p primo, $p \nmid a \in \mathbb{Z}$, $a^r \equiv 1 \pmod p$
Entonces el orden de a mód p divide a n

Cor orden de a mód p divide $p-1$

Dem k = orden de a mód p
$\Rightarrow a^k \equiv 1 \pmod p$ y k es el número natural más chico con esta propiedad.

Entonces
$a^n \equiv 1 \pmod n \Rightarrow \exists\, q$ $a^{kq+r} \equiv 1 \pmod n$
$0 \le r < k$

$\Rightarrow (a^k)^q a^r \equiv 1 \pmod n$

$\Rightarrow a^r \equiv 1 \pmod p$

Entonces, como $r < k$ y k es el orden de a mód. p
entonces, $r = 0$ y concluimos que $n = kq$ o $k \mid n$

Tma (Tma de raíces primitivas)
p primo $\exists\, g \in \mathbb{F}_p^\times$ t.q
$$\mathbb{F}_p^\times = \{g^1, g^2, \dots, g^{p-1}\}.$$

O sea para cada p existe una raíz primitiva

Obs g genera $\mathbb{F}_p^\times$
g tiene orden $p-1$

Ej En $\mathbb{F}_{11}$, 2 es una raíz primitiva.