

Clase 1 - División entera. Teo de división entera. Propiedades. N° primos. MCD.

Clase 2 - Identidad de Bezout. Coprimos. Propiedades de MCD. Algoritmo de Euclides.

Clase 3 - Propiedades MCD y mcm. Algoritmo extendido de Euclides y demostracion Id Bezout.

Clase 4 - Demostraciones prop MCD. Lema de Euclides. Ecuaciones diofánticas lineales.

Clase 5 - Corolarios del Lema de Euclides. Teorema Fundamental de la aritmética. Números primos.

Clase 6 - Teorema infinitos números primos. Teorema de mcm y MCD conociendo la factorización de a y b.

Clase 7 - Congruencias módulo n. Propiedades y corolarios.

Clase 8 - Cancelativas e inversas en congruencias módulo n.

Clase 9 - Ecuaciones con congruencia. Ecuaciones congruentes. Teorema chino de los restos.

Clase 10 - Teorema chino de los restos.

Clase 11 - Pequeño teorema de Fermat (2 partes). Pseudoprimos.

Clase 12 - Teorema Euler - Fermat. Función de Euler.

Clase 13 - Propos 3. Función Multiplicativa. Euler multiplicativa. Corolario.

Clase 14 - Demostración del Teorema : La función de Euler es multiplicativa.

Clase 15 - Demostración del Teorema Fermat - Euler. Aplicaciones.

Clase 16 - Grupos. Grupo Abeliano. Tabla de Cayley. Ejemplos.

Clase 17 - Grupo permutación. Grupo diedral. Subgrupo.

Clase 18 - Def Potencia. Órden de un elemento. Subgrupo generado por un elemento. Grupo cíclico.

Clase 19 - Ejemplos de grupos cíclicos y no cíclicos. Varios teoremas. Coclase en el grupo.

Clase 20 - Teorema de Lagrange. Corolarios 1, 2, 3, 4. Homomorfismo de grupos.

Clase 21 - Homomorfismo de grupos. Ker (f). Ejemplos. Propiedades de homomorfismo.

Clase 22 - Homomorfismo inyectivo. Corolarios. Teo de los órdenes. Propiedades de Im(f).

Clase 23 - Isomorfismos. Propiedades de los Isomorfismos. Ejemplos.

Clase 24 - Raíz primitiva mod n. Ejemplos. Lemas. Teorema de las raíces primitivas.

Clase 25 - Demostración de teorema U(p) cíclico. Demostración de lemas 3 y 4.

Clase 26 - Criptografía. Metodos Encriptado (Clave privada). Método de intercambio de clave.

Clase 27 - Clave pública : R.S.A. Ejemplos.

Clase 28 - Continuación de ejemplos clase pasada. Encriptado por bloques.

Divisibilidad en \mathbb{Z}

\mathbb{Z} = conjunto de números enteros $\{-\dots, -3, -2, -1, 0, 1, \dots, 101, \dots\}$

\mathbb{N} = conjunto de números naturales (≥ 1) $\{1, 2, 3, \dots, 101, \dots\}$

División entera

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

Ejemplo: ① $a = 4$, $b = 175$

Dividendo $175 \quad | \quad 4$ → divisor
 15 43 → cociente entero
 resto 3 8
 restos 3 8

$$175 = 4 \cdot 43 + 3$$

quotient
↓
divisor

② $a = 4$, $b = -175$

$$-175 = 4 \cdot (-43) + (-3) = 4(-43) + (-3) + 4 - 4 = 4(-44) + 1$$

resto
↓ quotient

Teorema de la división entera

Dados $b \in \mathbb{Z}$, $a \in \mathbb{N}$.

Existen y son únicos los números enteros q y r llamados "cociente entero" q y el "resto" r .

Tales que:

$$b = aq + r \quad 0 \leq r < a$$

Definición: $b \in \mathbb{Z}$, $a \in \mathbb{Z}$, $a \neq 0$ Se dice que b es múltiplo de a si $b = a$ (o que b es divisible entre a) si b

Cuando: $b = a \cdot q$

para algún entero q que se llama cociente de b sobre a y se denota $q = \frac{b}{a}$

Ejemplos: divisores de 12 : 1, 2, 3, 4, 6, 12, -12, -6, ...

divisores de 0 : todo $a \in \mathbb{Z}$ ($a \neq 0$)

Propiedad: si $a \parallel b$ y $a > 0$ $b \neq 0$ $\Rightarrow 0 < a \leq |b|$

Demostración:

$$\text{por } \mathbb{H} \quad a|b \Leftrightarrow \underset{\substack{\text{def} \\ q \in \mathbb{Z}}}{b = a \cdot q} \Leftrightarrow |b| = a \cdot |q| \underset{\substack{|a| \\ = |a| \text{ pues } a > 0}}{= |a|}$$

$\Rightarrow q \neq 0$ pues si no b sería 0 y por (H) $b \neq 0 \Rightarrow |q| \geq 1$

$$|b| = a|q| \Rightarrow a|q| \geq a \cdot 1 \Rightarrow |b| \geq a \quad \text{LQQD}$$

$|q| > 1$ $a > 0$

Obs: si $b \in \mathbb{N}, b \neq 1$ b tiene por lo menos dos divisores distintos en \mathbb{N} , 1 y b .
 "Divisores triviales" de b .

Definición: Cuando $P \in \mathbb{N}$, $P \neq 1$, tiene en \mathbb{N} solo los 2 divisores triviales y ningún otro entonces P se llama "número primo".

Propiedades:

$$\textcircled{1} \quad \left. \begin{array}{l} a|b \\ b|c \end{array} \right\} \Rightarrow a|c$$

$$\begin{aligned} \text{Demostración: Por (H) } ab &\Rightarrow \exists k \in \mathbb{Z} \mid b = a \cdot k \\ blc &\Rightarrow \exists k' \in \mathbb{Z} \mid c = b \cdot k' \end{aligned} \quad \boxed{\Rightarrow c = a \cdot k \cdot k'} \quad k''$$

$$\textcircled{2} \quad \left. \begin{matrix} ab \\ ac \end{matrix} \right\} \rightarrow a(b+c)$$

Demostración: Por (H) $a|b \Rightarrow \exists k \in \mathbb{Z} / b = a \cdot k$

$$a|c \Rightarrow \exists k' \in \mathbb{Z} / c = a \cdot k' \Rightarrow b+c = a \cdot k + a \cdot k' = a(\underbrace{k+k'}_{k''})$$

$$\textcircled{3} \quad \left. \begin{array}{l} ab \\ n \in \mathbb{Z} \\ n \neq 0 \end{array} \right\} \Rightarrow a.n | b.n$$

Demostración: Por \textcircled{H} $a|b \Rightarrow \exists k \in \mathbb{Z} / b = a \cdot k$

$$\Rightarrow b \cdot n = a \cdot k \cdot n \Rightarrow b \cdot n = a \cdot n \cdot k \Rightarrow a n | b n$$

$$\textcircled{4} \quad a|b \Rightarrow a|b \cdot n \quad \forall n \in \mathbb{Z}$$

Demostración: $a|b \Rightarrow \exists k \in \mathbb{Z} / b = a \cdot k$

$$b \cdot n = a \cdot k \cdot n = a \cdot k' \Rightarrow a|b \cdot n$$

Propiedad importante:

Si b y c son múltiplos de $a \Rightarrow$ cualquier combinación lineal de b y c (con coef Enteros) también es múltiplo de a .

Teorema

$$\begin{array}{ll} \textcircled{H} \quad a|b & \textcircled{T} \quad a|bx + cy \\ \left(a, b, c \in \mathbb{Z} \right) & a|c \\ a \neq 0 & x, y \in \mathbb{Z} \end{array}$$

Demostración: Por $\textcircled{H} \quad a|b \Rightarrow \exists k \in \mathbb{Z} / b = a \cdot k$

$$a|c \Rightarrow \exists k' \in \mathbb{Z} / c = a \cdot k'$$

$$\begin{aligned} bx &= a k x \\ cy &= a k' y \end{aligned} \quad \left\{ \Rightarrow bx + cy = a k x + a k' y = a(kx + k'y) = a k'' \right.$$

$$\Rightarrow a|bx + cy$$

Divisores comunes

12 y 8 "divisores comunes o compartidos"

naturales: 1, 2, 4

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

Identidad de Bezout

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

Definición: a y b se llaman "coprimos" si $\text{MCD}(a, b) = 1$

Propiedades de MCD(a, b)(1) MCD(a, b) es único

Demostración: si $d_1 = \text{MCD}(a, b)$, $d_2 = \text{MCD}(a, b)$

$$\Rightarrow \left\{ \begin{array}{l} d_1 \geq d_2 \quad \text{porque } d_1 \text{ es } \text{MCD}(a, b) \\ d_2 \geq d_1 \quad " \quad d_2 \quad " \quad " \end{array} \right\} \Rightarrow d_1 = d_2$$

(2) Sea $a' = \frac{a}{\text{MCD}(a, b)}$ y $b' = \frac{b}{\text{MCD}(a, b)}$ Entonces a' y b' son coprimos

Demostración: Hay que probar que $\text{MCD}(a', b') = 1$.

Sea $h \geq 1$ un divisor común de a' , b' . basta probar que $h \leq 1$.

$$\Rightarrow \left\{ \begin{array}{l} a' = h \cdot q_1 \\ b' = h \cdot q_2 \end{array} \right. \quad \text{de (H)} \quad \left\{ \begin{array}{l} a = [\text{MCD}(a, b)] \cdot a' \\ b = [\text{MCD}(a, b)] \cdot b' \end{array} \right.$$

$$a = ([\text{MCD}(a, b)] \cdot h) \cdot q_1 \quad [\text{MCD}(a, b)] \cdot h = e$$

$$b = ([\text{MCD}(a, b)] \cdot h) \cdot q_2 \quad 1 \leq e, e \text{ es un divisor común a } b \text{ y } a$$

$$\Rightarrow e \leq \text{MCD}(a, b)$$

$$\text{MCD}(a, b) \cdot h \leq \text{MCD}(a, b) \Rightarrow h \leq 1$$

Algoritmo de Euclides para hallar $\text{MCD}(a,b)$ Introducción:

$$\text{MCD}(765, 60) = d$$

$$\begin{array}{r} 765 \\ 45 \end{array} \left| \begin{array}{r} 60 \\ 12 \\ 0 \end{array} \right.$$

$$765 = 60 \cdot 12 + \boxed{45}^{r_0}$$

$$765 - 60 \cdot 12 = 45$$

$$\left. \begin{array}{l} d \mid 765 \\ d \mid 60 \end{array} \right\} \Rightarrow d \mid 765 - 60 \cdot 12 \Rightarrow d \mid 45$$

Lema 1

$d = \text{MCD}(a,b)$ y $a \geq b$ (si d es un divisor común ≠ $\text{MCD}(a,b)$ también funciona)

Si $r_0 \neq 0$ es el resto de la división entera de a entre b

$$a = b \cdot q_0 + r_0 \Rightarrow d \mid r_0$$

Lema 2

Si d divide a b y a $r_0 \neq 0$, siendo r_0 el resto de la división entera entre a y b
 $\Rightarrow d \mid a$

Demostración:

por (H) $\left\{ \begin{array}{l} a = b \cdot q_0 + r_0 \\ d \mid b \\ d \mid r_0 \end{array} \right\} \Rightarrow d \mid \text{CL de } b \text{ y } r_0 \Rightarrow d \mid b q_0 + r_0 \Rightarrow d \mid a$
 (coef enteros)

Conclusión:

$$\text{MCD}(a,b) = \text{MCD}(b, r_0)$$

donde r_0 es el resto de la división entera de a/b
 (suponemos $r_0 \neq 0$)

Algoritmo:

$$\text{Si } a \geq b \Rightarrow a = b q_0 + r_0 \quad 0 \leq r_0 < b$$

$$\text{Si } r_0 = 0 \Rightarrow \text{MCD}(a, b) = b$$

$$\text{Si } r_0 \neq 0 \Rightarrow b = r_0 q_1 + r_1 \quad (\text{MCD}(a, b) = \text{MCD}(b, r_0))$$

$$\text{Si } r_1 = 0 \Rightarrow \text{MCD}(b, r_0) = r_0$$

$$\text{Si } r_1 \neq 0 \Rightarrow r_0 = r_1 q_2 + r_2 \quad (\text{MCD}(b, r_0) = \text{MCD}(r_0, r_1))$$

↓

Hasta que al final el último resto es 0 y el penúltimo es el MCD.

Ejemplo:

$$\text{MCD}(765, 60) = \text{MCD}(60, 45) = \text{MCD}(45, 15) = 15$$

Mas propiedades de MCD(a, b)

$$\boxed{① \text{ Si } d|a \text{ y } d|b \Leftrightarrow d|\text{MCD}(a, b)}$$

Demostración:

$$\left. \begin{array}{l} d|a \\ d|b \end{array} \right\} \Rightarrow d \mid \underbrace{a - b q_0}_{r_0} \Rightarrow \left. \begin{array}{l} d|b \\ d|r_0 \end{array} \right\} \Rightarrow \left. \begin{array}{l} d|r_0 \\ d|r_1 \\ \vdots \\ d|r_k \\ d|0 \end{array} \right\}$$

este es el MCD(a, b)
por el algoritmo
de Euclides.

$$\boxed{② \forall n \in \mathbb{N} \quad \text{MCD}(a \cdot n, b \cdot n) = n \cdot \text{MCD}(a, b)}$$

Ejemplo:

$$\text{MCD}(765 \cdot 3, 60 \cdot 3) = 3 \cdot \text{MCD}(765, 60)$$

$$\text{MCD}(2295, 180) = 3 \cdot 15 \cdot 45$$

Demostración: (Próx. clase)

Propiedades de MCD(a,b)

($a, b, c, d, n, a', b' \in \mathbb{N}$)

$$\textcircled{1} \quad \left. \begin{array}{l} c|a \\ c|b \end{array} \right\} \Rightarrow c \mid \text{MCD}(a,b)$$

$$\textcircled{2} \quad a' = \frac{a}{\text{MCD}(a,b)} \quad , \quad b' = \frac{b}{\text{MCD}(a,b)} \quad \Rightarrow \quad a' \text{ y } b' \text{ son coprimos.}$$

$$\textcircled{3} \quad \left. \begin{array}{l} a = a' \cdot d \\ b = b' \cdot d \\ a' \text{ y } b' \text{ son coprimos} \end{array} \right\} \Rightarrow d = \text{MCD}(a,b)$$

Demostración:

$$\text{por } \textcircled{H} \quad \left. \begin{array}{l} d \mid a \\ d \mid b \end{array} \right\} \xrightarrow{\text{prop } \textcircled{1}} d \mid \text{MCD}(a,b) \quad \Rightarrow \quad \text{MCD}(a,b) = d \cdot q \quad \textcircled{*}$$

$$\left. \begin{array}{l} \text{MCD}(a,b) \mid a \Rightarrow a = q_1 \cdot \text{MCD}(a,b) \quad \textcircled{*} \\ \text{MCD}(a,b) \mid b \Rightarrow b = q_2 \cdot \text{MCD}(a,b) \quad \textcircled{*} \end{array} \right\} \xrightarrow{\textcircled{H}} \left. \begin{array}{l} a = q_1 \cdot d \cdot q \quad d \neq 0 \\ b = q_2 \cdot d \cdot q \quad \textcircled{H} \end{array} \right\} \Rightarrow \left. \begin{array}{l} a' = q_1 \cdot q \\ b' = q_2 \cdot q \end{array} \right\} =$$

$$\Rightarrow \left. \begin{array}{l} q \mid a' \\ q \mid b' \end{array} \right\} \xrightarrow{\textcircled{H}} q = 1 \quad \text{porque } \text{MCD}(a',b') = 1$$

$$\text{por } \textcircled{*} \quad \text{y } \textcircled{**} \quad \text{MCD}(a,b) = d$$

$$\textcircled{4} \quad [\text{MCD}(na, nb) = n \cdot \text{MCD}(a, b)]$$

Demostración:

$$\text{MCD}(a, b) \mid a \Rightarrow a = a' \cdot \text{MCD}(a, b) \Rightarrow n \cdot a = n \cdot \text{MCD}(a, b) \cdot a'$$

$$\text{MCD}(a, b) \mid b \Rightarrow b = b' \cdot \text{MCD}(a, b) \Rightarrow n \cdot b = n \cdot \text{MCD}(a, b) \cdot b'$$

$$\text{MCD}(a', b') = 1 \text{ por prop ②}$$

$$\left. \begin{array}{l} na = n \cdot \text{MCD}(a, b) \cdot a' \\ nb = n \cdot \text{MCD}(a, b) \cdot b' \\ a' \text{ y } b' \text{ son coprimos} \end{array} \right\} \xrightarrow{\text{prop ③}} n \cdot \text{MCD}(a, b) = \text{MCD}(n \cdot a, n \cdot b)$$

Definición: Si $a, b \in \mathbb{Z}$

$$\cdot a \neq 0, b \neq 0 \quad \text{MCD}(a, b) \stackrel{\text{def}}{=} \text{MCD}(|a|, |b|)$$

$$\cdot a=0, b \neq 0 \quad \text{MCD}(0, b) \stackrel{\text{def}}{=} |b| = \text{MCD}(b, 0)$$

$$\cdot a=0, b=0 \quad \text{MCD}(0, 0) \neq$$

Ejemplo: $\text{MCD}(-24, 15) = 3$

$$\text{MCD}(-24, -15) = 3$$

$$\text{MCD}(-8, 0) = 8$$

Definición: mcm(a, b) es el menor natural que es a la vez múltiplo de a y b .

Teorema: \exists y es único $\text{mcm}(a, b)$

para \mathbb{Z} : $\cdot a \neq 0, b \neq 0 \quad \text{mcm}(a, b) \stackrel{\text{def}}{=} \text{mcm}(|a|, |b|)$

$$\cdot a=0 \text{ y } b=0 \quad \text{mcm}(a, b) \stackrel{\text{def}}{=} 0$$

Ejemplo:

$$\text{mcm}(-6, -14) = 42$$

Propiedades de $\text{mcm}(a,b)$ ($a,b,c,d,e,d',n \in \mathbb{N}$)

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

Demostración:

Sea $m = \text{mcm}(a,b)$

$$\boxed{c = m \cdot q_0 + r_0} \quad 0 \leq r_0 < m \quad \textcircled{1}$$

por (H) $\left. \begin{array}{l} a|c \\ a|\text{mcm}(a,b) \end{array} \right\} \Rightarrow a|cx + ym \stackrel{(x,y \in \mathbb{Z})}{=} a|c - mq \Rightarrow a|r_0$

por (H) $\left. \begin{array}{l} b|c \\ b|\text{mcm}(a,b) \end{array} \right\} \Rightarrow b|cx + ym \Rightarrow b|c - mq \Rightarrow b|r_0$

$\left. \begin{array}{l} a|r_0 \\ b|r_0 \end{array} \right\} \Rightarrow r_0 \text{ es un múltiplo común de } a \text{ y } b$

$\nearrow r_0 = 0 \quad \textcircled{2}$
 $\searrow r_0 \in \mathbb{N} \Rightarrow r_0 \geq m$

por $\textcircled{1}$ y $\textcircled{2}$ $r_0 = 0 \Rightarrow c = m \cdot q_0 \Rightarrow \boxed{\text{mcm}(a,b) | c}$

(B) $\frac{\text{mcm}(a,b)}{a}$ y $\frac{\text{mcm}(a,b)}{b}$ son coprimos.

(C) $\text{MCD}(a,b) \cdot \text{mcm}(a,b) = a \cdot b$

(D) $\text{mcm}(n \cdot a, n \cdot b) = n \cdot \text{mcm}(a, b)$

Lema: "Algoritmo de Euclides extendido"

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

$$\text{MCD}(765, 60) \quad 765 = 60 \cdot \underbrace{12}_{q_0} + \underbrace{45}_{r_0} \quad \rightarrow \quad 60 = 45 \cdot \underbrace{1}_{q_1} + \underbrace{15}_{r_1} \quad \rightarrow \quad 45 = 15 \cdot \underbrace{3}_{q_2} + \underbrace{0}_{r_2}$$

$$\text{MCD}(\underbrace{765}_a, \underbrace{60}_b) = \boxed{15} = x \underbrace{765}_a + y \underbrace{60}_b$$

Identidad de Bezout

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

Demostación:

$$a = b \cdot q_0 + r_0 \implies r_0 = a + (-q_0)b \quad r_0 \text{ es CL de } a \text{ y } b$$

$$b = r_0 q_1 + r_1 \implies r_1 = b + (-q_1)r_0 \quad r_1 \text{ es CL de } a \text{ y } b$$

$$r_0 = r_1 q_2 + r_2 \implies r_2 = r_0 + (-q_2)r_1 \quad r_2 \text{ es CL de } a \text{ y } b$$

$$r_{k-2} = r_{k-1} q_k + r_k \implies r_k = r_{k-2} + (-q_k)r_{k-1} \quad r_k \text{ es CL de } a \text{ y } b$$

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

$$r_{k-1} = r_k q_{k+1} + 0$$

↓
MCD

Ejemplo: $\text{MCD}(765, 60) = 15$

$$r_0 = 45 = 765 - \underbrace{12 \cdot 60}_{q_0} \quad \rightarrow \quad \frac{1}{15} = 60 + (-1) \frac{1}{45} \quad \Rightarrow \quad 15 = 60 + (-1)(765 - 12 \cdot 60)$$

$$15 = 13 \cdot 60 - 765$$

Repaso propiedades $\text{mcm}(a,b)$ $(a, b, c, d, n \in \mathbb{N})$

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

$$\textcircled{2} \quad \boxed{\text{MCD}(a,b) \cdot \text{mcm}(a,b) = a \cdot b}$$

Demostración: $a \cdot b$ es múltiplo común de a y de b } $\stackrel{\text{prop. 1}}{\Rightarrow} \text{mcm}(a,b) | ab$

$$\Rightarrow a \cdot b = q \cdot \text{mcm}(a,b) \quad q \geq 1$$

$$\Rightarrow b = q \cdot \frac{\text{mcm}(a,b)}{a} = q | b \quad \left. \begin{array}{l} \\ q < \text{MCD}(a,b) \end{array} \right\}$$

$$a = q \cdot \frac{\text{mcm}(a,b)}{b} = q | a \quad \left. \begin{array}{l} \\ q < \text{MCD}(a,b) \end{array} \right\}$$

$$ab \leq \text{MCD}(a,b) \cdot \text{mcm}(a,b) \quad *$$

$$\left. \begin{array}{l} a = a' \cdot \text{MCD}(a,b) \\ b = b' \cdot \text{MCD}(a,b) \end{array} \right\} \Rightarrow ab = (\text{MCD}(a,b))^2 \cdot a' \cdot b' \Rightarrow \frac{ab}{\text{MCD}(a,b)} = \frac{a' \cdot b'}{\text{MCD}(a,b)} = ab'$$

$$\frac{ab}{\text{MCD}(a,b)} \text{ es múltiplo común de } a \text{ y } b \Rightarrow \frac{ab}{\text{MCD}(a,b)} \geq \text{mcm}(a,b)$$

$$\Rightarrow \boxed{ab \geq \text{MCD}(a,b) \cdot \text{mcm}(a,b)} \quad (**)$$

$$\stackrel{(*)}{=} \boxed{ab = \text{MCD}(a,b) \cdot \text{mcm}(a,b)}$$

(3)

$$\frac{\text{mcm}(a,b)}{a}, \frac{\text{mcm}(a,b)}{b} \text{ son coprimos}$$

Demostración:

Uso prop ② $\Rightarrow \left\{ \begin{array}{l} \frac{\text{mcm}(a,b)}{a} = \frac{b}{\text{MCD}(a,b)} \\ \frac{\text{mcm}(a,b)}{b} = \frac{a}{\text{MCD}(a,b)} \end{array} \right.$

Ya probamos que son coprimos.
(Propiedad del MCD)

(4)

$$\text{mcm}(n.a, n.b) = n \cdot \text{mcm}(a,b)$$

Demostración:

prop ② $\text{mcm}(n.a, n.b) \cdot \text{MCD}(n.a, n.b) = n^2 \cdot a \cdot b$

$\xrightarrow{\text{prop MCD}}$ $\text{mcm}(n.a, n.b) \cdot n \cdot \text{MCD}(a,b) = n^2 \cdot a \cdot b$

$\xrightarrow{\text{prop ②}} \text{mcm}(n.a, n.b) \cdot \text{MCD}(a,b) = n \cdot \text{MCD}(a,b) \cdot \text{mcm}(a,b)$

$$\Rightarrow \text{mcm}(n.a, n.b) = n \cdot \text{mcm}(a,b)$$

Recordamos:

Definición: $P \in \mathbb{N}$ es "primo" si tiene exactamente 2 divisores naturales diferentes el 1 y el P ($\Rightarrow P \neq 1$)

Lema de Euclides: Sean a y $b \in \mathbb{N}$

Si p es primo y $p \mid ab \Rightarrow p \mid a \circ p \mid b$

Corolario:

Si $n \mid a.b$ y $\text{MCD}(n,a) = 1 \Rightarrow n \mid b$

Demostración: (Lema)

Si $a=0$ es trivial porque $p|0$ siempre.

Si $a \neq 0$: o bien $p|a \rightarrow \text{LQD}$

$$\text{o bien } p \nmid a \rightarrow \boxed{\text{MCD}(p, a) = 1} \quad \text{por (H) } p \nmid a, b \quad \left. \begin{array}{l} p \text{ es divisor común} \\ \text{de } ab \text{ y } bp \\ p \nmid p \cdot b \end{array} \right\} \boxed{p \nmid \text{MCD}(ab, bp)}$$

$$\left. \begin{array}{l} \text{MCD}(p, a) = 1 \Rightarrow \text{MCD}(bp, ab) = b \\ p \nmid \text{MCD}(bp, ab) \end{array} \right\} = p \nmid b$$

Ecuaciones diofánticas lineales

$ax + by = c$ Donde a, b, c son enteros dados, x e y son enteros desconocidos.

"incógnitas" a determinar para que verifiquen la igualdad.

Pasos:① Test de incompatibilidad

Halla $\text{MCD}(a, b) = d$

Si c no es múltiplo de $d \Rightarrow$ la ecuación diof es incompatible

Si c es $d \Rightarrow c = d \cdot k$, halla $k = \frac{c}{d}$

② Id Bezout

Por la Id Bezout \exists enteros x_0 e y_0 / $d = x_0a + y_0b$

Halla x_0 e y_0 usando el algoritmo de Euclides Extendido.

③ Solución particular

$$c = d \cdot k = (x_0a + y_0b) \cdot k = a(\underbrace{x_0k}_{x_1}) + b(\underbrace{y_0k}_{y_1}) \Rightarrow ax_1 + bx_2 = c$$

paso ①

paso ②

$\Rightarrow (x_1, y_1)$ es una solución particular.

(4) Solución general

$$ax_1 + bx_1 = c$$

$$ax + bx = c$$

$$a(x - x_1) + b(y - y_1) = 0 \Rightarrow a(x - x_1) = -b(y - y_1)$$

$$a'd(x - x_1) = -b'd(y - y_1)$$

$$a'(x - x_1) = -b'(y - y_1) \quad (*)$$

$$\Rightarrow \begin{cases} a' \mid b'(y - y_1) \\ \text{MCD}(a', b') = 1 \end{cases} \Rightarrow a' \mid (y - y_1)$$

Entonces $y - y_1 = h \cdot a'$ $h \in \mathbb{Z}$, construyo $\boxed{y = y_1 + ha'}$ donde h es cualquiera.

$$(*) a'(x - x_1) = -b'(y - y_1) = -b' \cdot h \cdot a'$$

$$x - x_1 = -b' \cdot h \Rightarrow \boxed{x = x_1 - h \cdot b'}$$

Ejemplos:

$$\textcircled{1} \quad \frac{a}{24}x + \frac{b}{20}y = 53$$

$$\text{MCD}(24, 20) = 4$$

53 no es múltiplo de 4

$\Rightarrow \textcircled{1}$ es incompatible

$$\textcircled{2} \quad 24x + 20y = 52$$

paso 1: $\text{MCD}(24, 20) = 4$ 52 es 4

$$k = \frac{52}{4} = 13$$

paso 2:
$$4 = x_0 \cdot 24 + y_0 \cdot 20 \quad | \quad \text{ID BEZOUT}$$

$$24 = 20 \cdot 1 + 4 \Rightarrow 4 = 24 - 1 \cdot 20 \Rightarrow (x_0, y_0) = (1, -1)$$

$$20 = 5 \cdot 4 + 0$$

paso 3:
$$\begin{aligned} x_1 &= x_0 \cdot k = 1 \cdot 13 \\ y_1 &= y_0 \cdot k = -1 \cdot 13 \end{aligned} \quad \left. \begin{array}{l} \\ \end{array} \right\} (13, -13) \text{ es solución particular.}$$

Verificación: $24 \cdot 13 + 20(-13) = 52$

paso 4:
$$y = y_1 + h \cdot a' \quad (a' = \frac{a}{d})$$

$$y = -13 + 6h \quad h \in \mathbb{Z}$$

$$x = x_1 - h b' \quad (b' = \frac{b}{d})$$

$$x = 13 - 5h$$

todas las soluciones son $(x, y) = (13 - 5h, -13 + 6h)$ donde $h \in \mathbb{Z}$

Corolario 1 del lema de Euclides $(n \in \mathbb{N})$

$$\left. \begin{array}{l} n \mid a \cdot b \\ \text{MCD}(n, a) = 1 \end{array} \right\} \rightarrow n \mid b$$

Demostración:

$$\text{MCD}(n, a) = 1 \Rightarrow \text{MCD}(nb, ab) = b$$

$$\left. \begin{array}{l} \text{Por } \textcircled{H}: n \mid ab \\ \text{también } n \mid nb \end{array} \right\} \Rightarrow n \mid \text{MCD}(nb, ab) = b \Rightarrow n \mid b$$

Corolario 2 $(p \text{ y } q \text{ primos})$

$$\text{Si } p \mid q^m \text{ para algún } m \in \mathbb{N} \Rightarrow p = q$$

Demostración: Por inducción completa en $m \in \mathbb{N}$

$$\left. \begin{array}{l} \text{paso base: Si } m=1 \text{ por } \textcircled{H} \quad p \mid q \\ q \text{ es primo} \Rightarrow 1 \text{ y } q \text{ son los únicos divisores de } q \\ p \text{ es primo} \Rightarrow p \neq 1 \end{array} \right\} \Rightarrow p = q$$

$$\left. \begin{array}{l} \text{paso inductivo: } \textcircled{H} \quad m=h \\ p \mid q^h \\ h \text{ natural fijo} \\ p \text{ y } q \text{ son primos} \end{array} \right\} \Rightarrow p = q$$

$$\left. \begin{array}{l} \textcircled{T} \quad m=h+1 \\ p \mid q^{h+1} \\ p \text{ y } q \text{ son primos} \end{array} \right\} p = q$$

Demostración:

(IC)

$$p \mid q^{h+1} = q \cdot q^h$$

$$p \mid q \cdot q^h \quad \left. \begin{array}{l} \\ \text{Lema Euclides} \end{array} \right\} \Rightarrow p \mid q \text{ ó } p \mid q^h$$

p y q son primos

Si $p \mid q$ por paso base: $p = q$

Si $p \mid q^h$ por (HI): $p = q$

Corolario 3

(p, q_1, q_2, \dots, q_n son primos)

(m_1, \dots, m_h son naturales)

$$\boxed{\text{Si } p \mid q_1^{m_1} \cdot q_2^{m_2} \cdots q_h^{m_h} \Rightarrow p \text{ es igual a algún } q_i}$$

Demostración: Por inducción completa en $h \in \mathbb{N}$

paso base: $h=1$ $p \mid q_1$ son números primos, m_1 es natural.

$$p \mid q_1^{m_1} \xrightarrow{\text{coro 2}} p = q_1$$

paso Inductivo:

(HI) $h=k$

Vale la afirmación

(TI) $h=k+1$

Vale la afirmación

Demostración:

$$p \mid (q_1^{m_1} \cdot q_2^{m_2} \cdots q_k^{m_k}) q_{k+1}^{m_{k+1}} \quad \left. \begin{array}{l} \\ \text{Lema Euclides} \end{array} \right\} \Rightarrow p \mid q_{k+1}^{m_{k+1}} \text{ ó } p \mid q_1^{m_1} \cdots q_k^{m_k}$$

q_{k+1} y p es primo

Si

primer caso $p \mid q_{k+1}^{m_{k+1}}$ coro 2 $\Rightarrow p = q_{k+1}$

Segundo caso

$$p \mid q_1^{m_1} \cdots q_k^{m_k} \xrightarrow{\text{(II)}} p = q_i \text{ para algún } i$$

Definición: Sea $n \in \mathbb{N}$

$n=1$: "Factorización en números primos de n es vacía"
 " $n=1$ no tiene factores primos"

$n \geq 2$: $\rightarrow n$ es primo
 $n=p$

$n = p^1$] la factorización de n en factores primos es p^1

$\rightarrow n$ no es primo

$$\boxed{n = P_1^{m_1} P_2^{m_2} \dots P_h^{m_h}}$$

P_1, P_2, \dots, P_h primos.

m_1, \dots, m_h naturales (≥ 1)

Teorema fundamental de la aritmética

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

Existencia

A_n : " \forall natural $1 < m \leq n \exists$ una factorización de m en números primos"

Demostrar que A_n es verdadero para cada $n \geq 2$ fijo que se elija es equivalente a probar la Existencia en el TEO.

Demostración: Por IC en n .

paso base: $n=2$ ¿ A_2 se cumple? $1 < m \leq 2 \Rightarrow m=2$

Si pues $2 = 2^1$.

paso inductivo: \textcircled{H} A_h es verdadera para $h \geq 2$ fijo

\textcircled{T} A_{h+1} es verdadera

Demostración: Sea m un natural / $1 < m \leq h+1$

Caso 1: si m es primo $\Rightarrow m=p \Rightarrow m=p^1$

Caso 2 : Si m no es primo $\left. \begin{array}{l} m > 1 \\ \exists a \text{ divisor alm } a \neq 1 \text{ y } a \neq m \end{array} \right\} \Rightarrow \exists a \text{ divisor alm } a \neq 1 \text{ y } a \neq m$
 $a \text{ natural.}$

$$\boxed{m = a \cdot b} \Rightarrow 1 < a < m \Rightarrow \frac{m}{1} > \frac{m}{a} > \frac{m}{m} \Rightarrow m > \frac{m}{a} > 1$$

b

$$\Rightarrow \boxed{1 < b < m}$$

$$\text{(I)} \rightarrow \left. \begin{array}{l} m \leq h+1 \\ a < m \\ a \text{ natural} \end{array} \right\} \Rightarrow \boxed{a \leq h}$$

$$\left. \begin{array}{l} m \leq h+1 \\ b < m \\ b \text{ natural} \end{array} \right\} \Rightarrow \boxed{b \leq h}$$

(II) "Ah es verdadera" \forall natural $1 < a \leq n \Rightarrow \exists$ alguna factorización de a en números primos.

$$a = p_1^{m_1} p_2^{m_2} \cdots p_h^{m_h} \quad \begin{array}{l} p_1, p_2, \dots, p_h \text{ primos} \\ m_1, \dots, m_h \text{ naturales} \end{array}$$

$$b = q_1^{n_1} q_2^{n_2} \cdots q_k^{n_k} \quad \begin{array}{l} q_1, \dots, q_k \text{ primos} \\ n_1, \dots, n_k \text{ naturales} \end{array}$$

$$\Rightarrow \frac{a \cdot b}{m} = p_1^{m_1} \cdots p_h^{m_h} q_1^{n_1} \cdots q_k^{n_k}$$

Unicidad

$$\boxed{n = p_1^{m_1} p_2^{m_2} \cdots p_h^{m_h} = q_1^{n_1} q_2^{n_2} \cdots q_k^{n_k}}$$

Paso 1 : Probar que cada p_i es igual a algún q_j

Demostración : $p_i \mid n = q_1^{n_1} q_2^{n_2} \cdots q_k^{n_k}$ $\left. \begin{array}{l} \text{coro3} \\ p_i, q_1, q_2, \dots, q_k \text{ son primos} \end{array} \right\} \Rightarrow p_i \text{ es igual a algún } q_j$

Paso 2 : Probar que cada q_j es igual a algún p_i

Demostración : Análogo.

Por paso 1 y 2, el conjunto de los p_i y el conjunto de los q_j son el mismo.

Paso 3: Para cada $p_i (=q_j)$ la cantidad de veces que aparece en las dos descomposiciones es la misma.

Demostración: $p_1^{m_1} \cdots p_h^{m_h} = q_1^{n_1} \cdots q_k^{n_k}$

Junto todos los p_i y sumo sus exponentes. $m_1 \geq n_1$

$$p_1^{m_1} \cdot p_2^{m_2} \cdots p_h^{m_h} = p_1^{n_1} q_2^{n_2} \cdots q_k^{n_k} = A$$

$$p_1^{m_1 - n_1} \cdot p_2^{m_2} \cdots p_h^{m_h} = q_2^{n_2} \cdots q_k^{n_k} = A$$

Como el conjunto de factores primos de A es único y como p_1 no aparece a la derecha \Rightarrow tampoco puede aparecer a la izquierda

$$\Rightarrow m_1 - n_1 = 0 \Rightarrow m_1 = n_1.$$

Teorema: Existen infinitos números primos

Demostración: Supongamos por absurdo que el conjunto de todos los números primos fuera finito.

Sea $C = \{p_1, \dots, p_h\}$ el conjunto de todos los números primos.

Construyo n natural como $n = (p_1, p_2, \dots, p_h) + 1$

Por el teorema fundamental de la aritmética, existe la factorización del número natural n (que es ≥ 2) en números primos.

Por lo tanto existe algún primo $p_i \in C$ que es divisor de n .

$$\left. \begin{array}{l} p_i \mid n \\ p_i \mid (p_1, p_2, \dots, p_h) \end{array} \right\} \quad p_i \mid n - (p_1, p_2, \dots, p_h) \Rightarrow p_i \mid 1$$

Como el único divisor natural de 1 es 1 y p_i es primo, $p_i \neq 1$ $\{\text{ABS}\}$

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

Demostración: Por (H) n no es primo $\Rightarrow \exists d \in \mathbb{N} / d \mid n$ con $1 < d < n$

$$n = d \cdot h \quad h = \frac{n}{d} \quad h \in \mathbb{Z}$$

$$\text{por otro lado } 1 < d < n = \frac{n}{1} > \frac{n}{d} > \frac{n}{n} = 1 < h < n$$

$\swarrow h$

Para fijar ideas supongo que $d \leq h$.

$$n = d \cdot h \geq d \cdot d \Rightarrow n \geq d^2 \Rightarrow \sqrt{n} \geq d$$

Hemos probado que existe d' divisor de n con $1 < d < \sqrt{n}$, d natural.

Por el teorema fundamental de la aritmética sabemos que existe p' primo un divisor de d

$$\left. \begin{array}{l} p' | d \\ d | n \end{array} \right\} \Rightarrow p' | n$$

Ejemplo: Verificar que 127 es primo

$$\sqrt{127} = 11, \dots$$

Los posibles factores primos son entonces: 2, 3, 5, 7, 11

$2 \nmid 127, 3 \nmid 127, 5 \nmid 127, 7 \nmid 127, 11 \nmid 127 \Rightarrow 127$ es primo.

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

El $\text{MCD}(a, b)$ 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.

Demonstración:

Llamo h al número natural construido usando la receta.

El objetivo es demostrar que $h = \text{MCD}(a, b)$

$$a = p_1^{m_1} \cdots p_n^{m_n}$$

$$b = p_1^{m'_1} \cdots p_r^{m'_r}$$

$$h = q_1^{n_1} \cdots q_s^{n_s}$$

Por la construcción de h ,

h es un divisor común de a y b .

$$a = h \cdot a'$$

$$b = h \cdot b'$$

a' y b' con coprimos.

Supongamos por absurdo que a' y b' no son coprimos, entonces existe d divisor común de a' y b' , con $d > 1$.

Entonces, por el teorema fundamental de la aritmética existe p divisor de d.

$$\left. \begin{array}{l} p|d \\ p|a' \\ p|b' \end{array} \right\} \Rightarrow p \text{ es un factor primo común a } a' \text{ y } b'.$$

Pero $a' = \frac{a}{h}$ y $b' = \frac{b}{h} \Rightarrow p$ es un factor primo de $\frac{a}{h}$ y $\frac{b}{h}$, ABSURDO por construcción de h.

$$\left. \begin{array}{l} a = h \cdot a' \\ b = h \cdot b' \\ a' \text{ y } b' \text{ coprimos} \end{array} \right\} \Rightarrow h = \boxed{\text{MCD}(a, b)}$$

Ejemplo : $615 = 3 \cdot 5 \cdot 41$ $1845 = 3^2 \cdot 5 \cdot 41$ $\Rightarrow \text{MCD}(615, 1845) = 3 \cdot 5 \cdot 41 = 615$

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

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

No tiene por qué ser común a ambas factorizaciones.

Demostración : Ejercicio.

Congruencias módulo n: "Los enteros módulo n"Ejemplo: Un reloj

Si la aguja de las horas avanza 13 lugares = Si avanza 1 lugar = Si avanza 25 lugares = retroceder 11 lugares = retroceder 23 lugares = ...

$$\text{Avanzar } \overset{=}{0} \text{ lugares} = \{ 0, 12, 24, 36, \dots, -12, \dots \}$$

$$\text{Avanzar } \overset{=}{1} \text{ lugar} = \{ 1, 13, 25, \dots, -11, \dots \}$$

$$\text{Avanzar } \overset{=}{2} \text{ lugares} = \{ 2, 14, 26, \dots \}$$

$$\text{Avanzar } \overset{=}{11} \text{ lugares} = \{ 11, 23, \dots, -11, \dots \}$$

Queremos encontrar una buena forma tal que los números en cada conjunto sean "iguales" en algún sentido.

Vamos a decir que dos enteros dentro del mismo conjunto son Congruentes módulo 12

Definición: Dado $n \in \mathbb{Z}$ (fijo) y $a, b \in \mathbb{Z}$.

Decimos que a es congruente con b módulo $n \iff n \mid b-a$

Notación: $a \equiv b \pmod{n}$

Ejemplo: $n = 12$ (reloj)

$$12 \equiv 0 \pmod{12} \quad (12|12-0)$$

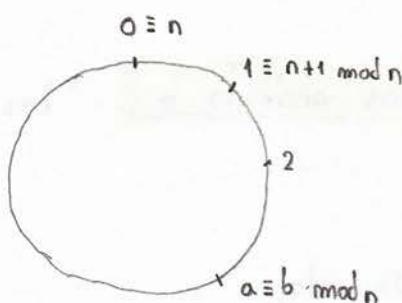
$$12 \equiv 24 \pmod{12} \quad (12|24-12)$$

$$13 \equiv 1 \pmod{12}$$

$$25 \equiv 1 \pmod{12}$$

$$37 \equiv 1 \pmod{12}$$

$$37 \equiv 13 \pmod{12}$$



$a \equiv b \pmod{n} \iff$ El lugar final
a avanzar "a"
lugares

= El lugar final
a avanzar "b"
lugares

Ejemplo:

* Si $n=0$, (no hay reloj)

$$a \equiv b \pmod{0} \iff 0 | b-a \iff a=b$$

* Si $n=1$

$$a \equiv b \pmod{1} \iff 1 | b-a \quad \text{Es decir, } a \equiv b \pmod{1} \quad \forall a, b \in \mathbb{Z}$$

Obs: $a \equiv b \pmod{-n} \iff a \equiv b \pmod{n}$
 $-n | b-a \qquad \qquad \qquad n | b-a$

Por eso generalmente se considera
 $n \in \mathbb{N}$.

Propiedades

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

Demostración: $a - r = q \cdot n \Rightarrow n | a - r \Rightarrow a \equiv r \pmod{n}$

"Todo entero es congruente módulo n, con el resto de dividirlo entre n"

②

$$a = q_1 n + r_1$$

$$b = q_2 n + r_2$$

$$a \equiv b \pmod{n} \Leftrightarrow r_1 = r_2$$

$$0 \leq r_1, r_2 < |n|$$

Demostración:

$$(\Rightarrow) \text{ Si } a \equiv b \pmod{n} \Rightarrow n \mid b-a \Rightarrow n \mid n(q_2 - q_1) + r_2 - r_1 \Rightarrow n \mid r_2 - r_1$$

$$\left. \begin{array}{l} r_2 - r_1 = c \cdot n \quad c \in \mathbb{Z} \\ 0 \leq r_2 - r_1 < n \end{array} \right\} \Rightarrow \left. \begin{array}{l} 0 \leq c \cdot n < n \\ c \in \mathbb{Z} \end{array} \right\} \Rightarrow c = 0 \Rightarrow r_2 - r_1 = 0 \Rightarrow r_1 = r_2$$

$$(\Leftarrow) \text{ Si } r_1 = r_2 \Rightarrow b-a = q_2 n + r_2 - q_1 n - r_1 \Rightarrow b-a = n(q_2 - q_1)$$

$$\Rightarrow n \mid b-a \Rightarrow a \equiv b \pmod{n}$$

Ejemplo: $n=5$

$a \in \mathbb{Z} \Rightarrow$ restos posibles conjuntos

$$a \equiv 0 \pmod{5} \longrightarrow \{a / a \equiv 0 \pmod{5}\} = \{k \cdot 5 \mid k \in \mathbb{Z}\} = [0] = \bar{0}$$

$$a \equiv 1 \pmod{5} \longrightarrow \{a / a \equiv 1 \pmod{5}\} = \{k \cdot 5 + 1 \mid k \in \mathbb{Z}\} = [1] = \bar{1}$$

$$a \equiv 2 \pmod{5} \longrightarrow \{a / a \equiv 2 \pmod{5}\} = \{k \cdot 5 + 2 \mid k \in \mathbb{Z}\} = [2] = \bar{2}$$

$$a \equiv 3 \pmod{5} \longrightarrow \{a / a \equiv 3 \pmod{5}\} = \{k \cdot 5 + 3 \mid k \in \mathbb{Z}\} = [3] = \bar{3}$$

$$a \equiv 4 \pmod{5} \longrightarrow \{a / a \equiv 4 \pmod{5}\} = \{k \cdot 5 + 4 \mid k \in \mathbb{Z}\} = [4] = \bar{4}$$

Obs: ① $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3] \cup [4]$

② Un entero no puede pertenecer a 2 conjuntos.

(Por unicidad del resto) Estos subconjuntos: $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$ son disjuntos.

Proposición: Dado n fijo.

La congruencia módulo n es una relación de equivalencia.

Demostración:

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

$$n|a-a \Rightarrow n|0 \quad \checkmark$$

Simétrica: $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

$$n|b-a \Rightarrow -n|a-b \Leftrightarrow n|a-b \Leftrightarrow b \equiv a \pmod{n}$$

Transitiva: $\begin{cases} a \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{cases} \Rightarrow a \equiv c \pmod{n}$

$$\begin{cases} n|b-a \\ n|c-b \end{cases} \Rightarrow n|b-a+c-b = n|c-a \Rightarrow a \equiv c \pmod{n}$$

Corolario: Las clases de equivalencia módulo n son una partición de \mathbb{Z} .

Notación: "La clase de a módulo n " = $\bar{a} = [a] = [a]_n$

Obs: $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \dots \cup \bar{n-1}$

Al conjunto de las clases de equivalencia $\{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$ se le llama Enteros módulo n y la notación es \mathbb{Z}_n

Propiedades: Sean $a \equiv b \pmod{n}$ y $a' \equiv b' \pmod{n}$

① $a+a' \equiv b+b' \pmod{n}$

② Si $c \in \mathbb{Z} \Rightarrow \begin{cases} ca \equiv cb \pmod{n} \\ ca \equiv cb \pmod{cn} \end{cases}$

③ $aa' \equiv bb' \pmod{n}$

Demostración: $n|b-a$ y $n|b'-a'$

$$bb' - aa' = bb' - ba' + ba' - aa' = b(b' - a') + a'(b - a) \Rightarrow n|bb' - aa' \Rightarrow aa' \equiv bb' \pmod{n}$$

Corolarios

$$\textcircled{1} \quad a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}, \quad \forall k \in \mathbb{N}$$

$$\textcircled{2} \quad a \equiv b \pmod{n}$$

$\left. \begin{array}{l} P(z) = a_0 + a_1 z + \dots + a_k z^k \\ \text{con } a_i \in \mathbb{Z} \end{array} \right\} \Rightarrow P(a) \equiv P(b) \pmod{n}$

Aplicación: Criterios de divisibilidad

Entre 3: Un entero es divisible entre 3 \Leftrightarrow la suma de sus dígitos es 3

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

$$a = a_k \dots a_1 a_0 \quad \text{Vamos a probar } a \equiv a_k + \dots + a_1 + a_0 \pmod{3}$$

$$\text{Demostración: } a = a_k \cdot 10^k + \dots + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0$$

$$10 \equiv 1 \pmod{3} \Rightarrow a \equiv a_k \cdot 1^k + \dots + a_1 \cdot 1 + a_0 \pmod{3}$$

$$\text{por corolario} \quad a \equiv a_k + \dots + a_0 \pmod{3}$$

Recordamos: $a \equiv b \pmod{n} \iff n | b - a$

$$\text{prop: } \left. \begin{array}{l} a \equiv b \pmod{n} \\ c \in \mathbb{Z} \end{array} \right\} \Rightarrow ca \equiv cb \pmod{n}$$

6 Vale el reciproco?

6 Cuando puedo cancelar c?

Ejemplos

① $10 \equiv 4 \pmod{6}$

$$2 \times 5 \equiv 2 \times 2 \pmod{6}$$

No podemos cancelar el 2, $5 \not\equiv 2 \pmod{6}$.

Obs: $5 \equiv 2 \pmod{3}$

② $10 \equiv 4 \pmod{3}$

$$2 \times 5 = 2 \times 2 \pmod{3}$$

y es cierto que $5 \equiv 2 \pmod{3}$

③ $12 \equiv 32 \pmod{10}$

$$4 \times 3 = 4 \times 8 \pmod{10}$$

$3 \not\equiv 8 \pmod{10}$, no puedo cancelar el 4 sin cambiar el módulo.

$3 \equiv 8 \pmod{5}$.

Propiedades

① $ca \equiv cb \pmod{cn} \Rightarrow a \equiv b \pmod{n}$

$c \neq 0$

Demostración: $ca \equiv cb \pmod{cn} \stackrel{\text{def}}{\iff} cn \mid cb - ca \iff cb - ca = cnk$

$$\iff b - a = nk \stackrel{\text{def}}{\iff} a \equiv b \pmod{n}$$

② Si $ca \equiv cb \pmod{n}$

$$\left. \begin{array}{l} c \neq 0 \\ \text{MCD}(c, n) = 1 \end{array} \right\} \Rightarrow a \equiv b \pmod{n}$$

Demostración: $ca \equiv cb \pmod{n} \stackrel{\text{def}}{\iff} n \mid cb - ca \iff n \mid c(b-a)$

$$\left. \begin{array}{l} n \mid c(b-a) \\ \text{MCD}(n, c) = 1 \\ c \neq 0 \end{array} \right\} \stackrel{\text{Lema Euclides}}{\Rightarrow} n \mid b-a \stackrel{\text{def}}{\iff} a \equiv b \pmod{n}$$

Ejemplo:

$$12 \equiv 32 \pmod{10}$$

$$2 \times 6 \equiv 2 \times 16 \pmod{10} \stackrel{\text{①}}{\iff} 6 \equiv 16 \pmod{5} \Rightarrow 2 \times 3 = 2 \times 8 \pmod{5}$$

$$\text{y como } \text{MCD}(2, 5) = 1 \stackrel{\text{②}}{\iff} 3 \equiv 8 \pmod{5}$$

Teorema

(H) $ca \equiv cb \pmod{n}$
 $c \neq 0$

(T) $a \equiv b \pmod{\frac{n}{d}}$
donde $d = \text{MCD}(c, n)$

Demostración:

$$c = d \cdot c' \quad \text{MCD}(c', n') = 1$$

$$n = d \cdot n'$$

$$ca \equiv cb \pmod{n} \iff d \cdot c' \cdot a \equiv d \cdot c' \cdot b \pmod{d \cdot n'} \stackrel{\substack{d \neq 0, c \neq 0 \\ \text{prop. ①}}}{\Rightarrow} c' \cdot a \equiv c' \cdot b \pmod{n'}$$

$$\left. \begin{array}{l} \text{prop. ②} \\ \text{MCD}(c', n') = 1 \\ n' = \frac{n}{d} \end{array} \right\} \Rightarrow a \equiv b \pmod{\frac{n}{d}}$$

Obs.: Si $\text{med}(c, n) \neq 1$

Siempre existe a y b tales que $a \not\equiv b \pmod{n}$ y $ca \equiv cb \pmod{n}$

$$5 \not\equiv 2 \pmod{6} \quad y \quad 2 \times 5 \equiv 2 \times 2 \pmod{6}$$

Ejemplos inversas, cancelativas:① En \mathbb{R}

$$\left. \begin{array}{l} ca = cb \\ c \neq 0 \end{array} \right\} \Rightarrow a = b$$

Demostración:

$$ca = cb$$

$$\text{como } c \neq 0 \Rightarrow \text{existe } \frac{1}{c} \Rightarrow \frac{1}{c}(ca) = \frac{1}{c}(cb)$$

$$\left(\frac{1}{c}c \right)a = \left(\frac{1}{c}c \right)b \Rightarrow 1 \cdot a = 1 \cdot b$$

② $C, A, B \in M_{n \times n}(\mathbb{R})$

$$\left. \begin{array}{l} CA = CB \\ C \text{ es invertible (det} \neq 0 \text{)} \end{array} \right\} \Rightarrow \exists C^{-1} \Rightarrow C^{-1}(CA) = C^{-1}(CB) \\ (C^{-1}C)A = (C^{-1}C)B \Rightarrow A = B$$

Definición: Decimos que un entero c es invertible módulo n si existe $e \in \mathbb{Z}$ tal que $c \cdot e \equiv 1 \pmod{n}$

Ejemplos:① 0 no es invertible módulo n si $n \neq 1$

$$0 \cdot e \equiv 1 \pmod{n} \Rightarrow 0 \equiv 1 \pmod{n} \stackrel{\text{def}}{\iff} n \mid 1 - 0 \Leftrightarrow n \mid 1 \Leftrightarrow n = 1$$

② 1 es invertible módulo n

$$1 \cdot 1 \equiv 1 \pmod{n}$$

③ módulo 3, ¿2 es invertible módulo 3?

$$2 \cdot e \equiv 1 \pmod{3} \Rightarrow 2 \cdot 2 \equiv 1 \pmod{3} \quad \checkmark$$

$$\Rightarrow 2 \cdot 5 \equiv 1 \pmod{3}$$

$$2 \cdot 8 \equiv 1 \pmod{3}$$

Obs: si $c \cdot e \equiv 1 \pmod{n} \Rightarrow c(e + k \cdot n) \equiv 1 \pmod{n}$

"El inverso de c módulo n " = $\exists e \mid ce \equiv 1 \pmod{n}$ no es único

Por ejemplo 2, 5, 8 son inversos de 2 módulo 3.

Propiedad

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

Demostración:

$$\left. \begin{array}{l} ce \equiv ce' \pmod{n} \\ cece \equiv ce'e' \pmod{n} \\ ce \equiv 1 \pmod{n} \end{array} \right\} \Rightarrow 1e \equiv 1e' \pmod{n} \Rightarrow e \equiv e' \pmod{n}$$

El inverso de c módulo n es único pero módulo n .

Ejemplo: Invertibles módulo 6

$$2 \cdot 0 \not\equiv 1 \pmod{6}$$

$$2 \cdot 1 \not\equiv 1 \pmod{6}$$

$$2 \cdot 2 \not\equiv 1 \pmod{6}$$

$$2 \cdot 3 \not\equiv 1 \pmod{6}$$

$$2 \cdot 4 \not\equiv 1 \pmod{6}$$

$$2 \cdot 5 \not\equiv 1 \pmod{6}$$

$\Rightarrow 2$ no es invertible módulo 6.

Los únicos enteros entre 1 y 6 invertibles módulo 6 son 1, 5.

$$5 \cdot 5 \equiv 1 \pmod{6}.$$

Ejemplo : 6 231 es invertible módulo 311?

$$231 \text{ es invertible módulo } 311 \stackrel{\text{def}}{\iff} \exists e \in \mathbb{Z} / 231 \cdot e \equiv 1 \pmod{311}$$

$$\iff \exists e / 311 | 231e - 1 \iff \exists e, k \in \mathbb{Z} / 231e - 1 = 311k$$

$$\iff 231e - 311k = 1 \iff \text{mcd}(231, 311) = 1$$

Teorema

$$c \text{ es invertible módulo } n \iff \text{mcd}(c, n) = 1$$

Además, si $\text{mcd}(c, n) = 1 \implies$ existen $e, k \in \mathbb{Z} / ce - nk = 1 \implies ce \equiv 1 \pmod{n}$

(Bezout)

Ecuaciones con congruencias

Nos interesa saber cuando una ecuación $cx \equiv b \pmod{n}$ tiene solución ($c, b, n \in \mathbb{Z}$) entera y cuantas soluciones módulo n hay.

Ejemplo:

$$\textcircled{1} \quad 4x \equiv 3 \pmod{6}$$

probando a mano:

$$x=0 \quad 4 \cdot 0 \not\equiv 3 \pmod{6}$$

$$x=4 \quad 4 \cdot 4 \not\equiv 3 \pmod{6}$$

$$x=1 \quad 4 \cdot 1 \not\equiv 3 \pmod{6}$$

$$x=5 \quad 4 \cdot 5 \not\equiv 3 \pmod{6}$$

$$x=2 \quad 4 \cdot 2 \not\equiv 3 \pmod{6}$$

La ecuación no tiene solución.

$$x=3 \quad 4 \cdot 3 \not\equiv 3 \pmod{6}$$

Usando la definición:

$$4x \equiv 3 \pmod{6} \iff 6 \mid 4x - 3 \iff 4x - 3 = 6 \cdot k \quad k \in \mathbb{Z} \iff [4x - 6k = 3]$$

no tiene sol
no tiene solución porque

$$\text{MCD}(4, 6) \neq 3$$

$$\textcircled{2} \quad 4x \equiv 2 \pmod{6}$$

Tiene soluciones: $x = 2$ y $x = 5$

Son 2 soluciones distintas ($2 \not\equiv 5 \pmod{6}$)

Hay infinitas: $x = 2 + 6k^1$

$$x = 5 + 6k^1$$

Otra forma de verlo es con la ecuación diofántica: $4x - 6k = 2$

Salución particular: $x_0 = 2$ todas las soluciones son: $x = 2 + \frac{6}{2}\alpha$, $\alpha \in \mathbb{Z}$
 $k_0 = 1$ $k = 1 + \frac{4}{2}\alpha$, $\alpha \in \mathbb{Z}$

$$x = 2 + 3\alpha$$

$$\text{Si } \alpha \text{ es par, } \alpha = 2k^1 \implies x = 2 + 6k^1$$

$$\text{Si } \alpha \text{ es impar, } \alpha = 2k^1 + 1 \implies x = 2 + 3(2k^1 + 1) = 5 + 6k^1$$

Teorema: Dados $c, n, b \in \mathbb{Z}$

La ecuación $cx \equiv b \pmod{n}$ tiene solución entera $\iff \text{MCD}(c, n) | b$

Además si $d = \text{MCD}(c, n)$, si existen soluciones, hay exactamente d soluciones distintas módulo n .

Demonstración:

Teo de ec diofánticas

$$\exists x \in \mathbb{Z} / cx \equiv b \pmod{n} \iff \exists x, k \in \mathbb{Z} / cx - nk = b \iff \text{MCD}(c, n) | b$$

Obs: El caso de c invertible módulo $n \iff \text{MCD}(c, n) = 1$

Es un caso particular de este teorema con $b=1$.

Obs: Por el teo de ec diofánticas, cuando $d = \text{MCD}(c, n) | b$, si (x_0, k_0) es solución, todas las soluciones son:

$$\begin{aligned} x &= x_0 + \frac{n}{d} \cdot \alpha \\ k &= k_0 + \frac{c}{d} \cdot \alpha \quad \alpha \in \mathbb{Z} \end{aligned}$$

\Rightarrow Todas las soluciones de $cx \equiv b \pmod{n}$ son: $x = x_0 + \left(\frac{n}{d}\right) \alpha, \alpha \in \mathbb{Z}$

Obs:

$$\left. \begin{array}{l} x_0 + 0 \cdot n' \\ x_0 + 1 \cdot n' \\ \vdots \\ x_0 + (d-1)n' \end{array} \right\}$$

Hay d , no son congruentes entre ellas módulo n .

Demonstración: $x_0 + \alpha_1 n' - (x_0 + \alpha_2 n') = (\alpha_1 - \alpha_2) n'$

$$0 \leq \alpha_1, \alpha_2 \leq d-1, \alpha_1 \neq \alpha_2, |\alpha_1 - \alpha_2| < d$$

$$\Rightarrow 0 < |(\alpha_1 - \alpha_2) n'| < d \cdot n' = n \Rightarrow n \nmid (x_0 + \alpha_1 n') - (x_0 + \alpha_2 n')$$

Además si $\alpha \geq d \Rightarrow \alpha = qd + r \quad 0 \leq r < d$

$$\Rightarrow n\alpha = qn'd + nr \Rightarrow x_0 + n\alpha' \equiv x_0 + nr \pmod{n}$$

Es decir:

$$\left\{ \begin{array}{l} x_0 + 0 \cdot n \\ \vdots \\ x_0 + (d-1)n \end{array} \right.$$

Son todas las soluciones distintas módulo n.

Ejemplo:

$$2x \equiv 4 \pmod{12}$$

Tiene solución? $\iff \text{MCD}(2, 12) \mid 4$

$$\begin{aligned} x_0 &= 2 & (\alpha=0) & \text{son las únicas soluciones} \\ x_0 &= 2 + 6 = 8 & (\alpha=1) & \text{módulo 12.} \end{aligned}$$

Todas las soluciones son $x = x_0 + \frac{n}{d}\alpha = 2 + 6\alpha$

Ecuaciones Congruentes

Ejemplo: Mirando el cielo observamos satélites.

- A los 3 meses vemos al satélite s_1 , que tiene período de 5 meses.
- A los 7 meses " " " s_2 , " " " 12 meses.
- A los 11 " " " " s_3 , " " " 13 meses.

Queremos saber si veremos a los 3 al mismo tiempo.

X = cantidad de meses que pasan hasta ver a los 3 juntos (Desde que empece a mirar)

$$X = 3 + 5k \quad k \in \mathbb{Z} \quad \text{porque en } X \text{ veo a } s_1$$

Es decir:

$$\left\{ \begin{array}{l} X \equiv 3 \pmod{5} \quad (s_1) \\ X \equiv 7 \pmod{12} \quad (s_2) \\ X \equiv 11 \pmod{13} \quad (s_3) \end{array} \right.$$

Esto se puede resolver con ecuaciones diofánticas y vamos a ver otra forma de resolverlo.

$$\text{Tomo: } \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 7 \pmod{12} \end{cases} \iff \begin{cases} x = 3 + 5\alpha & \alpha \in \mathbb{Z} \\ x = 7 + 12\beta & \beta \in \mathbb{Z} \end{cases}$$

$$\text{igualando: } 3 + 5\alpha = 7 + 12\beta \Rightarrow 5\alpha - 12\beta = 4$$

En este caso, tenemos solución porque $\text{MCD}(5, 12) = 1 \mid 4$

$$\alpha_0 = -4 \quad y \quad \beta_0 = -2 \quad \text{por ejemplo.}$$

Todas las soluciones son:

$$\boxed{\begin{aligned} \alpha &= -4 + 12k \\ \beta &= -2 + 5k \end{aligned}}$$

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 7 \pmod{12} \end{cases} \iff \begin{cases} x = 3 + 5\alpha \\ \alpha = -4 + 12k \end{cases} \iff x = 3 + 5(-4 + 12k) \quad k \in \mathbb{Z}$$

$$\iff x = 3 - 20 + 5 \cdot 12k \iff x = -17 + 60k \iff x \equiv -17 \pmod{60} \iff \boxed{x \equiv 43 \pmod{60}}$$

Obs:

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 7 \pmod{12} \end{cases} \iff x \equiv 43 \pmod{60}$$

Se resuelve ahora:

$$\begin{cases} x \equiv 43 \pmod{60} \\ x \equiv 11 \pmod{13} \end{cases}$$

6) Esto tiene solución?

$$43 + 60\alpha = 11 + 13\beta \Rightarrow 60\alpha - 13\beta = 11 - 43$$

Tiene solución porque $\text{MCD}(60, 13) = 1 \mid 11 - 43$

Teorema chino de los restos

Si m_1, m_2, \dots, m_k son enteros coprimos 2 a 2 ($\text{MCD}(m_i, m_j) = 1$)

Entonces el sistema:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

\Rightarrow tiene solución.

Si x_0 es solución, toda solución es $x \equiv x_0 \pmod{(m_1, \dots, m_k)}$

(La solución es única módulo m_1, \dots, m_k)

Teorema chino de los restos

Sean $m_1, m_2, \dots, m_k \in \mathbb{Z}$ coprimos 2 a 2 ($\text{MCD}(m_i, m_j) = 1$) y $a_1, a_2, \dots, a_k \in \mathbb{Z}$.

Entonces el sistema:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

Tiene solución entera.

Si x, x' son soluciones $\Rightarrow x \equiv x' \pmod{(m_1 \dots m_k)}$
(La solución es única módulo $m_1 \dots m_k$)

Demostración: Inducción en k .

paso base: $k=2$

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

El sistema tiene solución $\Leftrightarrow \exists x \in \mathbb{Z} / \underbrace{a_1 + \alpha m_1 \equiv a_2}_{\text{Ec 1}} \pmod{m_2}$

$$a_1 + \alpha m_1 \equiv a_2 \pmod{m_2} \Leftrightarrow \exists x \in \mathbb{Z} / m_1 \alpha \equiv a_2 - a_1 \pmod{m_2}$$

y esto tiene solución porque $\text{MCD}(m_1, m_2) = 1$
(Teorema de ecuaciones $ax \equiv b \pmod{n}$)

paso inductivo: Si tenemos k ecuaciones

El sistema con $k-1$ ecuaciones tiene solución x_0 por (H) y cualquier solución x cumple $x \equiv x_0 \pmod{(m_1 \dots m_{k-1})}$

El sistema:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_{k-1} \pmod{k-1} \\ x \equiv a_k \pmod{k} \end{cases}$$

N

$$\begin{cases} x = x_0 \pmod{(m_1 \dots m_{k-1})} \\ x \equiv a_k \pmod{m_k} \end{cases}$$

y como $\text{MCD}(m_k, m_i) = 1$
 $\forall i = 1, \dots, k-1$

\Rightarrow El sistema tiene solución única módulo $(m_1 \dots m_{k-1}) m_k$

Caso 2 ecuaciones

Unicidad de las soluciones

$$\text{Si } x \text{ y } x' \text{ son soluciones del sistema} \Rightarrow \begin{cases} x \equiv a_1 \pmod{m_1} \\ x' \equiv a_1 \pmod{m_1} \end{cases}$$

$$\Rightarrow x \equiv x' \pmod{m_1} \Rightarrow m_1 | x - x' \quad \left\{ \begin{array}{l} \text{Análogamente } m_2 | x - x' \\ \text{y} \end{array} \right. \quad \left. \begin{array}{l} \text{MCD}(m_1, m_2) = 1 \\ \Rightarrow m_1, m_2 | x - x' \Rightarrow x \equiv x' \pmod{m_1, m_2} \end{array} \right.$$

Otra forma de hallar soluciones

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 7 \pmod{12} \end{cases} \quad \text{Buscamos } x_0 \text{ una solución particular (cualquier otra es } x \equiv x_0 \pmod{60})$$

Como $\text{MCD}(5, 12) = 1 \Rightarrow x_0 = \alpha_{12} + \beta_5 \quad \alpha, \beta \in \mathbb{Z}$

(Bezout)

Obs:

$$\alpha_{12} + \beta_5 \equiv \alpha_{12} \pmod{5} \quad \alpha_{12} + \beta_5 \equiv \beta_5 \pmod{12}$$

$$\text{Buscamos } \alpha / \alpha_{12} \equiv 3 \pmod{5}$$

$$\text{Buscamos } \beta / \beta_5 \equiv 7 \pmod{12}$$

Obs: $\text{MCD}(5, 12) = 1 \Rightarrow 12$ es invertible módulo 5.

$$\Rightarrow \exists \gamma / 12\gamma \equiv 1 \pmod{5}$$

Entonces, para resolver $\alpha_{12} \equiv 3 \pmod{5}$ multiplicamos por "El inverso de 12 módulo 5"

$$\alpha_{12}\gamma \equiv 3\gamma \pmod{5} \Rightarrow \alpha \equiv 3\gamma \pmod{5}$$

Análogamente, para despejar β , multiplicamos por "un inverso de 5 módulo 12"

$$\text{Es decir, } \delta / 5\delta \equiv 1 \pmod{12} \quad (\exists \delta \text{ porque } \text{MCD}(5, 12) = 1)$$

$$\Rightarrow \beta \equiv 7\delta \pmod{12}$$

$$x_0 \equiv 3\gamma_{12} + 7\delta_5 \text{ es solución}$$

$$x_0 = 3(-2)12 + 7 \cdot 5 \cdot 5$$

$$\gamma \cdot 12 \equiv 1 \pmod{5}$$

$$\delta \cdot 5 \equiv 1 \pmod{12}$$

es solución y todas las soluciones

$$\gamma \cdot 2 \equiv 1 \pmod{5}$$

$$\delta = 5$$

son: $x \equiv x_0 \pmod{60}$

$$\gamma = 3 \circ \gamma = -2$$

$$(\text{Esto puede necesitar AEE})$$

Propiedad: Si $\text{MCD}(m_1, m_2) = 1$

Las soluciones de $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$ son: $X \equiv a_1 \alpha_1 m_2 + a_2 \alpha_2 m_1 \pmod{m_1, m_2}$

con $\alpha_1 m_2 \equiv 1 \pmod{m_1}$
 $\alpha_2 m_1 \equiv 1 \pmod{m_2}$

Demostración:

$$\begin{aligned} a_1 \alpha_1 m_2 + \underbrace{a_2 \alpha_2 m_1} &\equiv \underbrace{a_1 \alpha_1 m_2} \pmod{m_1} \equiv a_1 \pmod{m_1} \\ &\equiv 0 \pmod{m_1} \quad \stackrel{!}{\equiv} 1 \pmod{m_1} \end{aligned}$$

$$\begin{aligned} a_1 \alpha_1 m_2 + a_2 \underbrace{\alpha_2 m_1} &\equiv a_2 \pmod{m_2} \\ &\equiv 0 \pmod{m_2} \quad \equiv 1 \pmod{m_2} \end{aligned}$$

Con 3 ecuaciones:

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 7 \pmod{11} \\ x \equiv 11 \pmod{13} \end{cases}$$

Buscamos una solución particular:

$$X = 3 \cdot \alpha_1 \cdot 11 \cdot 13 + 7 \alpha_2 \cdot 13 \cdot 5 + 11 \alpha_3 \cdot 11 \cdot 5$$

$$\alpha_1 \cdot 11 \cdot 13 \equiv 1 \pmod{5} \quad \alpha_2 \cdot 13 \cdot 5 \equiv 1 \pmod{11}$$

$$(11, 13 \text{ y } 5 \text{ son coprimos}) \quad \alpha_3 \cdot 11 \cdot 5 \equiv 1 \pmod{13}$$

$$\alpha_1 \cdot 11 \cdot 13 \equiv 1 \pmod{5}$$

$$\alpha_2 \cdot 13 \cdot 5 \equiv 1 \pmod{11}$$

$$\alpha_1 \cdot 1 \cdot 3 \equiv 1 \pmod{5}$$

$$\alpha_2 \cdot 2 \cdot 5 \equiv 1 \pmod{11}$$

$$\boxed{\alpha_1 = 2}$$

$$\alpha_2 \cdot 10 \equiv 1 \pmod{11}$$

$$\alpha_2 \cdot -1 \equiv 1 \pmod{11}$$

$$\Rightarrow \boxed{\alpha_2 = -1}$$

$$\alpha_3 \cdot 5 \cdot 11 \equiv 1 \pmod{13}$$

$$\alpha_3 \cdot 5 \cdot -2 \equiv 1 \pmod{13}$$

$$\alpha_3 \cdot 3 \equiv 1 \pmod{13} \Rightarrow \boxed{\alpha_3 = 9}$$

Generalización:

Si m_1, \dots, m_k son enteros primos entre sí y $a_1, \dots, a_k \in \mathbb{Z}$, Entonces:

Una solución del sistema:

$$\left\{ \begin{array}{l} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{array} \right.$$

Es
$$x = a_1 \alpha_1 M_1 + a_2 \alpha_2 M_2 + \dots + a_k \alpha_k M_k$$

Donde $M_i = \frac{m_1 \dots m_k}{m_i} = \prod_{j \neq i} m_j$

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

Pequeno teorema de FermatParte 1Sea $a \in \mathbb{Z}$.

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

Demostración:* Si $a = 0$

$$a^p = 0^p \equiv 0 \equiv a \pmod{p}$$

* Si $a > 0$ Se demostrará por IC en a .paso base: $| a=1 |$

$$a^p = 1^p = 1 = a \Rightarrow a^p \equiv a \pmod{p}$$

paso inductivo:(H) para cierto natural a se cumple

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

(T) se cumple para el siguiente:

$$(a+1)^p \equiv (a+1) \pmod{p}$$

Demostración:

$$\left. \begin{array}{l} \text{En el práctico 4} \\ \text{dado } p \text{ primo, } \forall a, b \in \mathbb{Z} \end{array} \right\} (a+b)^p \equiv a^p + b^p \pmod{p}$$

$$\left. \begin{array}{l} (a+1)^p \equiv a^p + 1^p \equiv a^p + 1 \pmod{p} \\ \text{por (H)} \quad a^p \equiv a \pmod{p} \end{array} \right\} \Rightarrow a^p + 1 \equiv a + 1 \pmod{p}$$

$$\Rightarrow (a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p} \Rightarrow \boxed{(a+1)^p \equiv a+1 \pmod{p}} \quad \text{LQD}$$

* Si $a < 0$

$$a = -|a| \quad a^p = (-|a|)^p = (-1)^p (|a|)^p \equiv (-1)(|a|)^p \pmod{p}$$

$$\text{Si } p \text{ primo} \quad (-1)^p \equiv -1 \pmod{p}$$

$$a = -|a| = (-1)|a| \pmod{p}$$

Si pruebo que $|a|^p \equiv |a| \pmod{p} \Rightarrow$ deduzco que $(-1)(|a|)^p \equiv (-1)|a| \pmod{p}$
 $\iff a^p \equiv a \pmod{p}$

Parte 2:

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

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

Demostración:

por parte 1 $a^p \equiv a \pmod{p}$ p es primo $\Rightarrow p \geq 2 \Rightarrow p-1 \in \mathbb{N}$

$$a^p = \underbrace{a \cdot a \dots a}_{p \text{ veces}} = \underbrace{(a \dots a) \cdot a}_{p-1 \text{ veces}}$$

$$\left. \begin{array}{l} a^p = a^{p-1} \cdot a \\ a^p \equiv a = 1 \cdot a \pmod{p} \end{array} \right\} \Rightarrow \left. \begin{array}{l} a^{p-1} \cdot a \equiv 1 \cdot a \pmod{p} \\ \text{por (H) } \text{MCD}(p, a) = 1 \end{array} \right\} \Rightarrow \boxed{a^{p-1} \equiv 1 \pmod{p}}$$

propiedad cancelativa.

Ejemplo

Sea $a = 5$ y $p = 3$

$$\text{Hallar } 5^{-1} \pmod{3} \quad \text{por Fermat part 2} \quad a^{p-1} \equiv 1 \pmod{p} \Rightarrow 5^2 \equiv 1 \pmod{3} \Rightarrow 5 \cdot 5 \equiv 1 \pmod{3}$$

$$\Rightarrow 5 \equiv 5^{-1} \pmod{3}$$

Ejemplo

$$\text{Hallar } 2^{-1} \pmod{7} \quad a = 2 \quad p = 7$$

$$2 \not\equiv 0 \pmod{7} \Rightarrow 2^{7-1} \equiv 1 \pmod{7} \Rightarrow 2^6 \equiv 1 \pmod{7} \Rightarrow 2 \cdot 2^5 \equiv 1 \pmod{7}$$

$$\left. \begin{array}{l} \text{MCD}(2, 7) = 1 \Rightarrow \exists \text{ una única } 2^{-1} \pmod{7} \\ 2 \cdot 2^5 \equiv 1 \pmod{7} \end{array} \right\} \Rightarrow 2^{-1} \equiv 2^5 \pmod{7}$$

o sea $2^{-1} \equiv 32 \equiv 4 \pmod{7} \Rightarrow 2^{-1} \equiv 4 \pmod{7}$

Obs:

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

② Si p no es primo y si $a \not\equiv 0 \pmod{p}$ \Rightarrow La igualdad de fermat puede ser cierta.

Ejemplo: $p = 4$ $a = 5$ $a \not\equiv 0 \pmod{4}$

$$\text{no es primo. } a^{p-1} = 5^{4-1} = 5^3 = 125 \equiv 1 \pmod{4}$$

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

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

Ejercicio: Averiguar si 4 es pseudoprimo.

$$\text{Si } a = 0 \quad 0^4 = 0 \equiv 0 \pmod{4}$$

$$\text{Si } a \equiv 0 \pmod{4} \quad a^4 = a.a.a.a \equiv 0.0.0.0 = 0 \pmod{4}$$

$$a^4 \equiv a \pmod{4} \quad \text{cuando } a=0$$

$$\text{Si } a \equiv 1 \pmod{4} \quad a^4 = a.a.a.a \equiv 1.1.1.1 = 1 \equiv a \pmod{4}$$

$$a^4 \equiv a \pmod{4} \quad \text{cuando } a=1$$

$$\text{Si } a \equiv 2 \pmod{4} \quad a^4 = a.a.a.a \equiv 2.2.2.2 = 16 \equiv 0 \pmod{4}$$

$$\text{Luego } a^4 \not\equiv a \pmod{4} \quad \text{cuando } a \equiv 2 \pmod{4}$$

Entonces 4 no es pseudoprimo.

Ejemplo:

Si p es primo y si $a \not\equiv 0 \pmod{p}$

$$a^{p-1} \equiv 1 \pmod{p} \text{ Fermat}$$

Pero puede existir otro natural $q < p-1$ / $a^q \equiv 1 \pmod{p}$

$$a = 2 \quad p = 7$$

$$q = 3 < p-1 \quad 2^3 \equiv 1 \pmod{7}$$

Teorema de Euler - Fermat.

$$\text{Si } n \in \mathbb{N} \quad \text{y} \quad \text{MCD}(a, n) = 1 \quad \Rightarrow \quad a^{\varphi(n)} \equiv 1 \pmod{n}$$

" φ " es la llamada "Función de Euler"

Demostración: Próxima clase.

Definición: Función de Euler

$$\forall n \in \mathbb{N} \text{ (fijo)} \quad \varphi(n) = * \{ j \in \mathbb{N} : 1 \leq j \leq n, \text{ MCD}(n, j) = 1 \}$$

Ejemplos: $\varphi(1) = * \{ j \in \mathbb{N} : 1 \leq j \leq 1, \text{ MCD}(j, 1) = 1 \} = * \{ 1 \} \quad \boxed{\varphi(1) = 1}$

$$\varphi(2) = * \{ j \in \mathbb{N} : 1 \leq j \leq 2, \text{ MCD}(j, 2) = 1 \} = * \{ 1 \} \quad \boxed{\varphi(2) = 1}$$

$$\varphi(3) = * \{ j \in \mathbb{N} : 1 \leq j \leq 3, \text{ MCD}(j, 3) = 1 \} = * \{ 1, 2 \} \quad \boxed{\varphi(3) = 2}$$

$$\varphi(4) = * \{ j \in \mathbb{N} : 1 \leq j \leq 4, \text{ MCD}(j, 4) = 1 \} = * \{ 1, 3 \} \quad \boxed{\varphi(4) = 2}$$

$$\boxed{\varphi(5) = 4 = p - 1} \quad (\text{proposición 1})$$

$$\varphi(6) = * \{ 1, 5 \} \quad \boxed{\varphi(6) = 2}$$

Proposición 1:

$$\text{Si } p \text{ es primo} \quad \Rightarrow \quad \varphi(p) = p - 1$$

Demostración: $\forall j \geq 1$ como p es primo $\text{si } j < p \Rightarrow \text{MCD}(j, p) = 1$

Además cuando $j = p \quad \text{MCD}(j, p) = p \neq 1$

$$\Rightarrow \{ j \in \mathbb{N} : 1 \leq j \leq p, \text{ MCD}(j, p) = 1 \} = \{ 1, 2, 3, \dots, p-1 \}$$

$$\Rightarrow \varphi(p) = * \{ 1, 2, \dots, p-1 \} = \boxed{p-1}$$

Proposición 2 :

Si p es primo, $m \in \mathbb{N}$ y $n = p^m \Rightarrow \varphi(n) = \varphi(p^m) = p^{m-1}(p-1)$

Demuestra:

$$\text{si } n = p^m$$

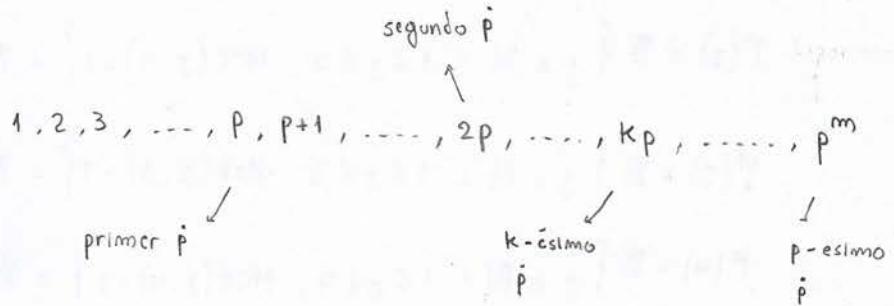
$$\varphi(n) = \varphi(p^m) = \#\left\{ j \in \mathbb{N} : 1 \leq j \leq p^m, \underbrace{\text{MCD}(j, p^m) = 1}_{\substack{\text{sabiendo que } p \text{ es primo} \\ p \nmid j}} \right\}$$

$$\Rightarrow \varphi(p^m) = p^m - \#\left\{ j \in \mathbb{N} : 1 \leq j \leq p^m / p \mid j \right\} = p^m - p^{m-1} = p^{m-1}(p-1)$$

En cada intervalo de exactamente p naturales consecutivos hay exactamente un (y uno solo) \dot{p} .

En cada intervalo de exactamente $k \cdot p$ naturales consecutivos hay exactamente k \dot{p} .

Miremos el intervalo de naturales consecutivos



Proposición 3:

$$\text{Si } p \text{ y } q \text{ son primos} \Rightarrow \varphi(p \cdot q) = (p-1)(q-1)$$

Demarcación:

$$\varphi(p \cdot q) = \#\left\{ j \in \mathbb{N} : 1 \leq j \leq pq, \underbrace{\text{MCD}(j, pq) = 1}_{p \nmid j \text{ y } q \nmid j} \right\}$$

Sean: $A = \{ j \in \mathbb{N} : 1 \leq j \leq pq : p \mid j \}$ (Conjunto de p entre 1 y pq)
 $B = \{ j \in \mathbb{N} : 1 \leq j \leq pq : q \mid j \}$ (Conjunto de q entre 1 y pq)

Calculemos $\varphi(p \cdot q)$ usando el principio de inclusión-exclusión

$$\varphi(p \cdot q) = pq - (\#A + \#B - \#(A \cap B))$$

$$\#A = q \quad (\text{hay } q \text{ múltiplos de } p \text{ entre 1 y } pq)$$

$$\#B = p \quad (\text{hay } p \text{ múltiplos de } q \text{ entre 1 y } pq)$$

$$\text{Si } j \in A \cap B \Rightarrow \begin{cases} j = p \\ j = q \end{cases} \Rightarrow j = \text{lcm}(p, q) = pq \quad \left. \begin{array}{l} \\ \\ 1 \leq j \leq pq \end{array} \right\} \Rightarrow j = pq \Rightarrow \#(A \cap B) = 1$$

$$\text{Entonces } \varphi(p \cdot q) = pq - (q + p - 1) = pq - q - p + 1 = (p-1)(q-1)$$

Definición: Una función $f: \mathbb{N} \rightarrow \mathbb{N}$ se llama "MULTIPLICATIVA" si $\forall n, m \in \mathbb{N}$ tales que $\text{MCD}(n, m) = 1$ se cumple:

$$f(m \cdot n) = f(m) \cdot f(n)$$

Teorema:

La función de Euler es "multiplicativa"

Demostración: Pendiente.Corolario: $\forall n \text{ natural}$

$$n = p_1^{m_1} \cdots p_k^{m_k}$$

 p_1, \dots, p_k primos diferentes 2 a 2.

(descomposición en factores primos)

Entonces $p_1^{m_1}, \dots, p_k^{m_k}$ son números coprimos 2 a 2.

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{m_1} \cdots p_k^{m_k}) \stackrel{\text{Teo}}{=} \varphi(p_1^{m_1}) \cdots \varphi(p_k^{m_k}) = p_1^{m_1-1}(p_1-1) \cdots p_k^{m_k-1}(p_k-1) = \\ &= \frac{p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}}{p_1 \cdot p_2 \cdots p_k} (p_1-1) \cdots (p_k-1) = \frac{n}{p_1 \cdots p_k} (p_1-1)(p_2-1) \cdots (p_k-1) = \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \end{aligned}$$

Conclusión: $\varphi(n) = n \cdot \prod_{\substack{p_i | n \\ p_i \text{ primo}}} \left(1 - \frac{1}{p_i}\right)$

Ejemplo: Hallar $\varphi(180)$

$$\varphi(180) = \varphi(2^2 \cdot 3^2 \cdot 5) = 180 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = \frac{180}{3} (2-1)(3-1)(5-1) = \boxed{48}$$

Retomamos: **Teorema:** La función de Euler es multiplicativa.

Es decir: **(H)** $\text{MCD}(m,n) = 1$ **(T)** $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

Demostración:

$$\text{Sean } C = \left\{ x \in \mathbb{N} \mid 1 \leq x \leq m \cdot n, \text{ MCD}(x, m \cdot n) = 1 \right\} \Rightarrow \#C = \varphi(m \cdot n)$$

$$A = \left\{ r \in \mathbb{N} \mid 1 \leq r \leq m, \text{ MCD}(r, m) = 1 \right\} \Rightarrow \#A = \varphi(m)$$

$$B = \left\{ s \in \mathbb{N} \mid 1 \leq s \leq n, \text{ MCD}(s, n) = 1 \right\} \Rightarrow \#B = \varphi(n)$$

El producto cartesiano $A \times B$ es, por def: $A \times B = \{(r, s) : r \in A, s \in B\} \subset \mathbb{N} \times \mathbb{N}$

$$\#(A \times B) = (\#A) \cdot (\#B)$$

Para demostrar el teorema basta probar que: $\#C = \#(A \times B)$

o sea, basta probar que existe alguna correspondencia biunívoca

$$F: A \times B \rightarrow C$$

Paso 1: Construir una función $F: A \times B \rightarrow C$, o sea que a cada (r, s) le haga corresponde un solo $x \in C$, $x = F(r, s)$.

Sea $r \in A$ fijo cualquiera, Sea $s \in B$ fijo cualquiera.

Considero este sistema de ecuaciones:

$$(S) \quad \begin{cases} x \equiv r \pmod{m} \\ x \equiv s \pmod{n} \end{cases} \quad \begin{array}{l} \xrightarrow{\text{teo chino}} \\ \xrightarrow{\text{por (H) } \text{MCD}(m, n) = 1} \end{array} \quad \begin{array}{l} \exists x \text{ solución de (S) y } x \text{ es única } (\pmod{m \cdot n}) \\ \text{O sea, } \exists \text{ único } x \in \mathbb{N}, 1 \leq x \leq m \cdot n / \text{ cumple (S). Denoto } x = F(r, s) \end{array}$$

Para terminar el 1^{er} paso falta probar que $x \in C$, o sea, falta probar que x es coprimo con $m \cdot n$.

Sea $d = \text{MCD}(m, n)$.

Por absurdo supongo $d \neq 1$ ($d > 1$ porque $d \in \mathbb{N}$) , $\exists p$ primo / $p \mid d$.

$$\left. \begin{array}{l} p \mid d \\ d \mid x \\ d \mid m, n \end{array} \right\} \Rightarrow \boxed{p \mid x}^*$$

$$\left. \begin{array}{l} p \mid m, n \\ p \text{ primo} \end{array} \right\} \xrightarrow{\text{lema Euler}} p \nmid n \circ \boxed{p \mid m}^{**}$$

Para fijar ideas supongo $p \mid m$
(Si $p \nmid n$ la prueba es similar)

$$(S) \Rightarrow x \equiv r \pmod{m}$$

$$r - x = rm = mn \cdot h \quad \text{para algún } h \in \mathbb{Z}.$$

$$\left. \begin{array}{l} r = x + mh \\ p \mid x \text{ y } p \mid m \end{array} \right\} \Rightarrow \boxed{p \mid r}$$

$$\left. \begin{array}{l} p \mid r \\ p \mid m \\ p \text{ primo} \end{array} \right\} \Rightarrow \text{MCD}(r, m) \neq 1 \Rightarrow r \notin A$$

Absurdo.

$$\boxed{\text{LQDD } F(r, s) = x \in C}$$

Paso 2: Probar que la F construida en el paso 1 es inyectiva. O sea:

$$(H) (r, s) \neq (r', s') \in A \times B$$

a sea $r \neq r'$ ó $s \neq s'$
en A en B

$$(T) x \neq x' \in C \quad \text{donde } x = F(r, s)$$

$$x' = F(r', s')$$

Supongo $r \neq r'$.

$$\left. \begin{array}{l} r \neq r' \\ r, r' \in A \end{array} \right\} \Rightarrow \boxed{r \not\equiv r' \pmod{m}}$$

$$(S) \left\{ \begin{array}{l} \boxed{x \equiv r \pmod{m}} \\ x \equiv s \pmod{n} \\ F(r, s) = x \end{array} \right.$$

$$\boxed{x \neq x'}$$

LQDD inyectividad de F .

$$(S') \left\{ \begin{array}{l} \boxed{x' \equiv r' \pmod{m}} \\ x' \equiv s' \pmod{n} \\ x' = F(r', s') \end{array} \right.$$

Paso 3 :

Probar que F es sobreyectiva, o sea:

$$\text{(H)} \quad x \in C \quad \text{(T)} \quad \exists r \in A, \exists s \in B \text{ tales que } x = F(r, s)$$

Construyo r así:

$$\begin{cases} r = m & \text{si } x = m \\ r = \text{resto de dividir } x \text{ entre } m & \text{si } x \neq m \end{cases}$$

$$\Rightarrow 0 \leq r \leq m, \quad \boxed{x \equiv r \pmod{m}} \quad \Rightarrow x = r + hm \text{ para algún } h \in \mathbb{Z}$$

Sea $d = \text{MCD}(r, m)$. Quiero probar que $d=1$ para deducir que $r \in A$.

$$\left. \begin{array}{l} d|r \\ d|m \end{array} \right\} \Rightarrow d|r+hm \Rightarrow d|x \quad \left. \begin{array}{l} d|x \\ d|m \Rightarrow d|m \cdot n \end{array} \right\} \Rightarrow \boxed{d=1} \quad \boxed{\text{LQOD, } r \in A}$$

$$\text{(H)} \quad x \in C$$

Construyo s así:

$$\begin{cases} s = n & \text{si } x = n \\ s = \text{el resto de dividir } x \text{ entre } n & \text{si } x \neq n \end{cases}$$

$$\Rightarrow 0 \leq s \leq n, \quad \boxed{x \equiv s \pmod{n}} \quad \Rightarrow x = s + kn \text{ para algún } k \in \mathbb{Z}$$

Idem que antes prueba que $\boxed{s \in B}$

$$\boxed{\text{i) y ii)}} \quad (S) \quad \begin{cases} x \equiv r \pmod{m} & r \in A \\ x \equiv s \pmod{n} & s \in B \end{cases}$$

Por definición de la función $F : x = F(r, s)$ LQOD la sobreyectividad de F

Quedaba pendiente: Recordemos.

Función de Euler

$$\varphi(n) = \#\{x \in \mathbb{N} : 1 \leq x \leq n, \text{ MCD}(x, n) = 1\}$$

Proposición 1

$$a \equiv b \pmod{n} \implies \text{MCD}(a, n) = 1 \iff \text{MCD}(b, n) = 1$$

Demostración:

(\Rightarrow) Sea $d = \text{MCD}(b, n)$. Hay que probar que $d = 1$.

Por (H) $a \equiv b \pmod{n} \iff a = b + kn$ para algún $k \in \mathbb{Z}$

$$\left. \begin{array}{l} d | b \\ d | n \end{array} \right\} \Rightarrow d | b + kn = a \Rightarrow \left. \begin{array}{l} d | a \\ d | n \end{array} \right\} \Rightarrow \boxed{d = 1}$$

Hip $\text{MCD}(a, n) = 1$
 \Rightarrow

(\Leftarrow) Análogo.

Proposición 2

$$\left. \begin{array}{l} \text{MCD}(a, n) = 1 \\ \text{MCD}(b, n) = 1 \end{array} \right\} \iff \text{MCD}(a \cdot b, n) = 1$$

Demostración:

(\Rightarrow) Sea $d = \text{MCD}(a \cdot b, n)$. Hay que probar que $d = 1$.

Por absurdo si $d \neq 1$, $\exists p$ primo $| p | d$.



$$\left. \begin{array}{l} d|a, b \\ d|n \\ p|d \end{array} \right\} \left. \begin{array}{l} p|n \\ p|a, b \\ p \text{ primo} \end{array} \right\} \xrightarrow{\text{Lema Euclides}} p|a \circ p|b$$

Caso 1 : ($p|a$)

$$\left. \begin{array}{l} p|a \\ p|n \\ p \text{ primo} \end{array} \right\} \Rightarrow \text{MCD}(a, n) \neq 1 \quad \text{Absurdo, contradice hipótesis.}$$

Caso 2 : ($p|b$)

$$\left. \begin{array}{l} p|b \\ p|n \\ p \text{ primo} \end{array} \right\} \Rightarrow \text{MCD}(b, n) \neq 1 \quad \text{Absurdo, contradice hipótesis.}$$

(\Leftarrow) : Ejercicio.

Teorema de Euler - Fermat

$$\boxed{a \in \mathbb{Z} \quad n \in \mathbb{N} \quad \text{MCD}(a, n) = 1 \quad \Rightarrow \quad a^{\varphi(n)} \equiv 1 \pmod{n}}$$

Demostración :

Sea $A = \{x \in \mathbb{N}, 1 \leq x \leq n, \text{MCD}(x, n) = 1\} = \{x_1, \dots, x_k\} \rightarrow x_i \neq x_j \text{ si } i \neq j \quad \# A = k$

por definición de la función de Euler $\boxed{\# A = \varphi(n)}$

Sea $B = \{y \in \mathbb{N} : \exists x \in A \text{ que cumple } ax = y\} = \{ax_1, ax_2, \dots, ax_k\}$

$\boxed{\# B = \# A = \varphi(n) = k}$ porque $ax_i \neq ax_j \text{ si } x_i \neq x_j$

Afirmación 1

Los diferentes elementos de B son no congruentes mod n dos a dos entre sí.

O sea: si $x_i \not\equiv x_j \pmod{n} \Rightarrow ax_i \not\equiv ax_j \pmod{n}$

Demostración:

$$\text{Si fuera } ax_i \equiv ax_j \pmod{n} \quad \left. \begin{array}{l} \\ \text{prop cancelativa} \end{array} \right\} \Rightarrow x_i \equiv x_j \pmod{n}$$

$\textcircled{H} \quad \text{MCD}(a, n) = 1$

$$x_i, x_j \in A \Rightarrow 1 \leq x_i \leq n$$

$1 \leq x_j \leq n$

$$\xrightarrow{\quad} \boxed{x_i = x_j}$$

LQDD.

Afirmación 2

Los elementos de B son todos coprimos con n.

O sea: si $x_i \in A \Rightarrow \text{MCD}(ax_i, n) = 1$

Demostración:

Sea $d = \text{MCD}(ax_i, n)$. Hay que probar que $d = 1$.

Por absurdo, si $d \neq 1 \Rightarrow \exists p \text{ primo} / p \mid d$.

$$\left. \begin{array}{l} d \mid n \\ d \mid ax_i \\ p \mid d \end{array} \right\} \Rightarrow \left. \begin{array}{l} p \mid n \\ p \mid ax_i \\ p \text{ primo} \end{array} \right\} \stackrel{\text{lema Euclides}}{=} p \mid a \circ p \mid x_i$$

Caso 1: ($p \mid a$)

$$\left. \begin{array}{l} p \mid a \\ p \mid n \\ p \text{ primo} \end{array} \right\} \Rightarrow \text{MCD}(a, n) \neq 1 \quad \text{Abs, contradice } \textcircled{H}$$

Caso 2: ($p \mid x_i$)

$$\left. \begin{array}{l} p \mid x_i \\ p \mid n \\ p \text{ primo} \end{array} \right\} \Rightarrow \text{MCD}(x_i, n) \neq 1 \quad \text{Abs, contradice } x_i \in A.$$

Para cada $y \in B$ construyo el único natural $r = F(y) / \begin{cases} y \equiv r \pmod{n} \\ 1 \leq r \leq n \end{cases}$

B Sz Def de la Función $F: B \rightarrow \mathbb{N}$

Afirmación 3

$$r = F(y) \in A \quad \forall y \in B$$

Demostración: Por construcción de la función $F : \begin{cases} r \equiv y \pmod{n} \\ 1 \leq r \leq n \end{cases}$

Por la afirmación ② $y \in B \Rightarrow \text{MCD}(y, n) = 1$

Por proposición ① : $\text{MCD}(r, n) = 1$.

$$\left. \begin{array}{l} 1 \leq r \leq n \\ \text{MCD}(r, n) = 1 \end{array} \right\} \Rightarrow r \in A \quad \text{LQQD.}$$

Afirmación 4

F es inyectiva, es decir $y \neq y'$ en $B \Rightarrow r \neq r'$ (en A) donde $\begin{cases} r = F(y) \\ r' = F(y') \end{cases}$

Demostración:

Por absurdo si $r = r'$

$$\left. \begin{array}{l} r = F(y) \Rightarrow y \equiv r \pmod{n} \\ r' = F(y') \Rightarrow y' \equiv r' \pmod{n} \end{array} \right\} \Rightarrow y \equiv y' \pmod{n}$$

$$\left. \begin{array}{l} y = y' \pmod{n} \\ y, y' \in B \end{array} \right\} \stackrel{\text{Afirmación 1}}{=} y = y' \quad \text{Absurdo (Contradice Hip } y \neq y' \text{ en } B)$$

LQQD

$$\left. \begin{array}{l} F: B \rightarrow A \\ \text{inyectiva} \end{array} \right\} \Rightarrow \boxed{\# F(B) = \# B} \quad *$$

conjunto imagen

Por afirmación ③ : $F(B) \subset A$ $\boxed{\# F(B) \leq \# A}$

Por afirmación ⑥ : $\boxed{\# B = \# A} \quad **$

$$\left. \begin{array}{l} \text{De } * \gamma ** \Rightarrow \# F(B) = \# A \\ F(B) \subset A \end{array} \right\} \Rightarrow F(B) = A \Rightarrow F \text{ es sobreyectiva en } A$$



F es biunívoca de B a A .

Considero :

$$\bullet \boxed{\prod_{y_i \in B} y_i} = y_1 y_2 \dots y_k = (ax_1) \dots (ax_n) = a^k \prod_{x_i \in A} x_i = \boxed{a^{\varphi(n)} \prod_{x_i \in A} x_i}$$

$$\bullet \boxed{\prod_{y_i \in B} y_i} = y_1 y_2 \dots y_k \equiv F(y_1) \cdot F(y_2) \dots F(y_k) \pmod{n} = \boxed{\prod_{x_i \in A} x_i \pmod{n}}$$

Conclusión :

$$\boxed{a^{\varphi(n)} \prod_{x_i \in A} x_i \equiv \prod_{x_i \in A} x_i \pmod{n}}$$

Por proposición 2, x_i y n son coprimos y por la cancelativa tengo

$$\boxed{a^{\varphi(n)} \equiv 1 \pmod{n}}$$

LQD teorema de Euler - Fermat.

Aplicaciones :

① $10^{60} \pmod{21}$

$$\text{MCD}(a, n) = \text{MCD}(10, 21) = 1$$

$$10^{\varphi(21)} \equiv 1 \pmod{21}$$

$$\begin{aligned}\varphi(21) &= \varphi(3 \cdot 7) = \varphi(3) \cdot \varphi(7) = \\ &= (3-1)(7-1) = 12\end{aligned}$$

$$10^{12} \equiv 1 \pmod{21}$$

$$\Rightarrow 10^{60} = 10^{12 \cdot 5} = (10^{12})^5 \equiv 1 \pmod{21}$$

Respuesta : $10^{60} \equiv 1 \pmod{21}$

② $10^{62} \pmod{21}$

$$10^{12} \equiv 1 \pmod{21}$$

$$62 = 5 \cdot 12 + 2$$

$$\begin{array}{r} 100 \longdiv{121} \\ 16 \quad 4 \\ \hline 8 \end{array}$$

$$10^{62} = (10^{12})^5 \cdot 10^2 \equiv 1^5 \cdot 10^2 \pmod{21} \Rightarrow 10^{62} \equiv 100 \pmod{21}$$

$$100 \equiv 16 \pmod{21}$$

Respuesta : $10^{62} \equiv 16 \pmod{21}$

③ $10^{59} \pmod{21}$

$$10^{12} \equiv 1 \pmod{21}$$

$$59 = 5 \cdot 12 - 1 \Rightarrow 10^{59} = (10^{12})^5 \cdot 10^{-1} \pmod{21} \equiv 1^5 \cdot 10^{-1} \pmod{21}$$

Hallar el inverso 10^{-1} de $10 \pmod{21}$ y ese inverso será $10^{59} \pmod{21}$

GRUPOS

Definición : $\langle G, * \rangle$ es un grupo si :

- G es un conjunto no vacío, $G \neq \emptyset$.
- $*$ es una operación definida para toda pareja ordenada (a, b) de elementos de G tales que cumple :
 - "Cierre" : $\forall (a, b) \in G \times G$ el resultado es único $a * b \in G$
(o sea $* : G \times G \rightarrow G$)
 - "Asociativa" : $\forall a, b, c \in G$
$$(a * b) * c = a * (b * c)$$
 - "Neutral o identidad" : \exists algún elemento $e \in G$ tal que $e * a = a * e = a \quad \forall a \in G$
 - "Opuesto o inverso" : $\forall a \in G$, \exists algún elemento $a' \in G$ tal que $a * a' = a' * a = e$

Definición : Un grupo $\langle G, * \rangle$ se llama "ABELIANO" si además de las condiciones anteriores vale la conmutativa : $a * b = b * a \quad \forall a, b \in G$

Notación:

- Cuando el grupo $\langle G, * \rangle$ es abstracto se usa la notación a' para indicar el opuesto o inverso de a en G .
- Cuando estoy con un ejemplo (no abstracto) con operación "Suma" por ejemplo : $\langle \mathbb{Z}, + \rangle$ o $\langle \mathbb{R}, + \rangle$
uso $-a$ para denotar el opuesto de a . (Inverso en la estructura de grupo $\langle \mathbb{Z}, + \rangle$)
- Se usa $a \cdot b$ ó ab para denotar $a * b$ (¡OJO! No se refiere a una operación de "multiplicar" necesariamente)
- Cuando estoy con un ejemplo (no abstracto) con operación producto, por ejemplo $\langle \mathbb{R}^+, \cdot \rangle$ uso la notación abstracta $a \cdot b$, a' inverso de a .

Contraejemplos: No son grupos $\langle \mathbb{R}, - \rangle$ $\langle \mathbb{R}, \cdot \rangle$ $\langle \mathbb{N}, + \rangle$

Ejemplos de grupos

① $M_{n \times n}(\mathbb{R}) = \{ \text{Matrices } n \times n \text{ de coeficientes reales} \}$ n natural fijo.

$\langle M_{n \times n}(\mathbb{R}), + \rangle$ es un grupo.

② Grupo lineal en \mathbb{R}^n , n natural fijo.

$GL_n = \{ \text{Matrices } n \times n \text{ con coeficientes reales invertibles, es decir con determinante } \neq 0 \}$

$\langle GL_n, \cdot \rangle$ es un grupo

prod. Matrices.

③ $\mathbb{Z}_n = \{ \text{Clases de congruencia de enteros m\'odulo } n \}$, n natural fijo.

$\langle \mathbb{Z}_n, + \rangle$ es un grupo

Ejemplo: $\mathbb{Z}_3 = \{ 0 \pmod 3, 1 \pmod 3, 2 \pmod 3 \}$

Obs: el opuesto de a en \mathbb{Z}_n es $-a \pmod n$

Tabla de Cayley

76

| $a \backslash b$ | 0 | 1 | 2 | 3 | 4 | 5 |
|------------------|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

En los casilleros se coloca el resultado de operar $a * b$

Teorema: \forall grupo $\langle G, * \rangle$ (Abstracto)

- (A) El neutro es único.
- (B) Para todo $a \in G$ su "opuesto o inverso es único"
- (C) Cancelativa de la estructura de grupo : $a * b = a * c \iff b = c$
 $b * a = c * a \iff b = c$

(D) Existencia y unicidad de solución de ecuaciones lineales en G

- $\forall a, b \in G$ Fijos, \exists y es única la solución x de la ecuación $a * x = b$
- $\forall a, b \in G$ Fijos, \exists y es única la solución y de la ecuación $y * a = b$

Demostración:

- (A) Sean e_1 y e_2 neutros, es decir:
- (i) $a * e_1 = e_1 * a = a \quad \forall a \in G$
 - (ii) $a * e_2 = e_2 * a = a \quad \forall a \in G$

En (i) uso en particular $a = e_2$ y obtengo $e_2 * e_1 = e_1 * e_2 = e_2$

En (ii) uso en particular $a = e_1$ y obtengo $e_1 * e_2 = e_2 * e_1 = e_1$

Por transitiva de la igualdad $e_1 = e_2$

- (C) (\Rightarrow) (H) $a * b = a * c \quad (\text{I}) \quad b = c$

Demostración:

$$\begin{aligned} \text{Por (H)} \quad a * b &= b * a \implies \bar{a}' * (a * b) = \bar{a}' * (a * c) \\ &\stackrel{\text{asoc}}{\implies} (\bar{a}' * a) * b = (\bar{a}' * a) * c \implies e * b = e * c \implies b = c \end{aligned}$$

- (\Leftarrow) (H) $b = c \quad (\text{I}) \quad a * b = a * c$

Demostración: Por unicidad del resultado de la operación

$$\mathbb{Z}_3 = \{ \text{congruencias módulo } 3 \}$$

$$\langle \mathbb{Z}_3, + \rangle$$

| a\b | 0 | 1 | 2 |
|-----|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

En la tabla Cayley, como consecuencia de la propiedad cancelativa:

En cada fila, no hay elementos repetidos, tampoco en las columnas.

Definición: El orden de un grupo $(G, *)$ es la cantidad de elementos que hay en G .

Notación: $|G| = \# G$

Ejemplos:

① $(\mathbb{Z}_n, +)$

$$\mathbb{Z}_n = \{0 \pmod n, \dots, (n-1) \pmod n\}$$

$$|\mathbb{Z}_n| = n$$

② (U_n, \cdot) producto de clases de equiv $\pmod n$

$$U_n = \{\text{Clases de congruencia de } \mathbb{Z} \pmod n \text{ tales que } \exists \text{ inverso } \pmod n\} = \{a \in \mathbb{Z} : 1 \leq a \leq n, \text{MCD}(a, n) = 1\}$$

$$(a \pmod n \text{ es invertible} \iff \text{MCD}(a, n) = 1)$$

El neutro es $1 \pmod n$

$$|U_n| = \varphi(n) \quad \text{Por definición de la función de Euler.}$$

Permutaciones de n elementos

$$A_n = \{1, 2, 3, \dots, n\}$$

Definición: Una permutación de n elementos es una transformación biunívoca $f: A_n \rightarrow A_n$

S_n denota el conjunto de todas las permutaciones de n elementos

$$\# S_n = n!$$

notación: $f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$

Ejemplo:

$$A_3 = \{1, 2, 3\}$$

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \text{Permutación "identidad"}$$

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad c = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

(S_n, \circ) → composición de funciones ($g \circ f$ significa aplicar primero f y luego al resultado aplicarle g)

$$a^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = b \quad b \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad c \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = d$$

$$a \circ a = b$$

$$a \circ a \circ a = e$$

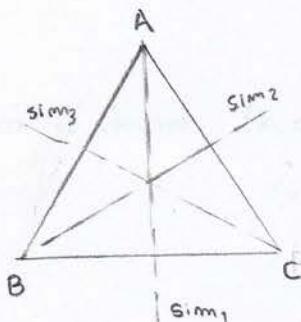
$$c \circ a = d$$

$$a \circ c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f \quad \left. \right\} \Rightarrow \text{no es abeliano.}$$

Obs: Solo S_2 es abeliano.

Grupo diedral

Ejemplo: D_3 : { "movimientos" del plano que transforman al triángulo en si mismo }



$$\text{Sim}_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \quad \text{Sim}_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$

$$\text{Sim}_3 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

$$\text{id} = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} \quad \text{rot}_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} \quad \text{rot}_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

$$|D_3| = 3! = 6$$

(D_3, \circ) composición de movimientos del plano

$$\text{id} = e^*$$

$$\text{Sim}_3 = f^*$$

$$\text{rot}_1 = a^*$$

$$\text{Sim}_2 = d^*$$

$$\text{rot}_2 = b^*$$

$$\text{Sim}_1 = c^*$$

$$\text{rot}_1 \circ \text{rot}_1 = \text{rot}_2$$

$$\text{rot}_1 \circ \text{rot}_1 \circ \text{rot}_1 = \text{id}$$

$$\text{Sim}_1 \circ \text{rot}_1 = \text{Sim}_2$$

$$\text{rot}_1 \circ \text{sim}_1 = \text{sim}_3$$

Conociendo sim_1 y rot_1 , generé todos los otros elementos.

Subgrupo:

Sea $(G, *)$ un grupo, $(S, *)$ es subgrupo de $(G, *)$ si :

$$\textcircled{1} \quad S \subset G, \quad S \neq \emptyset$$

\textcircled{2} La operación $*$ de $(S, *)$ es "La misma" que la de $(G, *)$ después de restringida a los elementos de S .

\textcircled{3} $(S, *)$ es en sí mismo un grupo.

TEOREMA:

(H) i) Si $(G, *)$ es un grupo

ii) $S \neq \emptyset$, S es un subconjunto de G

iii) Si $(S, *)$ cumple propiedades de ① cierre en S ($\forall a, b \in S \rightarrow a * b \in S$)

② opuesto/inverso en S ($\forall a \in S, a^{-1} \in S$)

(T) Entonces $(S, *)$ es un subgrupo de G .

TEOREMA 2:

(H) i) $(G, *)$ es un grupo. $|G|$ es finito.

ii) $S \neq \emptyset$, S es un subconjunto de G .

iii) $(S, *)$ cumple propiedades de cierre en S

(T) Entonces $(S, *)$ es subgrupo de G y además...

Ejemplo

Sea $(\mathbb{Z}, +)$ un grupo. $(\mathbb{Z}^{\text{pares}}, +)$ subgrupo de \mathbb{Z} .

$(\mathbb{Z}^{\text{s}}, +)$ subgrupo de \mathbb{Z}

La unión de 2 subgrupos no tiene que dar otro subgrupo

$$\left. \begin{array}{l} 4 \text{ es par} \\ 5 \text{ es } \frac{5}{2} \end{array} \right\} \Rightarrow 4+5=9 \quad 9 \notin \text{unión}$$

Definición de Potencia

Sea $(G, *)$ un grupo, y sea $a \in G$, definimos:

$$a^1 = a$$

$$a^2 = a * a$$

$$a^n = \underbrace{a * \dots * a}_{n \text{ veces}}$$

$$a^0 = e_G \text{ (neutro del grupo)}$$

def

$$a^{-1} \stackrel{\text{def}}{=} \text{inverso de } a \text{ en } (G, *)$$

$$a^{-n} \stackrel{\text{def}}{=} (\bar{a}^1) * \dots * (\bar{a}^1)$$

n veces

$$a^{m+n} = a^m * a^n$$

$$\forall n, m \in \mathbb{Z}$$

$\forall a \in G$

Si el grupo es aditivo, lo denotamos:

$$a^1 = 1 \cdot a = a$$

$$a^2 = 2 \cdot a = a + a$$

$$a^n = n \cdot a = \underbrace{a + \dots + a}_{n \text{ veces}}$$

$$a^0 = 0 \cdot a = e_G$$

$$a^{-1} = -1 \cdot a = -a$$

$$a^{-n} = -n \cdot a = (-a) + \dots + (-a)$$

n veces

$$a^{m+n} = (m+n)a = (ma) + (na)$$

suma
enteros

operación del grupo

Definición: Orden de un elemento $a \in G$ un grupo G .

Caso 1: Si $\exists n \in \mathbb{N} / a^n = e_G$

Se llama orden de a , $\theta(a)$, al mínimo n natural que lo cumple.

Caso 2: Si $\nexists n \in \mathbb{N} / a^n = e_G$

Se dice que el orden de a es infinito.

Definición: Subgrupo generado por un elemento $a \in G$.

Dado $(G, *)$ un grupo, $a \in G$.

Considero el conjunto $\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$ $\langle a \rangle$ se llama subgrupo generado por a .

(Hay que demostrar que es un grupo)

Propiedades:

① $\langle a \rangle$ es un subgrupo de G que contiene a a .

Demostración:

Por la definición de $\langle a \rangle$, $\langle a \rangle$ es el conjunto de todas las potencias de a .
Entonces $a^k \in \langle a \rangle$, $a \in \langle a \rangle$.

Ahora tenemos que ver que $\langle a \rangle$ es un subgrupo de G . Para eso debemos verificar las propiedades de cierre y de existencia del inverso.

$$\begin{aligned} 0) \text{"cierre"} \quad & \text{sea } g \in \langle a \rangle \Rightarrow g = a^n \\ & \text{Sea } g' \in \langle a \rangle \Rightarrow g' = a^m \end{aligned} \quad \left. \right\} \Rightarrow g * g' = a^{n+m} \in \langle a \rangle$$

$$3) \text{"inverso"} \quad \text{sea } g \in \langle a \rangle \Rightarrow g = a^n$$

$$g^{-1} = (a^n)^{-1} = (\bar{a}^1)^n = \bar{a}^{-n} \in \langle a \rangle$$

↓
probar
práctica

$\Rightarrow \langle a \rangle$ es un subgrupo de G

② $\langle a \rangle$ es el menor de los subgrupos de G que contiene a a .
(O sea, si $H \subset G / a \in H$, entonces $H \supset \langle a \rangle$)

Demostración:

Demostración:

Sea H un subgrupo de G / $a \in H$

$$\left. \begin{array}{l} H \text{ subgrupo} \\ a \in H \end{array} \right\} \Rightarrow \begin{array}{l} \text{vale la propiedad} \\ \text{de cierre en } H \end{array} \Rightarrow \begin{array}{l} a * a \in H \\ a^2 \in H \\ \vdots \\ a^n \in H \quad \forall n \in \mathbb{N} \end{array} \quad (\text{Verificar por IC})$$

• Luego $a^0 = e$, $e \in H$ pues H es subgrupo de G .

• $a^{-n} / n \in \mathbb{N}$, $a^{-n} \in H$ pues a^{-1} es el inverso de $a \in H$
 \Rightarrow con H subgrupo, $a^{-1} \in H$.

$$\Rightarrow a^n \in H \quad \forall n \in \mathbb{Z} \Rightarrow \langle a \rangle \subset H.$$

Teorema:

④ $\theta(a) < \infty$ ($\theta(a)$ es finito)

$$\theta(a) = m_0$$

⑤ El conjunto $H = \{e, a, a^2, \dots, a^{m_0-1}\}$ es el subgrupo generado por a , es decir $H = \langle a \rangle$
(Se cumple que $|\langle a \rangle| = \theta(a)$)

Demostración:

Sea $H = \{e, a, a^2, \dots, a^{m_0-1}\}$ probaremos que $H \subset A$ y $A \subset H$.

(1) $H \subset \langle a \rangle$ es trivial por definición de $\langle a \rangle$

(2) $\langle a \rangle \subset H$

Si $g \in \langle a \rangle$, hay que probar que $g \in H$. $g = a^n$, para algún $n \in \mathbb{Z}$: (hago la división entera)

$$\Rightarrow n = q \cdot m_0 + r, \quad 0 \leq r \leq m_0 - 1 \quad (*)$$

$$g = a^n = a^{q \cdot m_0 + r} = a^{q \cdot m_0} * a^r = (a^{m_0})^q * a^r = e^q * a^r = a^r \in H$$

pues cumple (*)

$$\Rightarrow g \in H \Rightarrow \langle a \rangle \subset H \Rightarrow \langle a \rangle = H$$

Definición:

Un grupo $(G, *)$ se llama cíclico si se cumple:

- i) $|G|$ es finito
- ii) $G = \langle a \rangle$ para algún $a \in G$

Ejemplos:

① ¿Cuál es el subgrupo de $(\mathbb{Z}, +)$ generado por 5?

$$\text{es } \{ \dots, -10, -5, 0, 5, 10, \dots \} \text{ (múltiplos de 5)}$$

② Consideremos $(\mathbb{Z}_6, +)$

$$\mathbb{Z}_6 = \{ 0 \pmod{6}, 1 \pmod{6}, 2 \pmod{6}, 3 \pmod{6}, 4 \pmod{6}, 5 \pmod{6} \}$$

es un grupo cíclico.

$$\varrho(2) \text{ es } 3 \text{ pues } 2^3 = 2+2+2 = 0 \pmod{6}$$

$$\varrho(3) \text{ es } 2 \text{ pues } 3^2 = 3+3 = 0 \pmod{6}$$

$$\varrho(1) \text{ es } 6 \text{ pues } 1^6 = 1+1+1+1+1+1 = 0 \pmod{6}$$

Observar que $\langle 1 \rangle = (\mathbb{Z}_6, +)$. Esto prueba que es cíclico.

En general, con $n \geq 2$ natural:

$(\mathbb{Z}_n, +)$ es cíclico pues:

$$\{ 0 \pmod{n}, 1 \pmod{n}, \dots, n-1 \pmod{n} \} = \langle 1 \pmod{n} \rangle_{(\mathbb{Z}_n, +)}$$

Ejemplos: Grupos no cíclicos y cíclicos.

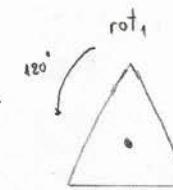
$$\textcircled{1} \quad (D_3, \circ)$$

$$D_3 = \{e, \text{rot}_1, \text{rot}_2, \text{sim}_1, \text{sim}_2, \text{sim}_3\}$$

$$\text{rot}_1' = \text{rot}_1$$

$$(\text{rot}_1)^2 = \text{rot}_1 \circ \text{rot}_1 = \text{rot}_2$$

$$(\text{rot}_1)^3 = \text{rot}_1 \circ \text{rot}_1 \circ \text{rot}_1 = e \Rightarrow \Theta(\text{rot}_1) = 3$$

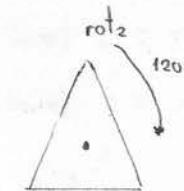


recordar def potencia

$$\text{rot}_2' = \text{rot}_2$$

$$(\text{rot}_2)^2 = \text{rot}_2 \circ \text{rot}_2 = \text{rot}_1$$

$$(\text{rot}_2)^3 = \text{rot}_2 \circ \text{rot}_2 \circ \text{rot}_2 = e \Rightarrow \Theta(\text{rot}_2) = 3$$



$$\text{Sim}_1' = \text{Sim}_1$$

$$(\text{Sim}_1)^2 = \text{Sim}_1 \circ \text{Sim}_1 = e \Rightarrow \Theta(\text{sim}_1) = 2$$

$$\text{Sim}_2' = \text{Sim}_2$$

$$(\text{Sim}_2)^2 = \text{Sim}_2 \circ \text{Sim}_2 = e \Rightarrow \Theta(\text{sim}_2) = 2$$

$$\text{Sim}_3' = \text{Sim}_3$$

$$(\text{Sim}_3)^2 = \text{Sim}_3 \circ \text{Sim}_3 = e \Rightarrow \Theta(\text{sim}_3) = 2$$

Concluimos:

$$|D_3|$$

$$\Theta(a) \neq 6 \quad \forall a \in D_3 \Rightarrow (D_3, \circ) \text{ no puede ser cíclico.}$$

(2) $(U(5), \cdot)$

$$U(5) = \{ 1 \pmod 5, 2 \pmod 5, 3 \pmod 5, 4 \pmod 5 \}$$

$$2^1 \equiv 2 \pmod 5$$

$$2^2 \equiv 4 \pmod 5$$

$$2^3 \equiv 8 \equiv 3 \pmod 5$$

$$2^4 \equiv 16 \equiv 1 \pmod 5$$

$\downarrow e_{U(5)}$

$$\Rightarrow \begin{array}{|c|} \hline \varnothing(2) = 4 = |U(5)| \\ \hline \langle 2 \rangle = U(5) \end{array}$$

 $U(5)$ es cíclico y2 es generador de $U(5)$

$$3^1 \equiv 3 \pmod 5$$

$$3^2 \equiv 9 \equiv 4 \pmod 5$$

$$3^3 \equiv 27 \equiv 2 \pmod 5$$

$$3^4 \equiv 81 \equiv 1 \pmod 5$$

$\downarrow e_{U(5)}$

$$\Rightarrow \begin{array}{|c|} \hline \varnothing(3) = 4 = |U(5)| \\ \hline \langle 3 \rangle = U(5) \end{array}$$

3 es generador de $U(5)$

$$4^1 \equiv 4 \pmod 5$$

$$4^2 \equiv 16 \equiv 1 \pmod 5$$

$\downarrow e_{U(5)}$

$$\Rightarrow \begin{array}{|c|} \hline \varnothing(4) = 2 \end{array}$$

4 no es generador de $U(5)$ Teorema: (Práctico 6, Ej 8)Si $(G, *)$ es un grupo, $a \in G$ cualquiera.Si $\exists m$ natural / $a^m = e_G \iff \varnothing(a)$ es finito y $\varnothing(a) \mid m$ (Recordar: $\varnothing(a) = n_0 = \text{mínimo natural} / a^{n_0} = e$)

Corolario 1 :

Si $(G, *)$ es un grupo, $a \in G$ cualquiera.

Si \exists 2 naturales $i < j$ tales que $a^i = a^j \Rightarrow \Theta(a)$ es finito y $\Theta(a) \mid j-i$

Demostración:

Considero $(a^{-1})^i \stackrel{\text{def pot}}{=} \underbrace{a^{-1} * a^{-1} * \dots * a^{-1}}_{i \text{ veces}}$ $(a^{-1})^i$ lo denotamos a^i por convención.

por (H) $a^i = a^j$

$$e_G = a^{-i} * a^i = a^{-i} * a^j = a^{j-i} \Rightarrow e_G = a^{j-i}$$

Llamando $m = j-i$ estoy en las hipótesis del teorema anterior

Entonces, $\Theta(a)$ es finito y $\Theta(a) \mid m \Rightarrow \Theta(a) \mid j-i$

Corolario 2 :

Si $(G, *)$ es un grupo, $a \in G$ cualquiera.

Existen 2 naturales $i < j$ tales que $a^i = a^j \iff i \equiv j \pmod{\Theta(a)}$

Demostración: Ejercicio. (Usar Col.)Coclases en el grupo

Dado un grupo $(G, *)$, dado un subgrupo de G , S .

fijo $a \in G$.

Se llama "Coclase" de a con respecto al subgrupo S al conjunto:

$$\text{" } a * S \text{ " } \stackrel{\text{def}}{=} \left\{ g \in G \mid g = a * s \text{ para algún } s \in S \right\}$$

notación

Obs: $a \in (a * S)$ pues $e \in S$ y $a = a * e$

Ejemplo:

$$\textcircled{1} \quad \text{Si } S \text{ es finito, } S = \{ \lambda_1, \lambda_2, \dots, \lambda_k \} \quad |S| = k$$

$$a * S = \{ a * \lambda_1, a * \lambda_2, \dots, a * \lambda_k \}$$

* $(a * S) = |S|$ porque todos los elementos de $a * S$ son $\neq 2a^2$ pues si.

$$a * \lambda_1 = a * \lambda_2 \Rightarrow \lambda_1 = \lambda_2$$

Propiedad: Si S es finito, toda coclase tiene igual cantidad de elementos que S

\textcircled{2} Sea $(\mathbb{Z}, +)$ un grupo

$$|\mathbb{Z}| = \infty$$

Sea $(\mathbb{Z}^8, +)$ un subgrupo

$$|\mathbb{Z}^8| = \infty$$

$$a = 3 \in \mathbb{Z}$$

$$a + \mathbb{Z}^8 = \{ n \in \mathbb{Z} \mid n = 3 \pmod 8 \}$$

$$* a + \mathbb{Z}^8 = \infty$$

Pero solo hay 8 coclases respecto a \mathbb{Z}^8 , diferentes.

Teorema:

(H) $(G, *)$ grupo cualquiera.
 S subgrupo de G .

(T) Sean $a * S$ y $b * S$ dos coclases cualesquiera respecto de S , se cumple:

- O bien son disjuntas, o bien coinciden.

Demostración:

Si $\exists g \in (a * S) \cap (b * S)$, hay que probar que $\underbrace{a * S}_{\text{conjunto.}} = \underbrace{b * S}_{\text{conjunto.}}$

$$\begin{aligned} g \in (a * S) &\Rightarrow g = a * s_1 \quad \text{para cierto } s_1 \in S \\ g \in (b * S) &\Rightarrow g = b * s_2 \quad \text{para cierto } s_2 \in S \end{aligned} \quad \left. \right\} \Rightarrow a * s_1 = b * s_2$$

$$\Rightarrow \begin{cases} a = b * s_2 * s_1^{-1} \\ a * s_1 * s_2^{-1} = b \end{cases} \quad \bigcup_{s' \in S}$$

Sea $g' \in a * S$ cualquiera $\Rightarrow g' = a * s' = b * s_2 * s_1^{-1} * s' = \underbrace{b * s' \in S}_{\in S} \Rightarrow g' \in b * S$

Todo elemento g' de la coclase $a * S$ pertenece también a $b * S$

$$a * S \subset b * S$$

La otra inclusión se demuestra cambiando los roles de a y b .

Relación:

Sean $a, b \in G$,

Decimos que $a \sim b$ cuando $a * s = b * s$

Esta es una relación de equivalencia.

Teorema de Lagrange

(H) G es un grupo finito.
 S es un subgrupo de G

$$(T) |S| \mid |G|$$

Demostración:

Ya probamos que las coclases $a * S$ respecto de S cumplen:

① $\forall a \in G, a \in (a * S)$

por lo tanto la unión de todas las coclases respecto de S es G

② 2 coclases cualesquiera si son distintas como conjuntos, entonces son disjuntas.

③ $* (a * S) = |S|$ cualquiera sea la coclase $a * S$

$$\left. \begin{array}{l} G \text{ es finito por (H)} \\ \text{① , ②} \end{array} \right\} \Rightarrow |G| = \text{suma del cardinal de cada coclase.}$$

(3)

$$\left. \begin{array}{l} |G| = k \cdot |S| \end{array} \right\}$$

donde k es la cantidad de coclases distintas entre sí.

$$\Rightarrow |S| \mid |G|$$

Corolario 1

Todo grupo de orden primo es cíclico.

Demostración:

Para probar que G es cíclico hay que encontrar un $a \in G / \langle a \rangle = G$.

Tomemos $a \in G, a \neq e$. (Cualquiera pero $\neq e$)

Entonces $\langle a \rangle$ es un subgrupo de G



$|\langle a \rangle| = \vartheta(a) \geq 2$ (porque si fuera 1, $a^1 = e \Rightarrow a = e$ contradice elección de $a \neq e$)

por teorema de lagrange:

$$|\langle a \rangle| \mid |G| \stackrel{\text{p primo}}{\Rightarrow} |\langle a \rangle| = p$$

\downarrow
 ≥ 2

Concluimos:

$$\left. \begin{array}{l} |\langle a \rangle| = p \\ \langle a \rangle \subset G \\ |G| = p \end{array} \right\} \Rightarrow \langle a \rangle = G \quad (G \text{ es cíclico por estar generado por } a)$$

Corolario 2

Para todo grupo G finito, $\forall a \in G \quad \vartheta(a) \mid |G|$

Demostración:

$$\text{Sea } m = \vartheta(a) \stackrel{\text{df}}{=} a^m = e_G$$

Por teo.

$$\left. \begin{array}{l} |\langle a \rangle| = \vartheta(a) \\ \text{Por teo lagrange} \end{array} \right\} \Rightarrow \vartheta(a) \mid |G|$$

$$|\langle a \rangle| \mid |G|$$

Corolario 3

Para todo grupo G finito, $\forall a \in G \quad \Rightarrow a^{|G|} = e$

Demostración:

Por corolario 2: $|G| = k \cdot \vartheta(a) \quad k \in \mathbb{N}$

$$\boxed{\begin{array}{l} \vartheta(a) \stackrel{\text{def}}{=} \\ a^{\vartheta(a)} = e_G \end{array}}$$

$$a^{|G|} = a^{k \cdot \vartheta(a)} = (\underbrace{a^{\vartheta(a)}}_{e_G})^k$$

$$a^{|G|} = e_G = \underbrace{e_G \times \dots \times e_G}_{k \text{ veces}} = e_G \quad \Rightarrow a^{|G|} = e_G$$

Corolario 4 : Caso particular del corolario 3 para $G = U(n)$. Teo Euler-Fermat.

Sea $G = (U(n), \cdot)$ n natural.

$$|G| = \varphi(n) = |U(n)|$$

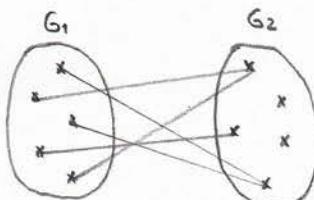
\
def de función
Euler.

Sea $a \in U(n) = G$, a probar que: $a^{\varphi(n)} \equiv 1 \pmod{n}$ o sea $a^{\varphi(n)} = e_{U(n)}$

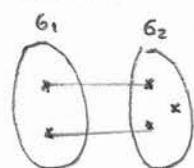
Aplicamos el corolario 3, en el caso particular $G = U(n)$.

Homomorfismos de grupos

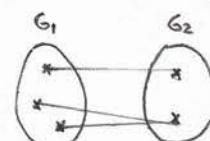
Sean G_1, G_2 dos grupos, sea $f: G_1 \rightarrow G_2$



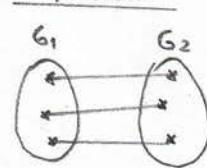
inyectiva:



sobreyectiva:



biyectiva:



$f: G_1 \rightarrow G_2$ se llama "homomorfismo de grupos" si:

① $f: G_1 \rightarrow G_2$ con $(G_1, *)$ y (G_2, \otimes) son grupos.

② $\forall a, b \in G_1 \quad f(a * b) = f(a) \otimes f(b)$

Homomorfismo de grupos

Sean $(G, *)$ y (G', \otimes) grupos.

$f: G \rightarrow G'$ se llama homomorfismo si $\forall a, b \in G$ se cumple:

$$f(a * b) = f(a) \otimes f(b)$$

Homomorfismo trivial : $f: G \rightarrow G'$ tal que $f(a) = e_{G'}$ $\forall a \in G$ ($\text{Ker}(f) = G$)

Definición : Si $f: G \rightarrow G'$ es un homomorfismo de grupos, se llama núcleo de f ($\text{Ker}(f)$) al siguiente conjunto :

$$\text{Ker}(f) = \{ a \in G \mid f(a) = e_{G'} \}$$

Ejemplo : $G = (\mathbb{Z}, +)$ $G' = (\mathbb{R}^+, \cdot)$

$j: \mathbb{Z} \rightarrow \mathbb{R}^*$ definida así : $f(n) = 2^n$.

Se cumple que $f(n+m) = f(n) \cdot f(m)$ pues $f(n+m) = 2^{n+m} = 2^n \cdot 2^m = f(n) \cdot f(m)$

En este ejemplo $\text{Ker}(j) = \{0\} = \{e_G\}$

Ejemplo : Determinante de matrices

$$GL_n = \{ M_{n \times n}(\mathbb{R}) \mid \det(a) \neq 0 \}$$

Sea $G = (GL_n, \cdot)$, $G' = (\mathbb{R}^*, \cdot)$

$$f: GL_n \rightarrow \mathbb{R}^* \quad / \quad f(A) = \det(A) \quad \forall A \in GL_n$$

$$\text{Ker}(f) = \{ A \in GL_n \mid \det(A) = 1 \}$$

Como $\det(A \cdot B) = \det(A) \cdot \det(B)$ probamos fácil que f es homomorfismo.

Ejemplo: Traza de matrices.

$$M_{n \times n} = \{ \text{Matrices } n \times n \text{ con coeficientes reales} \} \quad G = (M_{n \times n}, +) \quad G' = (\mathbb{R}, +)$$

$$f: M_{n \times n} \rightarrow \mathbb{R} \quad / \quad f(A) = \text{traza}(A) \quad \forall A \in M_{n \times n}$$

$$\text{Ker}(f) = \{ A \in M_{n \times n} \mid \text{traza}(A) = 0 \}$$

Ejemplo: Sea $n_0 \in \mathbb{N}$, fijo.

$$G = (\mathbb{Z}, +) \quad G' = (\mathbb{Z}_{n_0}, +) \quad \mathbb{Z}_{n_0} = \{ \text{Clases de congruencia m\'odulo } n_0 \text{ de enteros} \}$$

$$\mathbb{Z}_{n_0} = \{ 0 \pmod{n_0}, \dots, n_0 - 1 \pmod{n_0} \}$$

$$f: \mathbb{Z} \rightarrow \mathbb{Z}_{n_0} \quad / \quad f(m) = [m]$$

↓ clase de congruencia
de $m \pmod{n_0}$

$$\text{Ker}(f) = \{ \text{Todos los enteros m\'ultiplos de } n_0 \}$$

Ejemplo:

$$g: \mathbb{Z}_{n_0} \rightarrow \mathbb{Z} \quad / \quad g([m]) = \text{resto de dividir entre } n_0$$

$$g: \mathbb{Z}_7 \rightarrow \mathbb{Z} \quad / \quad g([m]) = \text{resto de dividir entre } 7$$

$$[6] + [5] \neq [11] = [4]$$

g no es un homomorfismo de grupos.

Ejemplo :

$$G = (\mathbb{R}^*, \cdot) \quad G' = (\mathbb{Z}_2, +)$$

Sea $f: G \rightarrow G'$ definida como: $f(a) = \begin{cases} 0 \pmod{2} & \text{si } a > 0 \\ 1 \pmod{2} & \text{si } a < 0 \end{cases}$

¿Es un homomorfismo?

¿ $\forall a, b \in \mathbb{R}^*$, $f(a.b) = f(a) + f(b)$?

Por definición de f : $f(a.b) = \begin{cases} 0 \pmod{2} & \text{si } a.b > 0 \\ 1 \pmod{2} & \text{si } a.b < 0 \end{cases}$

$$f(a) + f(b) = \begin{array}{l} \textcircled{1} \begin{cases} 0+0 \equiv 0 \pmod{2} \\ a>0, b>0 \end{cases} \quad \textcircled{2} \begin{cases} 0+1 \equiv 1 \pmod{2} \\ a>0, b<0 \end{cases} \end{array}$$

$$\begin{array}{l} \textcircled{3} \begin{cases} 1+0 \equiv 1 \pmod{2} \\ a<0, b>0 \end{cases} \quad \textcircled{4} \begin{cases} 1+1 \equiv 0 \pmod{2} \\ a<0, b<0 \end{cases} \end{array}$$

Por lo tanto $f(a.b) = f(a) + f(b) \quad \forall a, b \in \mathbb{R}^*$, luego f es homomorfismo.

$$\ker(f) = \mathbb{R}^+ = \{x \in \mathbb{R} / x > 0\}$$

Es un subgrupo del dominio de f que era (\mathbb{R}^*, \cdot)

Propiedades de homomorfismo.

f es un homomorfismo / $f: G \rightarrow G'$, G, G' grupos.

① $f(e_G) = e_{G'}$

Demostración:

$$\underbrace{f(e_G)}_{\text{en } G} = f(e_G \cdot e_G) = \overbrace{f(e_G) \cdot f(e_G)}^{\text{en } G'}$$

$$e_{G'} \cdot f(e_G) = e_{G'} \cdot f(e_G) \cdot f(e_G)$$

$$e_{G'} = e_{G'} \cdot f(e_G) = f(e_G) \Rightarrow f(e_G) = e_{G'}$$

② $\forall a \in G, f(a^{-1}) = [f(a)]^{-1}$

③ $\forall a \in G, \text{ si } \theta(a) \text{ es finito} \Rightarrow \theta(f(a)) \mid \theta(a)$

Demostración:

$$\text{Sea } m = \theta(a), \quad a^m = e_G \quad \Rightarrow \quad f(a^m) = f(e_G) \stackrel{\text{prop}}{=} e_{G'}$$

$$\Rightarrow f(\underbrace{a \cdot a \cdots a}_{m \text{ veces}}) = e_{G'}$$

Por definición de homomorfismo:

$$f(\underbrace{a \cdot a \cdots a}_{m \text{ veces}}) = f(a) \cdot f(a) \cdots f(a) = f(a)^m \Rightarrow e_{G'} = (f(a))^m$$

Entonces m es múltiplo de $\theta(f(a)) \therefore \theta(f(a)) \mid \theta(a)$

④ $\text{Ker}(f)$ es un subgrupo de G

Demostración:

Sean $a, b \in \text{Ker}(f)$ hay que probar que $a \cdot b \in \text{Ker}(f)$ y que $a^{-1} \in \text{Ker}(f)$



$$a, b \in \text{Ker}(f) \Leftrightarrow \begin{cases} f(a) = e_6 \\ f(b) = e_6 \end{cases}$$

$$f \text{ es homomorfismo} \Rightarrow f(a) \cdot f(b) = f(a.b) \Rightarrow e_6' \cdot e_6' = f(a.b) \Rightarrow e_6' = f(a.b)$$

$$a \cdot b \in \ker(f)$$

$$\text{Si } a \in \ker(f) \Rightarrow f(a) = e_G$$

$$f(a \cdot a^{-1}) = f(e_6) = e_6$$

$$= f(a) \cdot f(\bar{a}') = e_6' \Rightarrow f(\bar{a}') = e_6' \Rightarrow \boxed{\bar{a}' \in \ker(f)}$$

LQ QD

$$|\ker(f)| \leq |G|$$

Teorema:

Un homomorfismo $f: G \rightarrow G'$ de grupos es inyectivo $\Leftrightarrow \text{Ker}(f) = \{e_G\}$

Teorema: Homomorfismos inyectivos

Un homomorfismo de grupos $f: G \rightarrow G'$ es inyectivo $\leftrightarrow \ker(f) = \{e_G\}$

Demostración:

$$\text{(}\Rightarrow\text{)} \quad \text{(H)} \ f \text{ es inyectiva} \quad \text{(T)} \ \ker(f) = \{e_G\}$$

$$f(e_G) = e_{G'}$$

$$\left. \begin{array}{l} \text{Sea } a \in \ker(f) \stackrel{\text{def}}{\Rightarrow} f(a) = e_{G'} \\ \text{Por (H) } f \text{ es inyectiva} \end{array} \right\} \Rightarrow e_G = a$$

Probamos que $\forall a \in \ker(f)$

$$a = e_G$$

$$\text{o sea } \boxed{\ker(f) = \{e_G\}}$$

$$\text{(}\Leftarrow\text{)} \quad \text{(H)} \ \ker(f) = \{e_G\} \quad \text{(T)} \ f \text{ es inyectiva}$$

Sean $a, b \in G \mid f(a) = f(b)$ Hay que probar que $a = b$

$$f(a) = f(b) \rightarrow f(a) \cdot f(b^{-1}) = f(b) \cdot f(b^{-1}) \stackrel{\text{Homo...}}{\Rightarrow} f(a \cdot b^{-1}) = f(b \cdot b^{-1})$$

$$\Rightarrow f(ab^{-1}) = f(e_G) = e_{G'} \Rightarrow \boxed{f(ab^{-1}) = e_{G'}}$$

$$\left. \begin{array}{l} ab^{-1} \in \ker(f) \\ \text{por (H) } \ker(f) = \{e_G\} \end{array} \right\} \Rightarrow a \cdot b^{-1} = e_G \Leftrightarrow ab^{-1}b = e_Gb \Leftrightarrow ae_G = e_Gb \Leftrightarrow \boxed{a = b}$$

Corolarios

$$\textcircled{1} \quad |G| = p, \quad p \text{ primo.}$$

$f: G \rightarrow G'$ homomorfismo

$$\left. \begin{array}{l} |G| = p \\ f: G \rightarrow G' \text{ homomorfismo} \end{array} \right\} \rightarrow \begin{cases} 0 \text{ bien } f \text{ es trivial } (f(a) = e_{G'} \forall a \in G) \\ 0 \text{ bien } f \text{ es inyectiva} \end{cases}$$

Demostración:Ker(f) es subgrupo de G .

por teo lagrange

$$\left. \begin{array}{l} |\text{Ker}(f)| \mid |G| = p \\ |\text{Ker}(f)| = p \end{array} \right\} \Rightarrow \begin{cases} |\text{Ker}(f)| = 1 \\ |\text{Ker}(f)| = p \end{cases}$$

Caso 1:

$$\text{Si } |\text{Ker}(f)| = 1 \Rightarrow \text{Ker}(f) = \{e_G\} \stackrel{\text{THI}}{\Rightarrow} f \text{ es inyectiva.}$$

Caso 2:

$$\left. \begin{array}{l} |\text{Ker}(f)| = p = |G| \\ \text{Ker}(f) \subset G \end{array} \right\} \Rightarrow \text{Ker}(f) = G \Rightarrow f \text{ es trivial.}$$

$$\textcircled{2} \quad f: G \rightarrow G' \text{ homomorfismo}$$

$p = |G| \text{ primo}$

$$\left. \begin{array}{l} p = |G| \text{ primo} \\ |G| > |G'| \end{array} \right\} \rightarrow f \text{ es trivial}$$

Demostración:

Deriva del corolario 1

Ejemplo:

Sea $f: \mathbb{Z}_4 \rightarrow \mathbb{Z}_3$ homomorfismo. Probar que f es trivial.

$$\forall a \in \mathbb{Z}_4, \quad \boxed{\vartheta(f(a)) \mid \vartheta(a)}$$

$$\vartheta(f(a)) = |\langle f(a) \rangle| \quad | \quad |\mathbb{Z}_3| = 3 \quad \Rightarrow \quad \vartheta(f(a)) \mid 3 \quad \begin{cases} \vartheta(f(a)) = 1 \\ \vartheta(f(a)) = 3 \end{cases}$$

$$\vartheta(a) = |\langle a \rangle| \quad | \quad |\mathbb{Z}_4| = 4 \quad \Rightarrow \quad \vartheta(a) \mid 4$$

$$\text{como } \vartheta(a) \mid 4 \Rightarrow \begin{cases} \vartheta(f(a)) \mid 4 \\ \vartheta(f(a)) \mid 3 \end{cases} \quad \Rightarrow \quad \vartheta(f(a)) = 1$$

$$f(a) = b$$

$$b' = e_{G'} \quad \text{porque } \vartheta(b) = 1 \quad \Rightarrow \boxed{f(a) = e_{G'}}$$

Esto demuestra que $f(a) = e_{G'} \quad \forall a \in G$
o sea, f es trivial.

Propiedades

Si $f: G \rightarrow G'$ homomorfismo

$$\begin{aligned} \textcircled{1} \quad & \text{ Si } |G'| \text{ es finito} \\ & \text{ Si } a \in G / \vartheta(a) \text{ finito} \end{aligned} \quad \left. \begin{array}{l} \\ \end{array} \right\} \Rightarrow \vartheta(f(a)) \mid \text{MCD}(\vartheta(a), |G'|)$$

$$\textcircled{2} \quad \begin{array}{l} \text{ Si } |G|, |G'| \text{ es finito} \\ \text{ MCD}(|G|, |G'|) = 1 \end{array} \quad \left. \begin{array}{l} \\ \end{array} \right\} \Rightarrow f \text{ es trivial}$$

Demostración:

Cuando $\vartheta(a)$ es finito, probamos que $\vartheta(f(a))$ también es finito

por teo Lagrange: $\begin{cases} \vartheta(f(a)) = |\langle f(a) \rangle| \mid |G'| \\ \vartheta(a) = |\langle a \rangle| \mid |G| \end{cases}$

$$\boxed{\vartheta(f(a)) \mid \vartheta(a)}$$

$$\boxed{\vartheta(f(a)) \mid |G'|}$$

* $\theta(f(a))$ es divisor común de $\theta(a)$ y $|G'| \Rightarrow \theta(f(a)) \mid \text{MCD}(\theta(a), |G'|)$ B_{prop 1}

* $\theta(f(a))$ es un divisor común de $|G|$ y $|G'|$, por (H) $\text{MCD}(|G|, |G'|) = 1$

$$\Rightarrow \theta(f(a)) = 1 \Rightarrow f(a)^1 = e_{G'} \Rightarrow f(a) = e_{G'} \quad \forall a \in G \Rightarrow f \text{ es trivial} \quad \text{prop 2}$$

Ejemplo:

$$f: D_3 \rightarrow \mathbb{Z}_2 \quad \text{homomorfismo.}$$

(D_3, \circ) grupo diedral.

$(\mathbb{Z}_2, +)$ grupo.

$$D_3 = \{ \text{id}, \text{rot}_1, \text{rot}_2, \text{sim}_1, \text{sim}_2, \text{sim}_3 \}$$

$$\mathbb{Z}_2 = \{ 0 \pmod{2}, 1 \pmod{2} \}$$

Probar que f es:

- o bien trivial

- o bien está definida:

$$\begin{cases} f(\text{id}) = 0 \pmod{2} \\ f(\text{rot}_1) = 0 \pmod{2} \\ f(\text{rot}_2) = 0 \pmod{2} \\ f(\text{sim}_1) = 1 \pmod{2} \\ f(\text{sim}_2) = 1 \pmod{2} \\ f(\text{sim}_3) = 1 \pmod{2} \end{cases}$$

Demostración:

$$\forall a \in D_3 : \theta(f(a)) \mid |\mathbb{Z}_2| = 2 \quad \begin{cases} \theta(f(a)) = 1 \\ \theta(f(a)) = 2 \end{cases}$$

$$\theta(f(a)) \mid \theta(a) \quad \forall a \in D_3$$

$$\theta(f(a))$$

$$\theta(a)$$

$$- \theta(f(\text{id})) = \theta_G(0) = 1$$

$$\theta_G(\text{id}) = 1$$

$$- \theta_G(f(\text{rot}_1)) \mid \theta_G(\text{rot}_1) = 3 \quad \left\{ \begin{array}{l} \theta_G(f(\text{rot}_1)) = 1 \\ \theta_G(f(\text{rot}_1)) \mid |\mathbb{Z}_2| = 2 \end{array} \right.$$

$$\theta_G(\text{rot}_1) = 3$$

$$\text{rot}_1 \circ \text{rot}_1 \circ \text{rot}_1 = \text{rot}_1^3 = \text{id}$$

$$\theta_G(f(\text{rot}_2)) = 3$$

$$\theta_G(\text{sim}_1) = 2$$

$$\text{sim}_1 \circ \text{sim}_1 = \text{sim}_1^2 = \text{id}$$

$$\theta_G(f(\text{sim}_2)) = 2$$

$$\theta_G(f(\text{sim}_3)) = 2$$

$$\text{Entonces } f(\text{rot}_1)^1 = e_{G'} = 0 \pmod{2}$$

$$\begin{cases} f(\text{sim}_1) = 1 \pmod{2} \\ 0 \pmod{2} \end{cases}$$

$$- \text{sim}_1 \circ \text{rot}_1 = \text{sim}_2$$

$$\text{rot}_1 \circ \text{sim}_1 = \text{sim}_3$$

$$\text{Como } f \text{ es homomorfismo : } \left. \begin{array}{l} f(\text{sim}_2) = f(\text{sim}_1) + f(\text{rot}_1) \\ f(\text{sim}_3) = f(\text{rot}_1) + f(\text{sim}_1) \end{array} \right\} \Rightarrow f(\text{sim}_2) = f(\text{sim}_1) = f(\text{sim}_3)$$

$$f(\text{sim}_3) = f(\text{rot}_1) + f(\text{sim}_1)$$

LQOD

Teorema de los órdenes para homomorfismos de grupos.

Sea $f: G \rightarrow G'$ homomorfismo de grupos, $|G|$ finito.

Entonces :

$$|G| = |\text{Ker}(f)| \cdot |\text{Im}(f)|$$

Propiedades de $\text{Im}(f)$

$f: G \rightarrow G'$ es homomorfismo de grupos.

① $\text{Im}(f)$ es un subgrupo de G'

Demostración :

cierre : Si $x, y \in \text{Im}(f)$ en $G' \Rightarrow x * y \in \text{Im}(f)$ en G'

$x \in \text{Im}(f) \Rightarrow x = f(a)$ para algún $a \in G$

$y \in \text{Im}(f) \Rightarrow y = f(b)$ para algún $b \in G$

$$x * y = f(a) * f(b) = f(a * b) \underset{\substack{| \\ \text{Homomo...}}}{\Rightarrow} x * y \in \text{Im}(f)$$

Inverso: Si $x \in \text{Im}(f) \Rightarrow x^{-1} \in \text{Im}(f)$

$x \in \text{Im}(f) \Rightarrow x = f(a)$ para algún $a \in G$

$$\boxed{x^{-1} = f(a^{-1})} \text{ prop} \Rightarrow x^{-1} \in \text{Im}(f)$$

② $|\text{Im}(f)| \mid |G|$

Demostración :

Por prop 1 $\text{Im}(f)$ es subgrupo de G' $\left\{ \begin{array}{l} \text{teo Lagrange} \\ \Rightarrow |\text{Im}(f)| \mid |G'| \end{array} \right.$
 $|G'|$ es finito

Afirmación: Sea $(G, *)$ un grupo. $\forall a, b \in G$. $f: G \rightarrow G'$ homomorfismo.
 Sea (G', \otimes) un grupo
 La coclase de a coincide con la coclase de $b \iff f(a) = f(b)$

Demostración:

$$\begin{aligned} a * S = b * S &\iff a \in b * S \iff a = b * s \text{ para algún } s \in S \\ &\iff b^{-1} * a = s \text{ para algún } s \in S = \text{Ker}(f) \iff b^{-1} * a \in \text{Ker}(f) \\ &\iff \underset{\text{def Ker}(f)}{f(b^{-1} * a)} = e_{G'} \iff \underset{\text{def homomorfismo}}{f(b^{-1}) \otimes f(a)} = e_{G'} \iff \underset{\text{prop}}{(f(b))^{-1} \otimes f(a)} = e_{G'} \\ &\quad f(b^{-1}) = f(b)^{-1} \\ &\iff f(a) = f(b) \end{aligned}$$

Consecuencia:

※ coclases diferentes = ※ elementos diferentes que se obtienen (en G') de aplicar f a todos los elementos de G .

$$\Rightarrow \text{※ coclases diferentes} = |\text{Im}(f)| \quad \textcircled{1}$$

Teorema de los ordenes para homomorfismos de grupos

(H) $f: G \rightarrow G'$ homomorfismo de grupos, $|G|$ es finito.

(T) $|G| = |\text{Ker}(f)| \cdot |\text{Im}(f)|$

\downarrow subgrupo de G'
 \downarrow subgrupo de G

Demostración: Ya probamos: \forall grupo finito

- $\forall a \in G$, $a \in a * S$
- 2 coclases que se intersectan, son la misma (como conjunto)
- Para cada coclase, su cantidad de elementos es $|S|$

$$|S| \cdot (\text{cantidad de colectas}) = |G| \quad ②$$

Por ①, ② $\Rightarrow |G| = |\ker(f)| \cdot |\operatorname{Im}(f)|$ LQDD

Isomorfismos

Definición: $f: G \rightarrow G'$ es un "isomorfismo de grupos" si es:

- f un homomorfismo de grupos
- f es biyectiva

Definición: Dos grupos G, G' son "isomorfos" si \exists algún isomorfismo:

$$f: G \rightarrow G'$$

Obs: Si G, G' son isomorfos $\Rightarrow |G| = |G'|$

$$f: G \rightarrow G' \text{ es isomorfismo} \iff \begin{cases} \ker(f) = \{e_G\} \\ \operatorname{Im}(f) = G' \end{cases}$$

Obs: Si $f: G \rightarrow G'$ es biyectiva \Rightarrow existe otra función f^{-1} biyectiva tal que:

$$f^{-1}: G' \rightarrow G \mid \forall a \in G : f^{-1}(f(a)) = a$$

$$\forall x \in G' : f(f^{-1}(x)) = x$$

Proposición:

Si $f: G \rightarrow G'$ es un isomorfismo $\Rightarrow f^{-1}: G' \rightarrow G$ también lo es.

Demostración:

Hay que probar que $f^{-1}(x+y) = f^{-1}(x) + f^{-1}(y) \quad \forall x, y \in G'$

Es decir, $\forall x, y \in G' \mid x = f(a) \quad y = f(b)$ para algún $a, b \in G$

Propiedades de isomorfismo

Sea $f: G \rightarrow G'$ isomorfismo, entonces:

① $\forall a \in G$, si $\theta(a)$ es finito $\Rightarrow \theta(a) = \theta(f(a))$

Demostración:

$$\left. \begin{array}{l} f \text{ es isomorfismo} \Rightarrow f \text{ es homomorfismo} \\ \theta(a) \text{ finito} \end{array} \right\} \Rightarrow \boxed{\theta(f(a)) \mid \theta(a)}$$

Por proposición, $f^{-1}: G' \rightarrow G$ también es isomorfismo $\Rightarrow \theta(f^{-1}(f(a))) \mid \theta(f(a)) \wedge f(a) \in G$

Por definición de transformación inversa $f^{-1}(f(a)) = a$

$$\Rightarrow \boxed{\theta(a) \mid \theta(f(a))}$$

$$\Rightarrow \theta(a) = \theta(f(a)) \quad \text{LQOD.}$$

② Si G es cíclico $\Rightarrow G'$ también lo es.

Además, un generador de G' es $f(a)$ donde a es un generador de G .

Demostración:

(H) $G = \langle a \rangle$ para algún $a \in G$. $G = \{e_G, a, a^2, \dots, a^i, \dots, a^{m-1}\}$ $m = \theta(a)$

(T) $G' = \langle f(a) \rangle$

$$\text{Im}(f) = G' = \{e_{G'}, f(a), f(a^2), \dots, f(a^i), \dots, f(a^{m-1})\}$$

$$\Rightarrow \text{por homomorfismo } f(a^2) = f(a \cdot a) = f(a) * f(a) = (f(a))^2$$

$$\text{Im}(f) = G' = \{e_{G'}, f(a), (f(a))^2, \dots, (f(a))^i, \dots, (f(a))^{m-1}\}$$

$$\Rightarrow G' = \langle f(a) \rangle \quad \text{LQOD}$$

③ Si G es abeliano $\Rightarrow G'$ también lo es.

Ejemplos:

① Averiguar si $(\mathbb{Z}_6, +)$ y (S_3, \circ) son isomorfos.

permutaciones de
3 elementos

$$|\mathbb{Z}_6| = 6$$

$$|S_3| = 3! = 6$$

\mathbb{Z}_6 es abeliano.

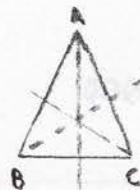
S_3 no es abeliano (La composición de permutaciones de 3 elem.
no es conmutativa)

Conclusión: \mathbb{Z}_6 y S_3 no son isomorfos

② S_3 y D_3 son isomorfos.

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\text{rot}_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$



Definición: Sea $n \geq 2$ natural fijo. Consideremos el grupo $(U(n), \cdot)$

Sea $a \in U(n)$, a se llama raíz primitiva mod n si $U(n) = \langle a \rangle$

Obs: Si existe a raíz primitiva mod $n \Rightarrow U(n)$ es cíclico y está generado por a .

Obs: ① a es raíz primitiva mod $n \Leftrightarrow \varphi(a) = |U(n)|$ o sea $\varphi(a) = \varphi(n)$

② a es raíz primitiva mod $n \Leftrightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$
 $\forall d$ natural $< \varphi(n) \quad a^d \not\equiv 1 \pmod{n}$

③ a es raíz primitiva mod $n \Leftrightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$
 $\forall d$ natural $\neq \varphi(n) \quad / \quad d \mid \varphi(n) \quad a^d \not\equiv 1 \pmod{n}$

Ejemplos:

① $U(2) = \{1 \pmod{2}\}$

$$\langle 1 \rangle = U(2)$$

1 es raíz primitiva mod 2, es la única raíz primitiva mod 2.

② $U(3) = \{1 \pmod{3}, 2 \pmod{3}\}$

$$2^2 = 4 \equiv 1 \pmod{3} \quad \Rightarrow \quad \varphi(2 \pmod{3}) = 2$$

$$\varphi(2) = |U(3)| \quad \langle 2 \rangle = U(3)$$

2 es raíz primitiva mod 3, es la única raíz primitiva mod 3.

③ $U(4) = \{1 \pmod{4}, 3 \pmod{4}\}$

$$3^2 = 9 \equiv 1 \pmod{4} \quad \varphi(3 \pmod{4}) = |U(4)| = 2 \quad \langle 3 \rangle = U(4)$$

3 es raíz primitiva mod 4.

$$(4) \quad U(5) = \{ 1 \pmod 5, 2 \pmod 5, 3 \pmod 5, 4 \pmod 5 \}$$

$$2^2 = 4 \pmod 5$$

$$\varphi(\bar{2}) = |U(5)| = 4$$

$$2^3 = 8 \equiv 3 \pmod 5$$

$$\langle 2 \rangle = U(5)$$

$$2^4 = 16 \equiv 1 \pmod 5$$

2 es raíz primitiva mod 5.

$$3^2 = 9 \equiv 4 \pmod 5$$

$$\varphi(\bar{3}) = 4$$

$$3^3 = 27 \equiv 2 \pmod 5$$

$$\langle 3 \rangle = U(5)$$

$$3^4 \equiv 6 \equiv 1 \pmod 5$$

3 es raíz primitiva mod 5.

$$4^2 = 16 \equiv 1 \pmod 5$$

$$\varphi(\bar{4}) = 2 \neq |U(5)|$$

$$\langle 4 \rangle \neq U(5)$$

4 no es raíz primitiva mod 5.

$$(5) \quad U(8) = \{ 1 \pmod 8, 3 \pmod 8, 5 \pmod 8, 7 \pmod 8 \}$$

$$|U(8)| = \varphi(8) = 4$$

$$3^2 = 9 \equiv 1 \pmod 8$$

$$\varphi(\bar{3}) = 2 \neq |U(8)|$$

3 no es raíz primitiva mod 8

$$5^2 = 25 \equiv 1 \pmod 8$$

$$7^2 = 49 \equiv 1 \pmod 8$$

$$\varphi(\bar{5}) = \varphi(\bar{7}) = 2 \neq |U(8)|$$

5, 7 no son raíces primitivas mod 8

U(n) no es cíclico \Leftrightarrow no existen raíces primitivas mod n

Recordar:

G grupo

$$\left. \begin{array}{l} a \in G \\ a^h = e_G \end{array} \right\} \Leftrightarrow b \text{ es múltiplo de } \varphi(a) \text{ en } G$$

Lema 1(H) Si a es raíz primitiva mod n Si k es natural, $k \leq \varphi(n)$ y $\text{MCD}(k, \varphi(n)) = 1$ (T) a^k también es raíz primitiva mod n (o sea $\varphi(a^k) = \varphi(n)$)

Demostración:

Sea $m = \varphi(a^k)$

$$\text{Por teo Lagrange} \quad m = \varphi(a^k) \quad \left. \begin{array}{l} a^k \in U(n) \end{array} \right\} \Rightarrow m \mid |U(n)| = \varphi(n) \quad \text{o sea} \quad \boxed{m \mid \varphi(n)}$$

$$m = \varphi(a^k) \stackrel{\text{def}}{\Rightarrow} (a^k)^m \equiv 1 \pmod{n} \Rightarrow a^{k \cdot m} \equiv 1 \pmod{n} \stackrel{(H)}{\Rightarrow} \varphi(a) \mid k \cdot m$$

$$\left. \begin{array}{l} \varphi(n) \mid k \cdot m \\ \text{MCD}(k, \varphi(n)) = 1 \end{array} \right\} \stackrel{\text{Lema Euclides}}{\Rightarrow} \boxed{\varphi(n) \mid m}$$

$$\Rightarrow m = \varphi(n) \quad \text{o sea} \quad \varphi(a^k) = \varphi(n)$$

Lema 2(H) Si a es raíz primitiva mod n Si k es natural, $k \leq \varphi(n)$ y si $\text{MCD}(k, \varphi(n)) \neq 1$ (T) a^k no es raíz primitiva mod n (o sea $\varphi(a^k) \neq \varphi(n)$)

Demostración:

Tarea.

Proposición

Si existe alguna raíz primitiva $a \bmod n \Rightarrow$ La cantidad de raíces primitivas mod n
 es : $\varphi(\varphi(n))$

Demostación:

$$\textcircled{H} \quad \exists a \in U(n) \mid \langle a \rangle = U(n)$$

$$\vartheta(a) = |U(n)| = \varphi(n)$$

$$U(n) = \{e, a, a^2, \dots, a^{\varphi(n)-1}\}$$

Todo elemento de $U(n)$ es de la forma a^k .

Para encontrar las otras raíces primitivas mod n (además de a), tengo que mirar solo las potencias de a .

$$a^k \text{ con } 1 \leq k < \varphi(n)$$

Por Lemas 1, 2

$$\text{k} \cdot \text{MCD}(k, \varphi(n)) = 1 \iff a^k \text{ es raíz primitiva mod } n$$

Entonces, ¿Cuántas raíces primitivas mod n existen?

Hay tantas como: $\#\{k \leq n : 1 \leq k \leq \varphi(n) \mid k \text{ coprimo con } \varphi(n)\}$

Por definición de función de Euler es $\varphi(\varphi(n))$

Teorema de las raíces primitivas

Sea $n \geq 2$ natural.

Existen $\varphi(n)$ raíces primitivas mod $n \iff n$ es alguno de estos naturales

Caso 1 : $n = 2$

Caso 2 : $n = 4$

Caso 3 : $n = p^\alpha$ donde p primo e impar y $\alpha \in \mathbb{N}$ cualquiera.

Caso 4 : $n = 2p^\alpha$ donde p primo e impar y $\alpha \in \mathbb{N}$ cualquiera.

Demostración :

(\Leftarrow)

Caso 1 : $\text{(H)} \quad n = 2 \quad \text{(T) existen raíces primitivas mod } n$

→ Demostrado en ejemplo.

Caso 2 : $\text{(H)} \quad n = 4 \quad \text{(T) existen raíces primitivas mod } n$

Caso 3 : $\text{(H)} \quad n = p^\alpha \quad \text{(T) existen raíces primitivas mod } n$
 p primo impar
 $\alpha \in \mathbb{N}$

Caso 4 : $\text{(H)} \quad n = 2p^\alpha \quad \text{(T) existen raíces primitivas mod } n$
 p primo impar
 $\alpha \in \mathbb{N}$

Vamos a probar el caso 3 : Lo vamos a probar solamente en el caso $\alpha = 1$

(Sub teorema)

Si p es primo $\implies \exists$ raíces primitivas $(\text{mod } p)$ o sea $(U(p), \circ)$ es cíclico.

Pendiente, próxima clase.

Lema 3(H) $\forall n \text{ natural}, n \geq 2$

(T) $\vartheta(a \cdot b) = \vartheta(a) \cdot \vartheta(b)$

S. $a, b \in U(n)$

S. $\text{MCD}(\vartheta(a), \vartheta(b)) = 1$

Lema 4Sea la ecuación $x^a \equiv 1 \pmod{n}$ Si $d | \varphi(n) \Rightarrow$ La ecuación tiene exactamente d soluciones mod n .

Recordamos lemas clase anterior:

Lema 3:

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

$a, b \in U(n)$

$\text{MCD}(\vartheta(a), \vartheta(b)) = 1$

(T) $\vartheta(ab) = \vartheta(a) \cdot \vartheta(b)$

(Este lema vale en cualquier grupo abeliano)

Lema 4:

(H) $\forall p$ primo

si $d \mid \vartheta(p)$

(T) $x^d \equiv 1 \pmod{p}$ tiene exactamente d soluciones distintas módulo p.

Teorema:

Si p es primo $\Rightarrow U(p)$ es cíclico.

(Es decir $\exists a \in U(p) / \langle a \rangle = U(p)$ o sea $\vartheta(a) = \varphi(p) = p-1$)

Demostración:

Objetivo: $\exists a \in U(p) / \vartheta(a) = |U(p)|$ o sea $\vartheta(a) = \varphi(p) = p-1$

$$p-1 = q_1^{\alpha_1} \cdots q_h^{\alpha_h} \quad \text{con } q_i \text{ primos diferentes dos a dos}$$

Paso 1: Objetivo:

$\exists a_1 \in U(p) / \vartheta(a_1) = q_1^{\alpha_1}$

$\exists a_h \in U(p) / \vartheta(a_h) = q_h^{\alpha_h}$

Sea $d = q_1^{\alpha_1-1} \Rightarrow d \mid p-1 = |U(p)| \Rightarrow$ La cantidad de soluciones de

$x^d \equiv 1 \pmod{p}$ es d.

Sea $d' = q_1^{\alpha_1} = d \cdot q_1 \Rightarrow d' \mid p-1 \Rightarrow$ La cantidad de soluciones de

$x^{d'} \equiv 1 \pmod{p}$ es d'

$$\text{Si } x^d \equiv 1 \pmod{p} \Rightarrow (x^d)^{q_1} = x^{d'} \equiv 1 \pmod{p}$$

$$dq_1 > d$$

B.Sz

Entonces \exists alguna solución $a_1 \in U(p)$ que cumple: $x^{d'} \equiv 1 \pmod{p}$ y no cumple $x^d \equiv 1 \pmod{p}$

Es decir, $\exists a_1 \in U(p) / a_1^{q_1 \cdot \alpha_1} \equiv 1 \pmod{p}$ y no se cumple que $a_1^{\alpha_1} \not\equiv 1 \pmod{p}$

$$\Rightarrow \begin{cases} \theta(a_1) \mid q_1^{\alpha_1} \\ \theta(a_1) \nmid q_1^{\alpha_1-1} \end{cases} \Rightarrow \theta(a_1) = q_1^{\alpha_1}$$

Paso 2: $\theta(a_1)$ y $\theta(a_2)$ son coprimos $\xrightarrow{\text{Lema 3}} \theta(a_1 \cdot a_2) = \theta(a_1) \cdot \theta(a_2)$

Aplicando muchas veces el lema 3

$$\theta(a_1 \cdot a_2 \cdots a_h) = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdots q_h^{\alpha_h} = p-1 \Rightarrow U(p) \text{ es cíclico.}$$

————— 9 —————

Demostración Lema 3:

Sea $m = \theta(a)$, $m' = \theta(b)$

Por ④ $(m, m') = 1 \Rightarrow \text{mcm}(m, m') = m \cdot m' \cdot 1$

$$(a \cdot b)^{m \cdot m'} = a^{m \cdot m'} \cdot b^{m \cdot m'} = (a^m)^{m'} \cdot (b^{m'})^m = e^{m'} \cdot e^m = e \Rightarrow \theta(a \cdot b) \mid m \cdot m'$$

abeliano

Sea $h = \theta(a \cdot b)$

$$(a \cdot b)^h = e = a^h \cdot b^h \Rightarrow \begin{matrix} a^h = (b^h)^{-1} \\ | \quad | \\ \langle a \rangle \quad \langle b \rangle \end{matrix} \in \langle a \rangle \cap \langle b \rangle = S$$

$$\left. \begin{array}{l} |S| \mid |\langle a \rangle| = \theta(a) = m \\ |S| \mid |\langle b \rangle| = \theta(b) = m' \\ (m, m') = 1 \end{array} \right\} \Rightarrow |S| = 1 \Rightarrow S = \{e\} \Rightarrow \begin{matrix} a^h = e \\ b^h = e \end{matrix}$$

$$\left. \begin{array}{l} \theta(b) \mid h \Rightarrow m' \mid h \\ \theta(a) \mid h \Rightarrow m \mid h \end{array} \right\} \Rightarrow \text{mcm}(m, m') \mid h$$

$$\left. \begin{array}{l} m \cdot m' = h = \theta(a \cdot b) \end{array} \right\} \Rightarrow m \cdot m' \mid h$$

Vamos a probar algo mas fuerte:

$$h = \#\{ \text{raíces } \pmod p \text{ de polinomio de grado } d \} \leq d$$

Demostración Lema 4:

$$\text{Sea } K = \#\{ \text{soluciones distintas } \pmod p \text{ de } x^d \equiv 1 \pmod p \}$$

Paso 1 Obj: $h \leq d$

Supongamos por absurdo que $h > d$.

Elegí exactamente $d+1$ soluciones distintas $\pmod p$: a_1, a_2, \dots, a_{d+1}

$$a_i \not\equiv a_j \pmod p \quad \forall i \neq j$$

a_i verifica $P_d(x) \equiv 0 \pmod p$ $\mathbb{Z}_p, +, \cdot$

Bajo
por ruffini
operando $\pmod p$

$$P_d(x) \equiv (x - a_1) Q_{d-1}(x) \pmod p$$

$$\text{Como } a_2 \text{ es raíz } \Rightarrow P_d(a_2) \equiv (a_2 - a_1) Q(a_2) \equiv 0 \pmod p$$

Por el teorema de euclides $a_2 - a_1 \equiv 0 \pmod p$ \rightarrow no puede ser porque
 $a_1 \neq a_2$

$$P_{d-1}(a_2) \equiv 0 \pmod p$$

Entonces a_2 es raíz de $P_{d-1}(a_2)$, bajo por ruffini. $Q_{d-1}(x)$ dividido $x - a_2$

$$\Rightarrow P_d(x) = (x - a_1)(x - a_2) Q_{d-2}(x)$$

Bajo por ruffini una cantidad de veces finita con las d primeras raíces de $P_d(x)$

$$\Rightarrow P_d(x) = (x - a_1)(x - a_2) \dots (x - a_d)$$

$$a_{d+1} \text{ también es raíz } \Rightarrow 0 \equiv P_d(a_{d+1}) = (a_{d+1} - a_1) \dots (a_{d+1} - a_d) \equiv 0 \pmod p$$

Lema euclides . algún factor $(a_{d+1} - a_i) \equiv 0 \pmod p$

$$a_{d+1} \equiv a_i \pmod p \quad \text{para algún } i \leq d \quad \text{Absurdo!!}$$

Paso 2 : $\boxed{h \geq d}$

$$d \mid p-1 = \varphi(p) \implies p-1 = d \cdot h \quad h \in \mathbb{N}.$$

$$\text{Teorema euler-Fer} \implies x^{p-1} \equiv 1 \pmod{p} \quad \forall x \in U(p)$$

↓ tiene exactamente $p-1$ raíces diferentes

$$d \cdot h = p-1 \quad (x^d)^h - 1 \equiv 0 \pmod{p} \quad \text{tiene } p-1 \text{ raíces distintas}$$

$$\alpha^{h-1} \equiv (\alpha-1)(\alpha^{h-1} + \alpha^{h-2} + \dots + \alpha + 1) \equiv 0 \pmod{p}$$

$$(x^d)^{h-1} \equiv (x^{d-1})(x^{d(h-1)} + \dots + x^d + 1) \equiv 0 \pmod{p}$$

$$\text{Lemma Euclides: 0 bien } x^d - 1 \equiv 0 \pmod{p}$$

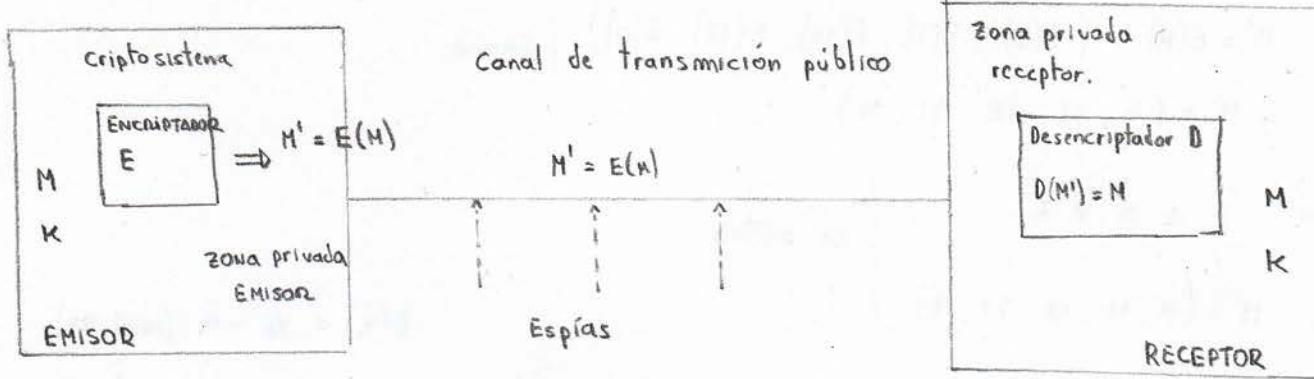
$$0 \text{ bien } (x^{d(h-1)} + \dots + x^d + 1) \equiv 0 \pmod{p}$$

$$p-1 = \underbrace{\#\{ \text{sol de } x^d - 1 \equiv 0 \pmod{p} \}}_h + \#\{ \text{sol de } (\quad) \} \leq d(h-1)$$

$$p-1 \leq h + d(h-1) \implies h \geq p-1 - dh + d = d$$

$$\Rightarrow \boxed{h \geq d} \quad \text{LQDD.}$$

Criptografía



M' es el mensaje encriptado

El mensaje M tiene longitud L . $M = (x_1, x_2, \dots, x_L)$ $0 \leq x_i \leq n-1$

$$E(M) = (E_1(x_1), E_2(x_2), \dots, E_L(x_L))$$

K = clave

ASCII $n = 128$

Se clasifican en : ① Clave "secreta" o "privada"
② Clave pública.

Clave secreta o privada

A) Método de encriptado

Método César

$$k = R$$

$$\text{Supongamos } n = 27$$

R es un número secreto entre 1 y 26 $1 \leq R \leq 26$

$$E(x_i) = x_i + k \pmod{n}$$

$$D(y_i) = y_i - k \pmod{n}$$

Verificación:

$$D(E(x)) = D\left(\underbrace{(x+k) \pmod{n}}_y\right) = [(x+k) \pmod{n} - k] \pmod{n}$$

$$= x \pmod{n}$$

Ejemplo:

Palabra: AHORA , $K = 4$

codifico : $M = (0, 7, 14, 17, 0)$

$$E(x_i) = x_i + 4 \pmod{27}$$

Encripto : $M' = E(M) = (E(0), E(7), E(14), E(17), E(0))$

} EMISOR

$$M' = (4, 11, 18, 21, 4)$$

decodifico : E L S V E

} se saltea

codifico : $M' = (4, 11, 18, 21, 4)$

$$D(y_i) = y_i - 4 \pmod{27}$$

Desencripto : $M = D(M') = (D(4), D(11), D(18), D(21), D(4))$

$$M = (0, 7, 14, 17, 0)$$

} RECEPTOR

Decodifico : AHORA.

Variación del método César

La función E es AFIN

La clave $K = (a, R)$ donde a es cte $1 \leq a \leq n-1$

o sea que $\text{MCD}(a, n) = 1 \Rightarrow \exists a^{-1} \pmod{n}$

$$E(x_i) = (ax_i + R) \pmod{n}$$

$$D(y_i) = a^{-1}(y_i - R) \pmod{n}$$

Método de Vigenere

supongamos $n = 27$

$K = (R_1, R_2, \dots, R_l)$ La clave tiene longitud l , hay 27^l claves posibles.

$$M' = (E_1(x_1), E_2(x_2), \dots, E_l(x_l))$$

$$E_i(x_i) \equiv (x_i + K_{i, \text{modo}}) \pmod{n}$$

$$D_i(y_i) \equiv (y_i - K_{i, \text{modo}}) \pmod{n}$$

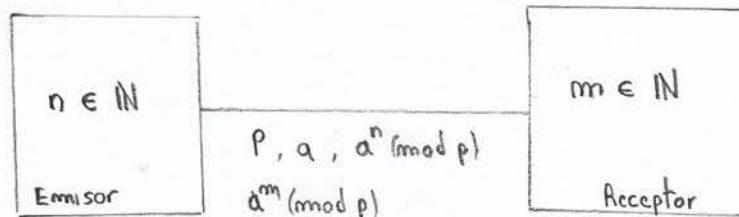
Método de Vernam

La clave es una palabra de longitud $l = L$ longitud del mensaje, c/u de sus componentes generada aleatoriamente.

La función E es afín.

(B) Método de intercambio de claveDiffie - Helmann

Quiero ponermee deacuerdo con el receptor sobre qué clave k_i usar (Ambas la misma)

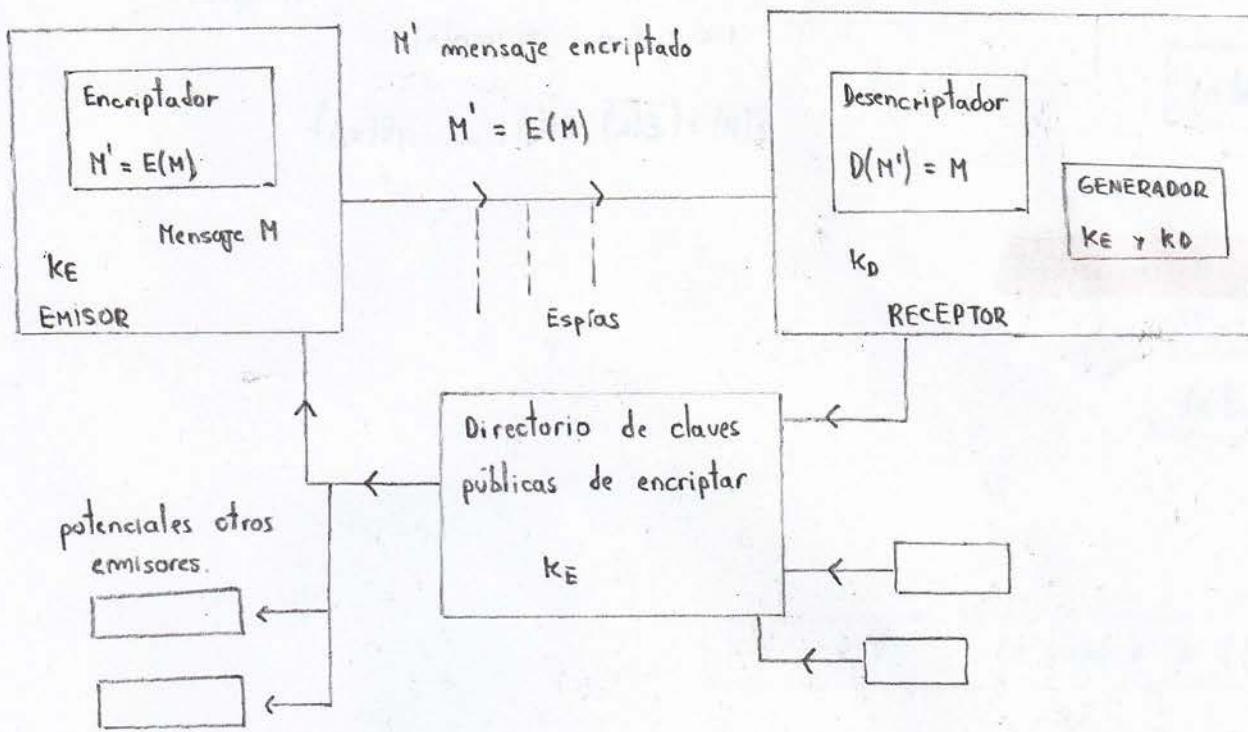


- ① El emisor y el receptor eligen un número p primo y $a / 1 < a < p$ y lo pasan por el canal.
- ② El emisor elige un número n .
- ③ El receptor elige un número m .
- ④ El emisor calcula $a^n \pmod{p}$ y lo envía por el canal.
- ⑤ El receptor " " $a^m \pmod{p}$ " "
- ⑥ La clave común es $a^{nm} \pmod{p} = (a^m)^n \pmod{p} = (a^n)^m \pmod{p}$ que tanto el emisor como el receptor pueden calcular.

Los espías solo conocen $P, a, a^n \pmod{p}, a^m \pmod{p}$.

Hallar $a^{nm} \pmod{p}$ sin saber n o m .

Problema del logaritmo discreto en \mathbb{Z}_p^*

Clave públicaR.S.A

I Generación de claves : (En el espacio privado de cada receptor). con cada receptor.

(A) Se inventan 2 números primos $p \neq q$ grandísimos.

$$n = p \cdot q \quad \varphi(n) = (p-1)(q-1)$$

(B) Se inventa un número e coprimo con $\varphi(n)$

(C) $KE = (e, n)$ es la clave de encriptado pública de cada receptor y la pública en el directorio.

(D) Se calcula por AEE $d = e^{-1} (\text{mod } \varphi(n))$

(E) $KD = (d, n)$ clave de desencriptado secreta de cada receptor.

II Función de encriptado:

Sea $x \pmod n$

recordamos: $M = (x_1, x_2, \dots, x_L)$ donde L es la longitud del mensaje.

$$E(x) \stackrel{\text{def}}{=} x^e \pmod n$$

$$1 < x_L < n \quad x_i \pmod n$$

$$E(M) = (E(x_1), E(x_2), \dots, E(x_L))$$

Función de desencriptado

$$D(y) = y^d \pmod n$$

Teorema:

$$D(E(x)) \equiv x \pmod n \quad \forall x \in \mathbb{Z}_n$$

Demostración:

$$D(E(x)) = D\left(\underbrace{x^e}_{y} \pmod n\right) = y^d \pmod n = x^{ed} \pmod n$$

$$\text{Hay que probar que } \boxed{x^{de} \equiv x \pmod n} \quad \forall x \in \mathbb{Z}_n$$

Caso 1: $\text{MCD}(x, n) = 1 \iff \begin{cases} x \not\equiv 0 \pmod p \\ x \not\equiv 0 \pmod q \end{cases}$

Demostración:

$$\text{MCD}(x, pq) = 1 \implies \boxed{x^{\varphi(n)} \equiv 1 \pmod n} \quad \text{Teo Euler}$$

$$d \cdot e \equiv 1 \pmod{\varphi(n)} \implies d \cdot e = 1 + k \cdot \varphi(n) \quad \text{para algún } k \in \mathbb{Z}$$

$$x^{de} = x^{1+k \cdot \varphi(n)} = x \cdot (x^{\varphi(n)})^k \stackrel{\substack{\downarrow \\ \text{Euler}}}{\equiv} x \cdot 1^k \pmod n \equiv x \pmod n$$

Caso 2 :

$$\begin{cases} x \equiv 0 \pmod{p} \\ x \not\equiv 0 \pmod{q} \end{cases} \quad ; \quad \begin{cases} x \not\equiv 0 \pmod{p} \\ x \equiv 0 \pmod{q} \end{cases}$$

Demostración:

$$x \not\equiv 0 \pmod{q} \stackrel{\text{Fermat}}{\Rightarrow} x^{q-1} \equiv 1 \pmod{q} \stackrel{\wedge(p-1)}{\Rightarrow} (x^{q-1})^{(p-1)} \equiv 1 \pmod{q}$$

$$x^{(q-1)(p-1)} \equiv 1 \pmod{q} \Rightarrow x^{\varphi(n)} \equiv 1 \pmod{q}$$

$$d.e \equiv 1 \pmod{\varphi(n)} \Rightarrow d.e = 1 + k \cdot \varphi(n) \text{ para algun } k \in \mathbb{Z}$$

$$x^{de} = x^{1+k\varphi(n)} = x \cdot (x^{\varphi(n)})^k \equiv x \pmod{q} \Rightarrow x^{de} - x \equiv 0 \pmod{q} \quad \textcircled{i}$$

$$x \equiv 0 \pmod{p}$$

$$x^{de} \equiv 0^{de} \equiv 0 \pmod{p} \Rightarrow x^{de} - x \equiv 0 \pmod{p} \quad \textcircled{ii}$$

$$\text{de } \textcircled{i} \text{ y } \textcircled{ii} \quad x^{de} - x \equiv 0 \pmod{n} \Rightarrow x^{de} \equiv x \pmod{n} \quad \text{LQDD.}$$

Caso 3 :

$$\begin{cases} x \equiv 0 \pmod{p} \\ x \equiv 0 \pmod{q} \end{cases} \Rightarrow x \equiv 0 \pmod{n}$$

Demostración:

$$x \equiv 0 \pmod{n} \Rightarrow x^{de} \equiv 0 \pmod{n} \Rightarrow x^{de} - x \equiv 0 \pmod{n}$$

$$\Rightarrow x^{de} \equiv x \pmod{n} \quad \text{LQDD}$$

Ejemplos

① Hallar si existe algún $x \in U(41)$ / $x^3 \equiv 15 \pmod{41}$

$$U(41) = \left\{ 1, 2, \dots, 40 \right\}_{(\text{mod } 41)} \quad |U(41)| = \varphi(41) = 40$$

$$\langle 2 \rangle = \left\{ \begin{array}{l} 1, 2, 4, 8, 16, -9, -18, 5, 10, 20, -1, -2, -4, -8, -16 \\ 2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}, 2^{13}, 2^{14} \\ , 9, 18, -5, -10, -20 \\ 2^{15}, 2^{16}, 2^{17}, 2^{18}, 2^{19} \end{array} \right\} \quad \vartheta(2) = 20$$

$$\langle 3 \rangle = \left\{ 1, 3, 9, -14, -1, -3, -9, 14 \right\} \quad \vartheta(3) = 8$$

Quiero hallar $\vartheta(x) = 5$, x debe estar en $\langle 2 \rangle$ porque $\vartheta(x) \mid \vartheta(2)$

$$2^{20} \equiv 1 \pmod{41} \Rightarrow (2^4)^5 \equiv 1 \pmod{41}$$

$$\boxed{x = 16} \quad \left. \begin{array}{l} \vartheta(16) = 5 \\ \vartheta(3) = 8 \\ \text{MCD}(5, 8) = 1 \end{array} \right\} \xrightarrow{\text{Lema}} \vartheta(16 \cdot 3) = \vartheta(16) \cdot \vartheta(3) \\ \vartheta(48) = 40$$

$$48 \equiv 7 \pmod{41} \Rightarrow \vartheta(7) = 40$$

7 es raíz primitiva mod 41

$$7 \equiv 7 \pmod{41}$$

$$7^2 \equiv 8 \pmod{41} \quad \Rightarrow \quad 7^3 \equiv 15 \pmod{41}$$

$$7^3 \equiv 56 \equiv 15 \pmod{41}$$

una solución posible de $x^3 \equiv 15 \pmod{41}$

es $x = 7 \pmod{41}$

② Demostrar que no existe $x \in U(41) / x^5 \equiv 15 \pmod{41}$

Supongamos por absurdo que existe $x \in U(41) / x^5 \equiv 15 \pmod{41}$

$$\left. \begin{array}{l} (x^5)^8 \equiv 15^8 \pmod{41} \\ x^{40} \equiv 1 \pmod{41} \end{array} \right\} \Rightarrow 15^8 \equiv 1 \pmod{41}$$

$$\varphi(15) \mid 8 \Rightarrow 15 \in \langle 3 \rangle \text{ absurdo !!}$$

| Resumen de la demostración | |
|----------------------------|---|
| 1 | El teorema CN implica que si $x \in U(41)$ entonces $x^5 \in U(41)$ |
| 2 | El teorema de Euler-Fermat implica que $x^{\varphi(41)} \equiv 1 \pmod{41}$ |
| 3 | Así pues $x^{40} \equiv 1 \pmod{41}$ |
| 4 | Por lo tanto $x^8 \equiv 1 \pmod{41}$ |
| 5 | Así pues $15^8 \equiv 1 \pmod{41}$ |
| 6 | Por lo tanto $15 \in \langle 3 \rangle$ |
| 7 | Por lo tanto $15^5 \equiv 15 \pmod{41}$ |
| 8 | Por lo tanto $15 \in U(41)$ |
| 9 | Por lo tanto $x \in U(41)$ |
| 10 | Por lo tanto $x^5 \in U(41)$ |
| 11 | Por lo tanto $x^5 \not\equiv 15 \pmod{41}$ |
| 12 | Por lo tanto es absurdo |

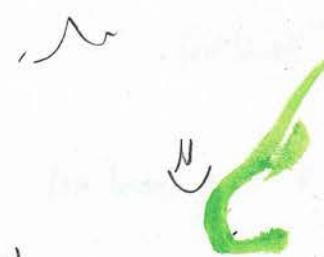
| Resumen de la demostración | |
|----------------------------|---|
| 1 | El teorema CN implica que si $x \in U(41)$ entonces $x^5 \in U(41)$ |
| 2 | El teorema de Euler-Fermat implica que $x^{\varphi(41)} \equiv 1 \pmod{41}$ |
| 3 | Así pues $x^{40} \equiv 1 \pmod{41}$ |
| 4 | Por lo tanto $x^8 \equiv 1 \pmod{41}$ |
| 5 | Así pues $15^8 \equiv 1 \pmod{41}$ |
| 6 | Por lo tanto $15 \in \langle 3 \rangle$ |
| 7 | Por lo tanto $15^5 \equiv 15 \pmod{41}$ |
| 8 | Por lo tanto $15 \in U(41)$ |
| 9 | Por lo tanto $x \in U(41)$ |
| 10 | Por lo tanto $x^5 \in U(41)$ |
| 11 | Por lo tanto $x^5 \not\equiv 15 \pmod{41}$ |
| 12 | Por lo tanto es absurdo |

| Resumen de la demostración | |
|----------------------------|---|
| 1 | El teorema CN implica que si $x \in U(41)$ entonces $x^5 \in U(41)$ |
| 2 | El teorema de Euler-Fermat implica que $x^{\varphi(41)} \equiv 1 \pmod{41}$ |
| 3 | Así pues $x^{40} \equiv 1 \pmod{41}$ |
| 4 | Por lo tanto $x^8 \equiv 1 \pmod{41}$ |
| 5 | Así pues $15^8 \equiv 1 \pmod{41}$ |
| 6 | Por lo tanto $15 \in \langle 3 \rangle$ |
| 7 | Por lo tanto $15^5 \equiv 15 \pmod{41}$ |
| 8 | Por lo tanto $15 \in U(41)$ |
| 9 | Por lo tanto $x \in U(41)$ |
| 10 | Por lo tanto $x^5 \in U(41)$ |
| 11 | Por lo tanto $x^5 \not\equiv 15 \pmod{41}$ |
| 12 | Por lo tanto es absurdo |

| Resumen de la demostración | |
|----------------------------|---|
| 1 | El teorema CN implica que si $x \in U(41)$ entonces $x^5 \in U(41)$ |
| 2 | El teorema de Euler-Fermat implica que $x^{\varphi(41)} \equiv 1 \pmod{41}$ |
| 3 | Así pues $x^{40} \equiv 1 \pmod{41}$ |
| 4 | Por lo tanto $x^8 \equiv 1 \pmod{41}$ |
| 5 | Así pues $15^8 \equiv 1 \pmod{41}$ |
| 6 | Por lo tanto $15 \in \langle 3 \rangle$ |
| 7 | Por lo tanto $15^5 \equiv 15 \pmod{41}$ |
| 8 | Por lo tanto $15 \in U(41)$ |
| 9 | Por lo tanto $x \in U(41)$ |
| 10 | Por lo tanto $x^5 \in U(41)$ |
| 11 | Por lo tanto $x^5 \not\equiv 15 \pmod{41}$ |
| 12 | Por lo tanto es absurdo |

| Resumen de la demostración | |
|----------------------------|---|
| 1 | El teorema CN implica que si $x \in U(41)$ entonces $x^5 \in U(41)$ |
| 2 | El teorema de Euler-Fermat implica que $x^{\varphi(41)} \equiv 1 \pmod{41}$ |
| 3 | Así pues $x^{40} \equiv 1 \pmod{41}$ |
| 4 | Por lo tanto $x^8 \equiv 1 \pmod{41}$ |
| 5 | Así pues $15^8 \equiv 1 \pmod{41}$ |
| 6 | Por lo tanto $15 \in \langle 3 \rangle$ |
| 7 | Por lo tanto $15^5 \equiv 15 \pmod{41}$ |
| 8 | Por lo tanto $15 \in U(41)$ |
| 9 | Por lo tanto $x \in U(41)$ |
| 10 | Por lo tanto $x^5 \in U(41)$ |
| 11 | Por lo tanto $x^5 \not\equiv 15 \pmod{41}$ |
| 12 | Por lo tanto es absurdo |

| Resumen de la demostración | |
|----------------------------|--|
| 1 | El sistema para la inducción es el siguiente: sea $x \in U(41)$ y tomemos un número de $n \in \mathbb{N}$ tal que $x^n \equiv 15 \pmod{41}$. Entonces $x^{n+5} \equiv 15^2 \pmod{41}$, es decir $x^{n+5} \not\equiv 1 \pmod{41}$. |
| 2 | Si $x^{n+5} \not\equiv 1 \pmod{41}$ entonces $x^{n+5} \in U(41)$ y $x^{n+5} \not\in \langle 3 \rangle$. |
| 3 | Por lo tanto $x^{n+5} \not\equiv 15 \pmod{41}$. |
| 4 | No se puede cumplir la contradicción. |

Ejemplos de la clase pasada:

① Hallar $x \mid x^3 \equiv 15 \pmod{41}$

Encontramos $x \equiv 7 \pmod{41}$ es solución pues $7^3 \equiv 15 \pmod{41}$

② Probamos que no existe $x \mid x^5 \equiv 15 \pmod{41}$

③ Hallar alguna solución x o probar que no existe solución de $x^{11} \equiv 15 \pmod{41}$

Probamos $x \equiv 7 \pmod{41}$ no cumple

Continuación del ejemplo 3.

Supongamos que hallo $y \pmod{41} \mid y^{11 \cdot h} \equiv 15 \pmod{41}$ para algún $h \in \mathbb{Z}$.

Tomo $x = y^h \pmod{41}$ que cumple $x^{11} \equiv 15 \pmod{41}$

$$7^3 \equiv 15 \pmod{41} \quad (e7)$$

$$7^{k \cdot 40} \equiv 1^k \equiv 1 \pmod{41} \quad \forall k \in \mathbb{Z} \quad (\text{Euler-Fermat})$$

$$7^{\frac{11h}{3+k \cdot 40}} \equiv 15 \pmod{41} \quad \forall k \in \mathbb{Z} \quad \Rightarrow 7^{11h} \equiv 15 \pmod{41} \quad \Rightarrow (7^h)^{11} \equiv 15 \pmod{41}$$

$$\Rightarrow x \equiv 7^h \pmod{41} \quad \text{verifica la ecuación} \quad x^{11} \equiv 15 \pmod{41}$$

Objetivo: Encontrar $h, k \in \mathbb{Z} \mid 3 + 40k = 11h$ y calcular como solución $x = 7^h$

$$3 + 40k = 11h \quad \text{con } k, h \in \mathbb{Z} \quad \Leftrightarrow 3 + k \cdot 40 \equiv 0 \pmod{11} \Leftrightarrow 3 + k \cdot 7 \equiv 0 \pmod{11}$$

$$\Leftrightarrow 7k \equiv -3 \pmod{11} \Leftrightarrow -4k \equiv -3 \pmod{11} \Leftrightarrow 4k \equiv 3 \pmod{11} \Rightarrow k = -2$$

$$3 + 40(-2) = 11h \Rightarrow 3 - 80 = 11h \Rightarrow h = -7$$

Por lo tanto, una solución de $x^7 \equiv 15 \pmod{41}$ es $x \equiv 7^{-1} \pmod{41}$

$$x \equiv (7^{-1})^7 \pmod{41}$$

hallemos $7^{-1} \pmod{41}$

$$\begin{matrix} 7^{-1} \\ 6 \end{matrix} \cdot 7 \equiv 1 \pmod{41}$$

$$\Rightarrow x \equiv 6^7 \pmod{41} \text{ es la solución}$$

Mirando $\langle 2 \rangle$ y $\langle 3 \rangle$ hallados la clase pusada: $2^7 \equiv 5 \pmod{41}$

$$3^7 \equiv 14 \pmod{41}$$

$$6^7 = (2 \cdot 3)^7 = 2^7 \cdot 3^7 \equiv 5 \cdot 14 = 70 \equiv -12 \equiv 29 \pmod{41}$$

$$x \equiv 29 \pmod{41}$$

Encriptado en bloques

$$\begin{array}{ccccccc} A & B & C & \dots & Z & - \\ \downarrow & \downarrow & \downarrow & & \downarrow & \downarrow \\ 0 & 1 & 2 & & 26 & 27 \end{array} \quad n = 28$$

Bloques de 4. Hay 28^4 bloques distintos.

$$\overbrace{x_{B_1} \quad x_{B_2} \quad x_{B_3} \quad x_{B_4}}^{\text{Terminan las clases}} \quad x_{B_5}$$

$$\begin{array}{c} \downarrow \downarrow \downarrow \downarrow \\ x_1 \ x_2 \ x_3 \ x_4 \\ \{ \\ x_i \pmod{28} \end{array}$$

$$\boxed{x_1 \ x_2 \ x_3 \ x_4}$$

$$0 \leq x_i < 27$$

$$\left. \begin{array}{c} | \\ 0 \leq x_i < 27 \end{array} \right\}$$

$$0 \leq x_{B_1} < 28^4 - 1$$

$$x_{B_1} = x_1 + 28x_2 + 28^2x_3 + 28^3x_4$$

$$Y_{B_i} = E(x_{B_i}) \pmod{28^4 - 1}$$

$$x_{B_i} = D(Y_{B_i}) \pmod{28^4 - 1}$$

Voy dividiendo entre 28

$$x = x_1 + 28(x_2 + 28x_3 + 28^2x_4)$$