USOS DE LA CONGRUENCIA

① CALCULAR EL RESTO DE LA DIVISIÓN DE 914 POR 31 SIN LA DIVISIÓN.

- QUEREMOS HALLAR $r \mid r < 31$ ES DECIR $914 \pmod{31}$
- $31 = 30 + 1 \Rightarrow 30 \equiv -1 \ (31)$ $[30 - (-1) = 31]$

EJEMPLO: $52x \equiv 8 \ (88)$

① VERIFICAR QUE TENGA SOLUCIÓN.

TIENE SOLUCIÓN SI EL $MCD(52, 88) \mid 8$

② SACAR EL MCM

$MCD(52, 88) = 4$

$88 = 52 \cdot 1 + 36$
$52 = 36 \cdot 1 + 16$
$36 = 16 \cdot 2 + \boxed{4}$
$16 = 4 \cdot 4 + 0$

COMO $4 \mid 8$ YA QUE: $8 = 4 \cdot 2$ TIENE SOLUCION LA ECUACIÓN.

②.1 SI EL MCD ES DIFERENTE DE 1 DIVIDIR TODO POR EL MCD

$52x \equiv 8 \ (88)$

$\boxed{13x \equiv 2 \ (22)}$

②.2 SACAR EL MCD ENTRE 13 Y 44 (**) Y VER SI TIENE SOL. $MCD(13, 22) = 1$ ✓

③ ENCONTRAR UNA SOLUCIÓN PARTICULAR x_0

(**) ④ HACER COMBINACIÓN LINEAL DEL MCD (casi siempre es 1)

$22 = 13 \cdot 1 + 9$
$13 = 9 \cdot 1 + 4$
$9 = 4 \cdot 2 + \boxed{1}$
$4 = 1 \cdot 4 + 0$

$1 = 9 - 4 \cdot 2$
$1 = 9 - (13 - 9) \cdot 2$
$1 = 9 - 2 \cdot 13 + 2 \cdot 9$
$1 = 3(22 - 13) - 2 \cdot 13$
$1 = 3 \cdot 22 - 3 \cdot 13 - 2 \cdot 13$
$\boxed{1 = 3 \cdot 22 - 5 \cdot 13}$

⑤ ESCRIBIR LA COMBINACIÓN LINEAL

$1 \equiv (-5) \cdot 13 + 3 \cdot 22 \ (22)$
$1 \equiv (-5) \cdot 13 \ (22) \equiv 0 \ (22)$

⑥ REESCRIBIR PARA QUE SE VEA PARECIDO A LA ECUACIÓN Y OBTENER EL x_0

$2 \equiv (-10) \cdot 13 \ (22)$
$(-10) \cdot 13 \equiv 2 \ (22)$

⑥ ESCRIBIR TODAS LAS SOLUCIONES

$x = x_0 + \frac{mod}{MCD(a,b)} \cdot K$

$x = -10 + 22K$

⑦ Darle valores a K para ir obteniendo los resultados que se encuentran dentro del rango que te dan.

ECUACIONES CON CONGRUENCIA

① → $aX \equiv b\,(m)$ TIENE SOLUCIÓN $\leftrightarrow$ $MCD(m,a) \mid b$

② → LAS SOLUCIONES SON: $\frac{a}{\delta} x_0 \equiv \frac{b}{\delta}\left(\frac{m}{\delta}\right)$

$$X \equiv \left[x_0 + \frac{m}{\delta} k\right]\,(m)$$

EJEMPLO

$$12X \equiv 20\,(28)$$

① $MCD(28,12) = 4$

$28 = 12 \cdot 2 + 4$

$12 = 4 \cdot 3 + 0$

② $4 \mid 20$ ✓ $\quad 4 \cdot 5 = 20$

VA A TENER SOLUCIONES.

③ SIMPLIFICO TODO POR EL MD

$$\frac{12X}{4} \equiv \frac{20}{4}\ \frac{(28)}{4}$$

$$3X \equiv 5\,(7)$$

$MCD(7,3) = 1 \Rightarrow 1 \mid 5$ ✓

DEMOSTRAR QUE $\sqrt{6}$ ES IRRACIONAL

SUPONEMOS QUE $\sqrt{6}$ ES RACIONAL:

$\sqrt{6} = \frac{a}{b}$ $\quad (a,b) = 1$ (IRREDUCIBLE, NO SE PUEDE SIMPLIFICAR)

$6 = \frac{a^2}{b^2} \rightarrow 6 \cdot b^2 = a^2 \rightarrow$ a^2 ES MULTIPLO DE 6

$a^2 = (6a)^2$

$6b^2 = (6a)^2 \rightarrow 6 \cdot b^2 = 6^2 \cdot a^2 \rightarrow b^2 = 6 \cdot a^2$

b^2 ES MULTIPLO DE 6 ABS NO SE CUMPLE $(a,b) = 1$

DEMOSTRACIÓN IRRACIONALIDAD DE $\sqrt{p}$ p-p PRIMO.

$\sqrt{p} = \frac{a}{b}$ $\quad (p \text{ PRIMO} > 1)$ $\quad a, b \in \mathbb{Z}$, $(a,b) = 1$

$a^2 = p \cdot b^2$

NÚMEROS PRIMOS

NÚMERO ENTERO POSITIVO 'P' SE DICE PRIMO SI:

- $P \geq 2$ (EL 1 NO ES PRIMO)
- LOS UNICOS DIVISORES ENTEROS POSITIVOS SON:
  - 1
  - P

2, 3, 5, 7, 11, 13, 17, 19.

- NO ES PRIMO SI SE PUEDE ESCRIBIR COMO PRODUCTO DE DOS NÚMEROS CUANDO ALGUNOS DE ELLOS NO ES P Ó 1.
- NO SE DESCOMPONEN

TEOREMA
TODO ENTERO $m \geq 2$ ES PRODUCTO DE PRIMOS.

- $P \nmid a$ $MCD(P, a) = 1$
- P y q PRIMOS y $P|q \Rightarrow P = q$

SEA P, NÚM. PRIMO:

* $P|xy \Rightarrow P|x$ Ó $P|y$
* $P|x_1 \dots x_i \Rightarrow P|x_j$
  $x_1 \leq x_j \leq x_i$

HAY INFINITOS PRIMOS

VER SI UN NUM ES PRIMO

FORMA 1 → CHEQUEAR LOS PRIMOS MENORES Q' LA RAIZ.

EJ. $31 \Rightarrow \sqrt{31} < \sqrt{36} = 6$ HASTA EL NÚMERO 5.

$2 \nmid 31$, $3 \nmid 31$, $4 \nmid 31$, $5 \nmid 31$

COMO NINGUNO DIVIDE A 31, 31 ES PRIMO.

TEOREMA FUNDAMENTAL DE LA ARITMETICA

LA FACTORIZACIÓN PRIMA DE UN NÚMERO ENTERO + ≥ 2 ES ÚNICA (SALVO EN EL REORDENAMIENTO)

$24 = 12 \cdot 2$
$24 = 6 \cdot 2 \cdot 2$
$24 = 3 \cdot 2 \cdot 2 \cdot 2$
$24 = 3 \cdot 2^3$

$24 = 4 \cdot 6$
$24 = 2 \cdot 2 \cdot 6$
$24 = 2 \cdot 2 \cdot 3 \cdot 2$
$24 = 2^3 \cdot 3$

PROPOSICIÓN

$m, m \geq 2$ CON → $m = p_1^{d_i} \dots p_r^{d_r}$, $m = p_1^{l_i} \dots p_r^{l_r}$

$m \mid m \iff d_i \leq l_i$

$m = 2 \cdot 3^3 \cdot 5 \cdot 7^3$
$m = 2 \cdot 3^2 \cdot 7^2$ → DIVIDE
$m' = 2 \cdot 3^3 \cdot 7$ (NO DIVIDE)

30870 | 315 | 578 ∤ 30870

COROLARIO

SEA P PRIMO, $P|m$ SI P APARECE EN LA FACTORIZACIÓN PRIMA DE m

EJ: $13 \mid 52$
$52 = 13 \cdot 2^2$

X	PAR	IMPAR
PAR	PAR	PAR
IMPAR	PAR	IMPAR

CONGRUENCIA

$a \equiv b \mod(m)$ ó $a \equiv b\ (m)$

a y $b \in \mathbb{Z}$ y $m \in \mathbb{N}$

$7 \equiv 3 \mod(2)$ pues $2 \mid 7-3$, $2 \mid 4$

$17 \equiv 8\ (3)$ pues $3 \mid 17-8$, $3 \mid 9$

a es congruente b módulo m si:

$m \mid a-b$ ó $a-b$ es divisible por m

PROPIEDADES BÁSICAS

- $a \equiv 0\ (m) \iff m \mid a$
- $a \equiv b\ (m) \iff b \equiv a\ (m)$ — $m \mid b-a$
- $a \equiv r\ (m)$ r = resto
- $a \equiv b\ (m) \iff$ Tienen el mismo resto al dividir por m

CUMPLE LA RST

RELACIÓN DE EQUIVALENCIA:

- REFLEXIVA $a \equiv a\ (m)$
- SIMETRICA $a \equiv b\ (m) \iff b \equiv a\ (m)$
- TRANSITIVA $a \equiv b\ (m)$ y $b \equiv c$ $\Rightarrow a \equiv c\ (m)$

TEOREMAS

- $p \mid \binom{p}{r}$ $0 < r < p$ (p, Primo)
- $(a+b)^p \equiv a^p + b^p \pmod p$

TEOREMA PEQUEÑO DE FERMAT

... p, primo y $A \in \mathbb{Z}$

- $a^p \equiv a \pmod p$
- Si $(p, a) = 1$, el MCD $= 1$, coprimos

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

COCIENTE Y RESTO

ALGORITMO DE LA DIVISIÓN:

$a = bq + r, \quad 0 \leq r < b$ — $q \rightarrow$ COCIENTE DE b POR a

$10 = 3 \cdot 3 + 1 \mid -5 = 2(-3) + 1$ — $r \rightarrow$ RESTO DE DIVIDIR b POR a

DESARROLLO EN BASE b ($b \geq 2$)

TAL COMO ESCRIBIMOS LOS NUMS. ESTÁN EN BASE 10.

$543 = 5 \cdot 100 + 4 \cdot 10 + 3 \cdot 1 = 5 \cdot 10^2 + 4 \cdot 10^1 + 3 \cdot 10^0$

• CONV. BASE 10 A OTRA BASE.

HACER ALGORITMO DE LA DIVISIÓN PERO CON b = BASE

569 → BASE 4

$569 = 4 \cdot 142 + 1$
$142 = 4 \cdot 35 + 2$
$35 = 4 \cdot 8 + 3$
$8 = 4 \cdot 2 + 0$
$2 = 4 \cdot 0 + 2$

• LLEGAR A LA BASE $\neq 0$

• LOS RESTOS ES EL NUM.

$569 = (20321)_4$

CONV. DE BASE m A BASE 10.

MÉTODO DE DESCOMPOS. POLINÓMICA

PONER LA PRIMERA CIFRA A BASE ELEVADA A LA POTENCIA QUE LE CORRESPONDA. DESPUÉS RESOLVER Y SUMAR.

$(1011)_3 \rightarrow$ BASE 10

$(1011)_3 = 1*3^3 + 0*3^2 + 1*3^1 + 1*3^0$

$(1011)_3 = 27 + 0 + 3 + 1 = \boxed{31}$

CONVERTIR DE BASE m A BASE m

$(2534)_7 \rightarrow$ BASE 4

$2 \cdot 7^3 + 5\,7^2 + 37 + 4 =$
$2 \cdot 343 + 5 \cdot 49 + 21 + 4 =$
$686 + 245 + 25 = \boxed{956}$

$(2534)_7 = (32330)_4$

PASAR A BASE 10 Y DESPUÉS DE 10 A LA OTRA

$956 = 4 \cdot 239 + 0$
$239 = 4 \cdot 59 + 3$
$59 = 4 \cdot 14 + 3$
$14 = 4 \cdot 3 + 2$
$3 = 4 \cdot 0 + 3$

SÍMBOLOS PARA BASE 16

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

PARES → DIVISIBLES POR 2

IMPARES → NO DIVISIBLES POR 2

OBSERVACIONES BÁSICAS

• $1 \mid A$ • $A \mid 0$ • $A \mid \pm A$ • $A \mid b$ y $b \mid c \Rightarrow a \mid c$ • $m \neq 0, a \mid b \leftrightarrow ma \mid mb$

• $A \mid B \Rightarrow A \mid BC$ • $A \mid B$ y $A \mid C \Rightarrow A \mid (B+C)$ • $a \mid b$ y $b \mid a \Rightarrow a = \pm b$

• $A \mid B$ y $A \mid C \Rightarrow rb + sc$

$a \mid b = b \overset{r}{\mid} a \overset{q}{\Rightarrow} b = aq$

• b es divisible por a
• a divide a b
• b es multiplo de a
• a es divisor de b

Ej: 216 → $6 = 2 \cdot 3$

MÁXIMO COMÚN DIVISOR

UN ENTERO NO NEGATIVO "D" ES MCD DE A Y B SI:

- $d|a$ y $d|b$ → Es un divisor de ambos
- $c|a$ y $c|b \Rightarrow c|d$ → Es el más grande

COMBINACIÓN LINEAL

$d = ra + sb$

ALGORITMO DE EUCLIDES

1. a, b
2. APLICAR ALGORITMO DIVISIÓN
   $a = b \cdot q + r$
3. SEGUIR
   $b = rq + r$
   $r = rq + r$
4. SI OBTENGO QUE EL RESTO IGUAL A 0:
   - ESE RESTO ES EL MCD

$d|a$ y $d|b \Rightarrow$

- $d|$ cualquier COMB. LINEAL
- $d|a+b$
- $d|B-A$
- $d|ab$
- $d|A-B$

EJEMPLO → MCD(72,174)

$174 = 72 \cdot 2 + 30$
$72 = 30 \cdot 2 + 12$
$30 = 12 \cdot 2 + 6$
$12 = 6 \cdot 2 + 0$

$MCD(72,174) = 6$

OBTENER EL MCD

OBTENER COMB LINEAL

$6 = 30 - 12 \cdot 2$
$6 = 30 - 2(72 - 30 \cdot 2)$
--DISTRIBUTIVA----
$6 = 30 - 2 \cdot 72 + 30 \cdot 2 \cdot 2$
---JUNTAR LOS 30---
$6 = 5(30) - 2 \cdot 72$
$6 = 5(174 - 72 \cdot 2) \cdot 2 \cdot 72$
$6 = 5 \cdot 174 - 10 \cdot 72 - 2 \cdot 72$
$\boxed{6 = 5 \cdot 174 - 12 \cdot 72}$

OBTENER EL MÁXIMO COMÚN DIVISOR

(OTRA FORMA PIOLA)

EL PRODUCTO DE LOS PRIMOS COMUNES AL MÍNIMO EXPONENTE.

Ej MCD $(2 \cdot 3^2 \cdot 5^3 \cdot 7, 2^3 \cdot 3 \cdot 5 \cdot 11)$

$6 = 2 \cdot 3 \cdot 5 \cdot 7^0 \cdot 11^0$

OBTENER EL MÍNIMO COMÚN MÚLTIPLO

PRODUCTO DE LOS PRIMOS COMUNES AL MAX. EXPONE

Ej: MCM $(2 \cdot 3^2 \cdot 5^3 \cdot 7, 2^3 \cdot 3 \cdot 5 \cdot 11)$

$M = 2^3 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$

SIRVE PARA DEMOSTRAR QUE DOS COSAS SON DIFE...

MÍNIMO COMÚN MÚLTIPLO

UN ENTERO NO NEGATIVO m ES EL MCM DE A Y B, SI:

- $A|m$, $B|m$ → Es múltiplo de ambos
- $A|C$ y $B|C \Rightarrow$ M|C (múltiplo más chico)

$$MCM(a,b) = \frac{|a \cdot b|}{MCD(a,b)}$$

EL MCM ES SIEMPRE POSITIVO LO Q' NO IMPORTA SI a, b SON + Ó -

EJEMPLO → MCM(8,14)

$$MCM = \frac{|8 \cdot 14|}{2} = \frac{112}{2} = \boxed{56}$$

$MCD(8,14) = 2$

$14 = 8 \cdot 1 + 6$
$8 = 6 \cdot 1 + 2$
$6 = 2 \cdot 3 + 0$