Comentarios

Büten Zar

FB

Letra

Ejercicio 1

Ejercicio 2

Ejercicio 3

Ejercicio 4

Ejercicio 5

Ejercicio 6

Ejercicio 7

Ejercicio 8

Ejercicio 9

Ejercicio 10

Ejercicio 11

Ejercicio 12

Ejercicio 1

Menu

a)

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

Demostración:

$$\text{por def:} \quad \left.\begin{array}{l} n \mid b-a \\ n \mid d-c \end{array}\right\} \Rightarrow n \mid b-a+d-c \Rightarrow n \mid b+d-(a+c) \Rightarrow a+c \equiv b+d \pmod{n}$$

$$\text{por def:} \quad \left.\begin{array}{l} n \mid b-a \Rightarrow n \mid bd-ad \\ n \mid d-c \Rightarrow n \mid da-ca \end{array}\right\} \Rightarrow n \mid bd-ca \Rightarrow ac \equiv bd \pmod{n}$$

b)

$$\left.\begin{array}{l} b \equiv c \pmod{n} \\ a \in \mathbb{Z} \end{array}\right\} \Rightarrow a+b \equiv a+c \pmod{n}$$

Demostración:

$$\left.\begin{array}{l} a \equiv a \pmod{n} \Rightarrow n \mid a-a \\ \text{reflexiva} \qquad Ⓗ \rightarrow n \mid c-b \end{array}\right\} n \mid c+a-(b+a) \Rightarrow a+b \equiv a+c \pmod{n}$$

c)

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

Demostración:

$$\left.\begin{array}{l} n \mid b-a \\ m \mid n \end{array}\right\} \xRightarrow{\text{transitiva}} m \mid b-a \Rightarrow a \equiv b \pmod{m}$$

d)

$$\boxed{\left.\begin{array}{l} a \equiv b \pmod{m} \\ n \in \mathbb{Z} \end{array}\right\} \Rightarrow na \equiv nb \pmod{m}}$$

Demostración :

por def :

$$m \mid b-a \Rightarrow m \mid (b-a)n \Rightarrow m \mid bn-an \Rightarrow an \equiv bn \pmod{m}$$

¿ Vale el recíproco ?

Solo vale si $\mathrm{MCD}(n,m)=1$

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

e)

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

Demostración:

por def :

$$m \mid b-a \Rightarrow m \mid (b-a)\left(\sum_{i=0}^{n-1} a^i b^{n-i}\right) \Rightarrow m \mid b^n - a^n \Rightarrow a^n \equiv b^n \pmod{m}$$

f)

$$\boxed{\left.\begin{array}{l} ac \equiv bc \pmod{m} \\ d = \mathrm{MCD}(c,m) \end{array}\right\} \Rightarrow a \equiv b \left(\bmod \frac{c}{d}\right)}$$

Demostración :

$$\begin{array}{l} c = d.c' \\ m = d.m' \end{array} \qquad \mathrm{MCD}(c',m')=1$$

$$ca \equiv cb \pmod{m} \Leftrightarrow d.c'.a \equiv d.c'.b \bmod (m'd) \Leftrightarrow m'd \mid (c'b-c'a)d$$

$$\Rightarrow m' \mid c'b - c'a \Leftrightarrow \left.\begin{array}{l} c'a \equiv c'b \pmod{m'} \\ \mathrm{MCD}(m',c')=1 \end{array}\right\} \xRightarrow{\text{prop ⓓ}} \left.\begin{array}{l} a \equiv b \pmod{m'} \\ m' = \frac{m}{d} \end{array}\right\} \Rightarrow a \equiv b \left(\bmod \frac{m}{d}\right)$$

Ejercicio 2

Menu

$$\begin{array}{l|l} a & n \\ \cline{2-2} r & \end{array} \Rightarrow a \equiv r \pmod{n}$$

① $\boxed{a \equiv 22 \pmod{14}}$

$$\boxed{\begin{array}{l|l} a & 2 \\ \cline{2-2} r_1 & \end{array} \Rightarrow a \equiv r_1 \pmod{2}}$$

por def: $14 \mid 22 - a \Rightarrow 14 \mid 22 \cdot 7 - 7a$

$$\Rightarrow \left.\begin{array}{l} 2 \mid 22 - a \\ 2 \mid r_1 - a \end{array}\right\} \Rightarrow \left.\begin{array}{l} 2 \mid 22 - r_1 \\ r_1 < 2 \end{array}\right\} \Rightarrow \boxed{r_1 = 0}$$

$$\boxed{\begin{array}{l|l} a & 7 \\ \cline{2-2} r_2 & \end{array} \Rightarrow a \equiv r_2 \pmod{7}}$$

por def: $\left.\begin{array}{l} 14 \mid 22 - a \\ 7 \mid 14 \end{array}\right\} \Rightarrow 7 \mid 22 - a$

$$\left.\begin{array}{l} 7 \mid r_2 - a \\ 7 \mid 22 - a \end{array}\right\} \Rightarrow \left.\begin{array}{l} 7 \mid 22 - r_2 \\ r_2 < 7 \end{array}\right\} \boxed{r_2 = 1}$$

$$\boxed{\begin{array}{l|l} a & 14 \\ \cline{2-2} r_3 & \end{array} \Rightarrow a \equiv r_3 \pmod{14}}$$

por def $\left.\begin{array}{l} 14 \mid 22 - a \\ 14 \mid r_3 - a \end{array}\right\} \left.\begin{array}{l} 14 \mid 22 - r_3 \\ r_3 < 14 \end{array}\right\} \Rightarrow \boxed{r_3 = 8}$

ⓑ $\boxed{a \equiv 13 \pmod{5}}$

$$\boxed{\begin{array}{l|l} 33a^3 + 3a^2 - 197a + 2 & 5 \\ \cline{2-2} r & \end{array} \Rightarrow 33a^3 + 3a^2 - 197a + 2 \equiv r \operatorname{mod}(5)}$$

por def: $5 \mid 13 - a \Rightarrow \left.\begin{array}{l} 5 \mid 13 . (-33a^2) + 33a^3 \\ 5 \mid r - 33a^3 - 3a^2 + 197a - 2 \end{array}\right\} 5 \mid r - 432a^2 + 197a - 2$

$$5 \mid 13 - a \Rightarrow \left.\begin{array}{l} 5 \mid 13(-432a) + 432a^2 \\ 5 \mid r - 432a^2 + 197a - 2 \end{array}\right\} 5 \mid r - 5419a - 2$$

$$5 \mid 13 - a \Rightarrow \left.\begin{array}{l} 5 \mid 13(-5419) + 5419a \\ 5 \mid r - 5419a - 2 \end{array}\right\} \left.\begin{array}{l} 5 \mid r - 70449 \\ r < 5 \end{array}\right\} \Rightarrow \boxed{r = 4}$$

ⓒ Hallar, para cada $n \in \mathbb{N}$, el resto de la división de $\sum_{i=1}^{n} (-1)^i . i!$ por 36

$$\sum_{i=1}^{n} (-1)^i . i! \equiv r \mod 36 \qquad \boxed{0 \leq r < 36}$$

para n = 1

$$(-1) \equiv r \mod 36 \qquad 36 \mid r + 1 \qquad \boxed{r = 35}$$

para n = 2

$$\sum_{i=1}^{2} (-1)^i . i! = -1 + 2 = 1 \equiv r \,(\mathrm{mod}\ 36) \Rightarrow 36 \mid r - 1 \qquad \boxed{r = 1}$$

para n = 3

$$\sum_{i=1}^{3} (-1)^i . i! = (-1) + 2 - 6 = -5 \equiv r \,(\mathrm{mod}\ 36) \Rightarrow 36 \mid r + 5 \qquad \boxed{r = 31}$$

para n = 4

$$\sum_{i=1}^{4} (-1)^i . i! = (-1) + 2 - 6 + 24 = 29 \equiv r \,(\mathrm{mod}\ 36) \Rightarrow 36 \mid r - 19 \qquad \boxed{r = 19}$$

para n = 5

$$\sum_{i=1}^{5} (-1)^i . i! = (-1) + 2 - 6 + 24 - 120 = -101 \equiv r \,(\mathrm{mod}\ 36) \Rightarrow 36 \mid r + 101 \qquad \boxed{r = 7}$$

para n = 6

$$\sum_{i=1}^{6} (-1)^i . i! = (-1) + 2 - 6 + 24 - 120 + 6! = -101 + 6! \equiv -101 \equiv r \,(\mathrm{mod}\ 36) \qquad \boxed{r = 7}$$

$$\underbrace{6 . 5 . 4 . \underbrace{3 . 2}}_{36} \equiv 0 \mod 36$$

para n = n

$$\sum_{i=1}^{5} (-1)^i . i! + \underbrace{\sum_{i=6}^{n} (-1)^i . i!}_{\equiv 0 \mod \dot{36}} \equiv \sum_{i=1}^{5} (-1)^i . i! \equiv r \,(\mathrm{mod}\ 36)$$

$$\boxed{r = 7}$$

para $n \geq 5$ $\boxed{r = 7}$

Ejercicio 3

Menu

Probar que si a y b son enteros y p un número primo entonces:

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

Demostración:

$$(a+b)^p = \sum_{0\le J\le p} C_J^p\, a^{p-J}\, b^J$$

binómio
Newton

$$\xrightarrow{def} \quad p \mid (a+b)^p - a^p - b^p \iff p \mid \sum_{1\le J\le p-1} C_J^p\, a^{p-J}\, b^J$$

Vamos a probar que $p \mid \sum_{i\le J\le p-1} C_J^p$

$$C_J^p = \frac{p(p-1)\dots 1}{(p-J)!\; J!} = \frac{p\cdot(p-1)(p-2)\dots 1}{(p-J)(p-J-1)\dots J(J-1)\dots 2}$$

$1\le J\le p-1$

Como p es primo, no tiene divisores menores que el salvo el 1.

$C_J^p \in \mathbb{Z}$

todos los factores del denomina
son menores que p

$$\Longrightarrow p \mid \sum_{i\le J\le p-1} C_J^p \Rightarrow p \mid \sum_{1\le J\le p-1} C_J^p\, a^{p-J}\, b^J \Rightarrow p \mid (a+b)^p - a^p - b^p$$

$$\overset{def}{\iff} (a+b)^p \equiv a^p + b^p \pmod{p}$$

¿Vale el resultado si p no es primo?

p = 4

$$4 \mid (a+b)^4 - a^4 - b^4 \iff 4 \mid \sum_{i\le J\le 3} C_J^4\, a^{4-J}\, b^J$$

$$C_1^4 = \frac{4.3.2.1}{3.2.1.1} = 4 \checkmark$$

$$C_2^4 = \frac{4.3.2.1}{2.1.2} = 6 \times$$

$\Rightarrow p \nmid C_J^p \Rightarrow$ no vale el recíproco.

Ejercicio 4 (Lo odio)

a) Hallar todos los $a \in \mathbb{Z} \;/\; a^3 \equiv 3 \pmod{11}$

$a \equiv r \pmod{11}$ o sea $a \equiv 0, 1, 2, \ldots, 10 \pmod{11}$

$\boxed{(\text{mod } 11)}$

$a \equiv$	$a^2 \equiv$	$a^3 \equiv$
0	0	0
1	1	1
2	4	8
3	$9 \equiv 2$	$2 \cdot 3 = 6$
4	$16 \equiv 5$	$5 \cdot 4 = 20 \equiv 9$
5	$25 \equiv 3$	$3 \cdot 5 = 15 \equiv 4$
6	$36 \equiv 3$	$3 \cdot 6 = 18 \equiv 7$
7	$49 \equiv 5$	$7 \cdot 5 = 35 \equiv 2$
8	$64 \equiv 9$	$9 \cdot 8 = 72 \equiv 6$
9	$81 \equiv 4$	$\boxed{9 \cdot 4 = 36 \equiv 3}$
10	$100 \equiv 1$	10

b) Probar que no existe ningun entero $a \;/\; a^3 \equiv -3 \pmod{13}$ o sea $a^3 \equiv 10 \pmod{13}$

$a \equiv r \pmod{13}$ o sea $a \equiv 0, 1, \ldots 12 \pmod{13}$

$\boxed{\text{mod } 13}$

$a \equiv$	$a^2 \equiv$	$a^3 \equiv$
0	0	0
1	1	1
2	4	8
3	$9 \equiv -4$	$-12 \equiv 1$
4	$16 \equiv 3$	$12 \equiv -1$
5	$25 \equiv 12 \equiv -1$	-5
6	$36 \equiv 10 \equiv -3$	$-18 \equiv -5$
7	$49 \equiv 10 \equiv -3$	$-21 \equiv -8 \equiv 5$
8	$64 \equiv 12 \equiv -1$	$-8 \equiv 5$
9	$81 \equiv 3$	$27 \equiv 1$
10	$100 \equiv 9 \equiv -4$	$-40 \equiv -1$
11	$121 \equiv 4$	$44 \equiv 5$
12	$144 \equiv 1$	12

queda demostrado que no hay ningun entero $a \;/\; a^3 \equiv -3 \pmod{13}$

c) Probar que $a^2 \equiv -1 \pmod 5 \iff a \equiv 2 \pmod 5$ ó $a \equiv 3 \pmod 5$

$a \equiv r \pmod 5$ o sea $a \equiv 0,1,2,3,4 \pmod 5$

(mod 5)

$a \equiv$	$a^2 \equiv$
0	0
1	1
2	$4 \equiv -1$
3	$9 \equiv 4 \equiv -1$
4	$16 \equiv 1$

Para verlo mejor:

$a \equiv 2 \pmod 5$

$a^2 = a \cdot a \equiv 2 \cdot 2 \pmod 5 \equiv -1 \pmod 5$

d) Probar que $a^7 \equiv a \pmod 7 \quad \forall a \in \mathbb{Z}$

$a \equiv r \pmod 7$ o sea $a \equiv 0, 1, \dots 6 \pmod 7$

Mod 7

$a \equiv$	$a^2 \equiv$	$a^3 \equiv$	$a^4 \equiv$	$a^7 \equiv$
0	0	0	0	$\boxed{0}$
1	1	1	1	$\boxed{1}$
2	4	$8 \equiv 1$	$16 \equiv 2$	$\boxed{2}$
3	$9 \equiv 2$	$6 \equiv -1$	4	$-4 \equiv \boxed{3}$
4	$16 \equiv 2$	$8 \equiv 1$	4	$\boxed{4}$
5	$25 \equiv 4$	$20 \equiv -1$	$16 \equiv 2$	$-2 \equiv \boxed{5}$
6	$36 \equiv 1$	$6 \equiv -1$	1	$-1 \equiv \boxed{6}$

Ejercicio 5

Menu

$$\boxed{x^2 - 1 \equiv 0 \pmod{35}}$$

$$\begin{tikzcd}
x^2 - 1 = (x+1)(x-1) \equiv 0 \pmod{35} \arrow[r, "\text{prop ⓒ}"] \arrow[dr] & (x+1)(x-1) \equiv 0 \pmod 7 \\
 & (x+1)(x-1) \equiv 0 \pmod 5
\end{tikzcd}$$

	$x-1 \equiv 0 \pmod 5$	$x+1 \equiv 0 \pmod 5$
$x-1 \equiv 0 \pmod 7$	$\boxed{36}$	$\boxed{29}$
$x+1 \equiv 0 \pmod 7$	$\boxed{6}$	$\boxed{34}$

$$\left.\begin{cases} x-1 \equiv 0 \pmod 5 & \rightarrow 5 \mid x-1 \\ x-1 \equiv 0 \pmod 7 & \rightarrow 7 \mid x-1 \end{cases}\right\} \Rightarrow 35 \mid x-1 \Rightarrow x = 36$$

$$MCD(7,5) = 1$$

$$\left.\begin{cases} x+1 \equiv 0 \pmod 5 \rightarrow 5 \mid x+1 & \rightarrow 35 \mid 7x+7 \\ x-1 \equiv 0 \pmod 7 \rightarrow 7 \mid x-1 & \rightarrow 35 \mid 5x-5 \end{cases}\right\} \Rightarrow 35 \mid 2x+12 \rightarrow x = 29$$

Análogo para los demás.

Ejercicio 6

Menu

a) Demostrar que $10^n \equiv (-1)^n \pmod{11}$

$$10 \equiv -1 \mod 11 \iff 11 \mid -1-10 \checkmark$$

$$\xRightarrow[\text{prop}]{} 10^n \equiv (-1)^n \pmod{11}$$

b) Enunciar y probar un criterio de divisibilidad entre 11.

Enunciado: Si la suma de los dígitos que ocupan un lugar par, menos la suma de los dígitos que ocupan lugar impar es $\dot{11}$, entonces el número es $\dot{11}$.

Vamos a probar: $\overset{\text{considero}}{(k \text{ es par})}$ $\quad a = a_k \ldots a_1 a_0$

$$a \equiv (a_0 + a_2 + \ldots + a_k) - (a_1 + a_3 + \ldots + a_{k-1}) \mod 11$$

Demostración:

$$a = 10^k a_k + \ldots + 10\, a_1 + a_0$$

$$\left.\begin{aligned} 10 &\equiv (-1) \mod 11 \\ a &\equiv a \mod 11 \end{aligned}\right\} \Longrightarrow a \equiv (-1)^k a_k + \ldots + (-1) a_1 + a_0 \mod 11$$

$$a \equiv (a_0 + \ldots + a_k) - (a_1 + \ldots a_{k-1}) \mod 11$$

c) Hallar el dígito d, de modo que $2d653874$ sea $\dot{11}$

$$a = 2d653874$$

$$a \equiv (4 + 8 + 5 + d) - (7 + 3 + 6 + 2) \mod 11$$

$$a \equiv d - 1 \mod 11 \quad \Rightarrow \boxed{d = 1}$$

Ejercicio 7

Menu

Demuestre que $4^n \equiv 4 \pmod{6}$ para todo entero $n \geq 1$

$$4 \equiv 2 \bmod 2 \implies \left.\begin{array}{l} 4^n \equiv 2^n \bmod 2 \\ 2^n \equiv 0 \bmod 2 \end{array}\right\} \implies \boxed{4^n \equiv 0 \bmod 2}$$

$$4 \equiv 1 \bmod 3 \implies 4^n \equiv 1^n \bmod 3 \implies \boxed{4^n \equiv 1 \bmod 3}$$

Considero el sistema

$$\begin{cases} x \equiv 0 \bmod 2 \\ x \equiv 1 \bmod 3 \end{cases}$$

por el teorema chino de los restos

$x = 4^n$ claramente es solución

$x = 4$ claramente es solución

$$x \equiv x' \bmod (m_1 . m_2)$$

$$\boxed{4^n \equiv 4 \bmod (2.3)}$$

Otra forma es por IC.

Ejercicio 8

ⓐ Probar que para todo $a \in \mathbb{Z}$ se cumple que:

$$a^2 \equiv 0 \pmod 4 \quad \text{ó} \quad a^2 \equiv 1 \pmod 4$$

r	r^2	
0	0	$\equiv 0 \mod 4$
1	1	$\equiv 1 \mod 4$
2	4	$\equiv 0 \mod 4$
3	9	$\equiv 1 \mod 4$

$$\begin{array}{l|l} a & 4 \\ \hline & k \\ r & \end{array}$$

$r = 0, 1, 2, 3$

$a \equiv r \pmod 4$

$$\boxed{\begin{array}{c} r^2 \equiv 0 \mod 4 \\ \text{o} \\ r^2 \equiv 1 \mod 4 \end{array}}$$

ⓑ Averiguar si $34567453560023456765434\underline{62}$ es un cuadrado perfecto

Llamemos n al número en cuestión

$n \equiv 62 \pmod 4$ por criterios de div entre 4

$62 \equiv x \pmod 4 \iff 4 \mid 62 - x \Rightarrow \boxed{x = 2} \Rightarrow n \equiv 2 \pmod 4$

$0 \leq x < 4$

por parte anterior todos los cuadrados perfectos son congruentes con 1 o con 0

$\Rightarrow$ n no es cuadrado perfecto.

ⓒ Probar que ningún número de la sucesión $a_1 = 11$ $a_2 = 111$ $a_3 = 1111$ $a_n = 11\ldots11$ es cuadrado perfecto.

<u>paso base</u>: $n = 1$ $a_1 = 11$ $11 \equiv 3 \pmod 4$ $\Rightarrow$ no es cuadrado perfecto

<u>Paso inductivo</u>:

Ⓗ $a_n = \underbrace{11\ldots11}_{n} \equiv 3 \pmod 4$ Ⓣ $a_{n+1} = \underbrace{11\ldots11\,1}_{n+1} \equiv 3 \pmod 4$

<u>Dem</u>: $a_{n+1} = a_n \cdot 10 + 1 \equiv 3 \cdot 10 + 1 \pmod 4 \Rightarrow a_{n+1} \equiv 31 \pmod 4 \Rightarrow a_{n+1} \equiv 3 \pmod 4$

$\Rightarrow$ ningún número de la sucesión es $\square$

Ejercicio 9

ⓐ $\boxed{3x \equiv 7 \pmod{16}}$

¿ MCD(3, 16) | 7 ? sí !

$y \in \mathbb{Z} \mid 3y \equiv 1 \mod 16 \iff 16 \mid 3y - 1$ $\boxed{y = 11}$

$3 \cdot 11 \cdot x \equiv 7 \cdot 11 \pmod{16} \implies \boxed{x \equiv 77 \pmod{16}}$

$x = 77 + 16k \quad \forall k \in \mathbb{Z}$

ⓑ $\boxed{2x + 8 \equiv 5 \pmod{33}}$

$2x + 8 - 8 \equiv 5 - 8 \pmod{33} \implies 2x \equiv -3 \pmod{33} \xRightarrow{-3 \equiv 30\ (33)} 2x \equiv 30 \pmod{33}$

$\left.\begin{array}{l} MCD(2,33) = 1 \\ 2x \equiv 30\ (33) \end{array}\right\} \implies \boxed{x \equiv 15 \pmod{33}}$

$x = 15 + 33k \quad \forall k \in \mathbb{Z}$

ⓒ $\boxed{3x + 9 \equiv 8x + 61 \pmod{64}}$

$3x \equiv 8x + 52 \pmod{64} \iff 64 \mid 3x - 8x - 52 \iff -5x \equiv 52 \mod (64)$

$\left.\begin{array}{l} y \in \mathbb{Z} \\ -5y \equiv 1 \pmod{64} \implies y = -13 \end{array}\right\}$ $\underbrace{-5 \cdot -13}_{\equiv 1\ (64)} x \equiv 52(-13) \mod (64)$

$\boxed{x \equiv 52(-13) \mod 64}$

$x = 52(-13) + 64k \quad \forall k \in \mathbb{Z}$

ⓓ $\boxed{6x - 1 \equiv 5 \pmod{12}}$

$$6x \equiv 6 \pmod{12} \implies \boxed{x \equiv 1 \pmod{2}}$$

todas las soluciones son $x = 1 + 2t \quad \forall t \in \mathbb{Z}$

ⓔ $\boxed{9x + 3 \equiv 5 \pmod{18}}$

$$9x \equiv 2 \pmod{18}$$

$MCD(9, 18) = 9$ ¿$9 | 2$? No! $\Rightarrow$ no hay solución

Menu

Ejercicio 10

ⓐ $\boxed{2 \text{ es invertible mod } n \iff n \text{ es impar}}$

$$2.e \equiv 1 \pmod{n} \overset{def}{\iff} n \mid \underbrace{2.e - 1}_{\text{es impar}} \implies \text{necesariamente } n \text{ tiene que ser impar.}$$

$$\text{Si } n = 2k+1 \implies \boxed{e = k+1}$$

ⓑ $\boxed{\text{Hallar } 71^{10} \bmod 141}$

$71^{10} \equiv b \mod 141$

$0 \leq b < 141$

usando parte anterior 2 es invertible módulo 141

$y \; e = 70 + 1 = 71$

$$\underbrace{2^{10} . 71^{10}}_{\downarrow} \equiv b . 2^{10} \mod 141$$

$$\implies 1 \equiv 2^{10} . b \mod 141 \iff 141 \mid 1024b - 1$$

$$141\,k = 1024b - 1$$

$$141\,k - 1024b = -1 \implies \boxed{1024b - 141\,k = 1}$$

Ec diofántica

cuidado con los signos el -443 en realidad es 443

paso 1 : $\text{MCD}(1024, 141) = 1 \quad y \quad 1 \mid 1 \quad \text{OK}$

paso 2 : $1 = x_0\, 1024 + y_0\, 141 \longrightarrow \boxed{x_0 = 61 \; , \; y_0 = -443}$ $\boxed{b = 61}$

$1024 = 141.7 + 37 \implies 37 = 1024 - 141.7$

$141 = 37.3 + 30 \implies 30 = 141 - 37.3 \longrightarrow 30 = 141 - 3(1024) + 141.21$

$37 = 30.1 + 7 \implies 7 = 37 - 30 \longrightarrow 7 = 1024 - 141.7 - 141.22 + 3.1024$

$30 = 7.4 + 2 \implies 2 = 30 - 7.4 \longrightarrow 2 = 141.22 - 3(1024) - 4(-141.29 + 4.1024$

$7 = 2.3 + 1 \implies 1 = 7 - 2.3 \longrightarrow 1 = 4.1024 - 29.141 - 3(138.141 - 19.102$

$$\boxed{1 = 61.1024 - 443.141}$$

Ejercicio 11

Menu

[Büten Zar]
B.Sz

ⓐ Determinar el último dígito de 3^{55} (esto es mod 10) ↗ porque es dígito.

$3^{55} \; \underline{|\,10}$ → $3^{55} - R = 10 \cdot q$ $\boxed{0 \leq R \leq 9}$

¿R?

$3^{55} \equiv R \pmod{10}$

$3^1 = 3$

$3^2 = 9$

$3^3 = 27$

$3^4 = 81 \equiv 1 \text{ mod}(10)$ $\Rightarrow$ $3^{52} \cdot 3^3 \equiv R \pmod{10}$

$3^3 \equiv R \pmod{10}$

$\Longleftrightarrow$ $10 \mid 27 - R$ $\Rightarrow$ $\boxed{R = 7}$

ⓑ Hallar el resto de la división de 12^{1257} entre 5

$12^{1257} \; \underline{|\,5}$

$12^{1257} \equiv R \pmod{5}$

¿R?

$12^1 = 12$

$12^2 = 144$

$12^3 = 1728$

$12^4 = 20736 \equiv 1 \pmod{5}$

$\Rightarrow$ $12^{1257} \equiv 12 \equiv R \pmod{5}$ $\Rightarrow$ $\boxed{R = 2}$

$5 \mid 12 - R$

Ejercicio 12

Menu

ⓐ Probar $2^{5n} \equiv 1 \pmod{31}$ ∀ $n \in \mathbb{N}$

Paso base

$n = 1$ $\quad 2^5 \equiv 1 \mod 31$

$32 \equiv 1 \mod 31$ OK!

Paso inductivo :

Ⓗ $n = h$ $\quad 2^{5h} \equiv 1 \mod 31$

Ⓣ $n = h+1$ $\quad 2^{5(h+1)} \equiv 1 \pmod{31}$

Demostración :

$$2^{5h+5} = 2^{5h} . 2^5 \equiv 1 \pmod{31} \overset{Ⓗ}{\Longrightarrow} 1 . 2^5 \equiv 1 \pmod{31}$$ se cumple paso base

$$\boxed{\text{Conclusión : } 2^{5n} \equiv 1 \pmod{31} \quad \forall\, n \in \mathbb{N}}$$

ⓑ Hallar el resto de la división de 2^{51833} por 31

$2^{51833} \,\underline{|\,31}$ $\quad \Longrightarrow \quad 2^{51833} \equiv R \pmod{31}$

¿R? $\qquad 0 \leq R < 31$

$$2^{51833} = 2^{51830} . 2^3 \equiv R \pmod{31} \overset{\text{parte Ⓐ}}{\Longrightarrow} 1 . 2^3 \equiv R \pmod{31}$$

$$31 \mid 8 - R \Longrightarrow \boxed{R = 8}$$

ⓒ Sea $k \in \mathbb{N}$. Sabiendo que $2^k \equiv 39 \pmod{31}$. hallar el resto de la división de k por 5.

$$2^k \equiv 39 \pmod{31} \Longrightarrow 2^k \equiv 8 \pmod{31}$$

por parte ⓑ $k = 5 . h + 3 \Longrightarrow$ $\boxed{\text{El resto buscado es 3}}$

Otra forma $\quad 2^{5h+r} \equiv 8 \pmod{31} \overset{\text{parte A}}{\Longrightarrow} 2^r \equiv 2^3 \mod 31 \Longrightarrow \boxed{r = 3}$

ⓓ Hallar el resto de la división de $43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999}$ por 31

$$\boxed{43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999} \equiv R \pmod{31}}$$

$(\Longrightarrow)$ $61 \equiv -1 \pmod{31} \Longrightarrow 61^{999} \equiv -1 \pmod{31}$

$$\boxed{43 \cdot 2^{163} + 11 \cdot 5^{221} - 1 \equiv R \pmod{31}}$$

$(\Longrightarrow)$ $5^{3} \equiv 1 \pmod{31} \Longrightarrow 5^{219} \equiv 1 \text{ mod } (31)$

$$\boxed{43 \cdot 2^{163} + 11 \cdot 5^{2} - 1 \equiv R \pmod{31}}$$

$(\Longrightarrow)$ por parte A) $2^{160} \equiv 1 \pmod{31}$

$$\boxed{43 \cdot 2^{3} + 11 \cdot 5^{2} - 1 \equiv R \pmod{31}}$$

$(\Longrightarrow)$ $43 = 32 + 11 = 2^{5} + 11$

$$\boxed{2^{3} \cdot 2^{5} + 11 \cdot 2^{3} + 11 \cdot 5^{2} - 1 \equiv R \pmod{31}}$$

$(\Longrightarrow)$ $2^{5} \equiv 1 \text{ mod } 31$ y $11 = 10 + 1$

$$\boxed{2^{3}(1 + 11) + 10 \cdot 5^{2} + 5^{2} - 1 \equiv R \pmod{31}}$$

$(\Longrightarrow)$ $12 = 3 \cdot 2^{2}$ y $10 = 5 \cdot 2$

$$\boxed{2^{5} \cdot 3 + 2 \cdot 5^{3} + 5^{2} - 1 \equiv R \pmod{31}}$$

$(\Longrightarrow)$ $2^{5} \equiv 1 \pmod{31}$ y $5^{3} \equiv 1 \pmod{31}$

$$\boxed{3 + 2 + 24 \equiv R \pmod{31}}$$

$$29 \equiv R \pmod{31} \Longrightarrow \boxed{R = 29}$$

Universidad de la República
Facultad de Ingeniería
Instituto de Matemática y Estadística

Menu

Matemática Discreta 2
Curso 2012

PRÁCTICO 4: CONGRUENCIAS

Ejercicio 1. Probar las siguientes propiedades:

a) $a \equiv b \pmod n$ y $c \equiv d \pmod n \Rightarrow a + c \equiv b + d \pmod n$ y $ac \equiv bd \pmod n$.

b) $b \equiv c \pmod n$ y $a \in \mathbb{Z} \Rightarrow a + b \equiv a + c \pmod n$.

c) $a \equiv b \pmod n$ y $m|n \Rightarrow a \equiv b \pmod m$.

d) $a \equiv b \pmod m$ y $n \in \mathbb{Z} \Rightarrow na \equiv nb \pmod m$. ¿Vale el recíproco?.

e) $a \equiv b \pmod m$ y $n \in \mathbb{N} \Rightarrow a^n \equiv b^n \pmod m$.

f) $ac \equiv bc \pmod m$ y $d = \operatorname{mcd}(c, m) \Rightarrow a \equiv b \pmod{m/d}$.

Ejercicio 2.

a) Si $a \equiv 22 \pmod{14}$, hallar el resto de dividir a a por 2, por 7 y por 14.

b) Si $a \equiv 13 \pmod 5$, hallar el resto de dividir a $33a^3 + 3a^2 - 197a + 2$ por 5.

c) Hallar, para cada $n \in \mathbb{N}$, el resto de la división de $\displaystyle\sum_{i=1}^{n} (-1)^i \cdot i!$ por 36.

Ejercicio 3. Probar que si a y b son enteros y p un número primo entonces

$$(a + b)^p \equiv a^p + b^p \pmod p$$

¿Vale el resultado si p no es primo?.

Ejercicio 4.

a) Hallar todos los $a \in \mathbb{Z}$ tales que $a^3 \equiv 3 \pmod{11}$.

b) Probar que no existe ningún entero a tal que $a^3 \equiv -3 \pmod{13}$.

c) Probar que $a^2 \equiv -1 \pmod 5 \Leftrightarrow a \equiv 2 \pmod 5$ ó $a \equiv 3 \pmod 5$.

d) Probar que $a^7 \equiv a \pmod 7$ para todo $a \in \mathbb{Z}$.

Ejercicio 5. Encontrar las cuatro soluciones (módulo 35) de la ecuación

$$x^2 - 1 \equiv 0 \pmod{35}.$$

Ejercicio 6.

a) Demostrar que $10^n \equiv (-1)^n \bmod 11$.

b) Enunciar y probar un criterio de divisibilidad entre 11.

c) Hallar el dígito d, de modo que el número $2d653874$ sea múltiplo de 11.

Ejercicio 7. Demostrar que $4^n \equiv 4 \pmod{6}$ para todo entero $n \geq 1$.

Ejercicio 8.

a) Probar que para todo $a \in \mathbb{Z}$ se cumple que

$$a^2 \equiv 0 (\operatorname{mod} 4) \qquad \text{ó} \qquad a^2 \equiv 1 (\operatorname{mod} 4).$$

b) Averiguar si 3456745356002345676543462 es un cuadrado perfecto.

c) Probar que ningún número de la sucesión

$$a_1 = 11, \quad a_2 = 111, \quad a_3 = 1111, \qquad a_n = 11\ldots 11$$

es un cuadrado perfecto.

Ejercicio 9. Resolver cada una de las congruencias siguientes:

a) $3x \equiv 7 \pmod{16}$,
b) $2x + 8 \equiv 5 \pmod{33}$,
c) $3x + 9 \equiv 8x + 61 \pmod{64}$.
d) $6x - 1 \equiv 5 \pmod{12}$
e) $9x + 3 \equiv 5 \pmod{18}$

Ejercicio 10.

a) Probar que 2 es invertible $\operatorname{mod} n$ si y solamente si n es impar. En tal caso, hallar el inverso.

b) Hallar $71^{10} (\operatorname{mod} 141)$.

Ejercicio 11.

a) Determinar el último dígito de 3^{55}.

b) Hallar el resto de la división de 12^{1257} entre 5.

Ejercicio 12.

a) Probar $2^{5n} \equiv 1 \pmod{31}$ para todo $n \in \mathbb{N}$.

b) Hallar el resto de la división de 2^{51833} por 31.

c) Sea $k \in \mathbb{N}$. Sabiendo que $2^k \equiv 39 \pmod{31}$, hallar el resto de la división de k por 5.

d) Hallar el resto de la división de $43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999}$ por 31.