Ejercicio 5.

a. 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?

b. Probar (por inducción) el Teorema de Fermat: $a^p \equiv a \pmod{p}$, para todo a entero y todo primo p.

a. $(a+b)^p = \sum_{i=0}^{p} C_i^p a^i b^{p-i} \equiv a^p + b^p \pmod{p}$.

$p \mid C_i^p \quad 0 < i < p$

$$C_i^p = \frac{p!}{i!\,(p-i)!} = p \cdot \frac{(p-1)!}{i!\,(p-i)!}$$

b. Inducción en a:

PB: $a = 0$ ✓

PI: Se cumple para a $\left(a^p \equiv a \ (p)\right)$

$$(a+1)^p \equiv a^p + 1^p \ (p) \equiv a+1 \ (p).$$

$$(a-1)^p \equiv a^p + (-1)^p \ (p) \equiv a-1 \ (p)$$

Si p impar $\Rightarrow (-1)^p = -1$
Si $p = 2$ $\Rightarrow (-1)^2 = 1 \equiv -1 \ (2)$

Ejercicio 3. Probar que $a \equiv b \pmod{m}$ si y solo si $a \equiv b + mi \pmod{mh}$ para algún i, $0 \leq i < h$.

$x \equiv 1 \ (2) \Rightarrow x = 1, 3, 5, 7, \ldots$

$x \equiv 1 \ (2 \cdot 3) \Rightarrow x = 1, 7, 13, \ldots$

($\Leftarrow$) Fácil, aplicar la def.

$(\Rightarrow)$ tengo $a-b = m \cdot k$

División entera de k entre h:

$k = h \cdot k' + i \qquad 0 \leq i < h$

$\Rightarrow \quad a - b = \dots$

Inversos: Si $n \in \mathbb{Z}$, decimos que a es invertible mód n si $\exists\, x /$

$a \cdot x \equiv 1 \ (\text{mód } n)$.

Esto pasa sii $\text{mcd}(a,n) = 1$

Además, x es único mód n.

Ejercicio 9.

a. Probar que 2 es invertible módulo n si y solamente si n es impar. En tal caso, hallar el inverso.

b. Resolver la ecuación $2x + 1 \equiv 0 \pmod{69}$.

a. Si $n = 2k+1$

¿ $2 \cdot x - 1 = \alpha(2k+1)$?

$2(k+1) - 1 = 2k + 2 - 1 = 2k+1 = n$

El inverso de 2 es $k+1$

y se escribe $2^{-1} \equiv \underbrace{k+1}_{\frac{n+1}{2}} \ (\text{mód } n)$

b. $2x + 1 \equiv 0 \ (\text{mód } 69)$

$$2x \equiv -1 \ (69)$$
$$2^{-1} \cdot 2 \cdot x \equiv -2^{-1} \ (69)$$
$$x \equiv -2^{-1} \ (69) \equiv -35 \ (69) \equiv 34 \ (69)$$

Ejercicio 10.

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

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

c. Hallar $71^{10} \pmod{141}$.

a. $3^{55} = 3^{54} \cdot 3 = 3^{2 \cdot 27} \cdot 3$

$= 9^{27} \cdot 3 \equiv (-1)^{27} \cdot 3 \ (10) \equiv -3 \ (10) \equiv 7 (10).$

b. Recordar: podemos la base

o sea $12^{1257} \equiv 2^{1257} \ (5).$

ya que $\boxed{12 \equiv 2 \ (5)}$

Ahora podemos usar Fermat:

$$2^5 \equiv 2 \ (5)$$
$$\cancel{2} \cdot 2^4 \equiv \cancel{2} 1 (5) \qquad 1257 = 4 \cdot k + 1$$
$$2^{1257} \equiv (2^4)^k \cdot 2^1 \equiv 2 \ (5).$$

c. $2^{-1} \equiv 71 \ (141)$

$$71^{10} \equiv (2^{-1})^{10} \ (141) \equiv (2^{10})^{-1} \ (141)$$

$$\equiv 1024^{-1} \ (141) \equiv 37^{-1} \ (141) \equiv \cdots$$

Para hallar x / $37 \cdot x \equiv 1 \ (141)$

usamos Bezout: $\exists \ x, y$ /

$$37 \cdot x + 141 \cdot y = 1 \implies 37 \cdot x \equiv 1 \ (141)$$

Para hallar x usamos AEE: ...

$\boxed{x = 61}$.

Ejercicio 12. 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. $9x + 3 \equiv 5 \pmod{18}$.

e. $9x + 3 \equiv 5 \ (18)$

$9x \equiv 2 \ (18)$ tiene sol sii

mcd$(9, 18) \mid 2$ pero no pasa.

No hay solución.

d. $6x \equiv 6 \ (12)$

$$\implies \boxed{x \equiv 1 \ (2)} \overset{\text{Ej } 3}{\implies} x \equiv 1 + i \cdot 2 \ (12)$$

$i = 0, 1, 2, 3, 4, 5$

Ejercicio 1. Resolver los siguientes sistemas de módulos coprimos de dos formas: por substitución y utilizando la solución particular vista en teórico.

a. $\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 5 \pmod{13} \end{cases}$ **b.** $\begin{cases} x \equiv 3 \pmod{14} \\ 2x \equiv 3 \pmod{11} \end{cases}$ **c.** $\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{12} \end{cases}$

TCR: El sistema $\begin{cases} x \equiv a \ (m) \\ x \equiv b \ (n) \end{cases}$

con $mcd(m,n) = 1$ tiene solución y es única mód $m \cdot n$.

a. $\begin{cases} x \equiv 3 \ (7) \\ x \equiv 5 \ (13) \longrightarrow x = 5 + 13 \cdot k \end{cases}$

$\Rightarrow \quad 5 + 13 \cdot k \equiv 3 \ (7)$

$6 \cdot k \equiv 5 \ (7)$

$(-1) k \equiv 5 \ (7)$

-1 siempre es invertible mód n y su inverso es -1.

$k \equiv -5 \ (7) \equiv 2 \ (7)$

Puedo tomar $\boxed{k = 2}$

$\Rightarrow \quad x = 5 + 13 \cdot 2 = 31$ es una solución

c. $\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 3 \pmod{7} \\ x \equiv 10 \pmod{12} \end{cases}$

Resolvemos la primera con la última $\begin{cases} x \equiv 5 \ (11) \\ x \equiv 10 \ (12) \longrightarrow x = 10 + 12 \cdot k \end{cases}$

$$\Rightarrow \quad 10 + 12k \equiv 5 \ (11)$$
$$k \equiv 5 - 10 \ (11)$$
$$\equiv 6 \ (11)$$
$$x = 10 + 12 \cdot 6 = 82.$$

El sistema original es eq. a

$$\begin{cases} x \equiv 82 \ (11 \cdot 12) \\ x \equiv 3 \ (7) \end{cases}$$

$$x = 82 + 11 \cdot 12 \cdot t$$

$$\Rightarrow \quad 82 + 11 \cdot 12 \cdot t \equiv 3 \ (7)$$
$$-2 + 4 \cdot 5 \cdot t \equiv 3 \ (7)$$
$$20 \cdot t \equiv 5 \ (7)$$
$$-t \equiv 5 \ (7) \Rightarrow t \equiv 2 \ (7)$$

$$x = 82 + 2 \cdot 11 \cdot 12$$
$$= 346$$

c. Hallar el menor par $x > 199$ que cumpla $2x + 3 \equiv 4 \pmod 5$ y $3x + 4 \equiv 3 \pmod 7$.

$$2^{-1} \equiv 3 \ (5) \qquad 3^{-1} \equiv 5 \ (7)$$

$$x \equiv 3 \ (5) \qquad x \equiv 2 \ (7)$$

$$\begin{cases} x \equiv 0 \ (2) \\ x \equiv 3 \ (5) \\ x \equiv 2 \ (7) \end{cases}$$

$$\Updownarrow$$

$$x \equiv 58 \ (70)$$

$$\boxed{x = 268} = 58 + 3 \cdot 70$$

Ejercicio 3. Investigar si los siguientes sistemas tienen solución, y en caso de que así sea, hallarlas todas (observar que cuando existen soluciones, son únicas módulo el m.c.m. de los módulos de cada ecuación).

a. $\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 6 \pmod{21} \\ x \equiv 11 \pmod{15} \end{cases}$ **b.** $\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 15 \pmod{21} \\ x \equiv 12 \pmod{15} \end{cases}$ **c.** $\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{15} \\ x \equiv 7 \pmod{18} \end{cases}$

$\begin{cases} x \equiv 6 \ (3) \\ x \equiv 6 \ (7) \end{cases}$ como 3 y 7 son coprimos $\Rightarrow$ tengo sol. y es única módulo 21.

$\begin{cases} x \equiv 6 \ (3) \\ x \equiv 6 \ (7) \end{cases} \iff \boxed{x \equiv 6 \ (21)}$

$\begin{cases} x \equiv 5 \ (2) \\ x \equiv 5 \ (2) \\ x \equiv 5 \ (2) \end{cases} \cancel{\iff} \quad x \equiv 5 \ (8)$

$\begin{cases} x \equiv 1 \ (7) \\ x \equiv 6 \ (21) \\ x \equiv 11 \ (15) \end{cases} \iff \begin{cases} x \equiv 1 \ (7) \\ x \equiv 6 \ (3) \equiv 0 \ (3) \\ x \equiv 6 \ (7) \\ x \equiv 11 \ (3) \equiv 2 \ (3) \\ x \equiv 11 \ (5) \equiv 1 \ (5) \end{cases}$

incompatibles

No hay solución.

b. $\begin{cases} x \equiv 1 \ (7) \\ x \equiv 15 \ (21) \\ x \equiv 12 \ (15) \end{cases} \iff \begin{cases} x \equiv 1 \ (7) \\ x \equiv 15 \ (3) \equiv 0 \ (3) \\ \cancel{x \equiv 15 \ (7) \equiv 1 \ (7)} \\ \cancel{x \equiv 12 \ (3) \equiv 0 \ (3)} \\ x \equiv 12 \ (5) \equiv 2 \ (5) \end{cases}$

$$\Leftrightarrow \begin{cases} x \equiv 1 \ (7) \\ x \equiv 0 \ (3) \\ x \equiv 2 \ (5) \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \ (7) \\ x \equiv 12 \ (15) \end{cases}$$

$x = 12 + 15 \cdot k \Rightarrow 12 + 15 \cdot k \equiv 1 \ (7)$

$k \equiv -11 \ (7) \equiv 3 \ (7)$

podemos tomar $\boxed{k = 3}$

$x = 12 + 15 \cdot 3 = 12 + 45 = 57$

c. $\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{15} \\ x \equiv 7 \pmod{18} \end{cases} \Leftrightarrow \begin{cases} x \equiv 3 \ (4) \\ x \equiv 6 \ (3) \equiv 0 \ (3) \\ x \equiv 6 \ (5) \equiv 1 \ (5) \\ x \equiv 7 \ (2) \equiv 1 \ (2) \\ x \equiv 7 \ (9) \end{cases}$ $\Rightarrow$ no son compatibles

Si $x \equiv 7 \ (9) \Rightarrow x \equiv 7 \ (3) \equiv 1 \ (3)$

contradice la segunda congruencia.

$\Rightarrow$ no hay solución.

c. $\begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 6 \pmod{15} \\ x \equiv \cancel{7}9 \pmod{18} \end{cases}$ $\iff$ $\begin{cases} x \equiv 3\ (4) \\ x \equiv 6\ (3) \equiv 0\ (3) \\ x \equiv 6\ (5) \equiv 1\ (5) \\ x \equiv 9\cancel{7}\ (2) \equiv 1\ (2) \\ x \equiv 9\cancel{7}\ (9) \equiv 0\ (9) \end{cases}$

Ahora la primer cong. implica la 5ta y la última implica la 2da

Entonces c. $\iff$ $\begin{cases} x \equiv 3\ (4) \\ x \equiv 1\ (5) \\ x \equiv 0\ (9) \end{cases}$

Ejercicio 5. Cuando pedimos calcular $a \pmod{m}$ nos referimos a hallar el entero $0 \leq x < m$ tal que $a \equiv x \pmod{m}$, en particular $a^{-1} \pmod{m}$ denota al inverso de a módulo m. En los siguientes casos, calcular:

a. los últimos dos dígitos de 7^{42} y de 23^{41};

b. $2^{61} \pmod{77}$ y $13^{31} \pmod{77}$ (sug. en el último caso descomponer módulo 7 y módulo 11);

a. Hay que calcular $7^{42}\ (100)$ y $23^{41}\ (100)$.

Fermat: 1. Si $mcd(a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1\ (n)$

2. Si $mcd(a,n) = 1$ y $m \equiv k\ (\varphi(n))$

$\Rightarrow a^m \equiv a^k\ (n)$.

Ej: $2^{107} \equiv 2^3\ (5)$ $\left(\varphi(5) = 4,\ y\ 107 \equiv 3\ (4) \right)$

Primero calculamos $\varphi(100) = \varphi(2^2 \cdot 5^2)$

$= \varphi(2^2) \cdot \varphi(5^2) = (2-1) \cdot 2^1 \cdot (5-1) \cdot 5^1$

$= 2 \cdot 4 \cdot 5 = 40.$

Por 2 de Fermat tenemos que

$7^{42} \equiv 7^2 \ (100) \equiv 49 \ (100),$

$23^{41} \equiv 23^1 \ (100) \equiv 23 \ (100).$

b. $2^{61} \equiv 2 \ (77)$

$\varphi(77) = \varphi(7) \cdot \varphi(11) = 6 \cdot 10 = 60.$

$x \equiv 13^{31} \ (77) \iff \begin{cases} x \equiv 13^{31} \ (7) & (1) \\ x \equiv 13^{31} \ (11) & (2) \end{cases}$

(1) $x \equiv 13^{31} \ (7) \equiv (-1)^{31} \ (7) \equiv -1 \ (7)$

(2) $x \equiv 13^{31} \ (11) \equiv 13^1 \ (11) \equiv 2 \ (11)$

$\varphi(11) = 10$

$x \equiv 13^{31} \ (77) \iff \begin{cases} x \equiv -1 \ (7) \\ x \equiv 2 \ (11) \end{cases}$

$x = 2 + 11 \cdot k \implies 2 + 11 \cdot k \equiv -1 \ (7)$

$4 \cdot k \equiv -3 \ (7)$

$\equiv 4 \ (7)$

$\implies k \equiv 1 \ (7) \implies x = 2 + 11 = 13.$

$\boxed{x \equiv 13 \ (77)}$

a. $132^{231} \pmod 7$).

b. $246^{218} \pmod{11}$.

c. Hallar el último dígito de $2^{1000000}$ representado en base 13.

d. Investigar si 257 es primo y calcular $3^{9990} \pmod{257}$.

e. $2^{69} \pmod{71}$.

f. $3^{279} \pmod{283}$.

g. $2^{156} \pmod{11}$.

h. $2^{30} \pmod 3$ y $2^{30} \pmod{37}$ y utilizarlos para calcular $2^{30} \pmod{111}$.

i. $347^{231} \pmod{35}$ (sugerencia: imitar lo hecho en la parte anterior).

j. $560^{48} \pmod{1001}$.

l. $2^{71} \pmod{111}$.

n. $70^{151} \pmod{252}$.

k. $22^{232} \pmod{36}$.

m. $12^{22} \pmod{100}$.

ñ. Hallar el resto de dividir 123^{253} entre 490 (sugerencia: hallar los restos de dividir 123^{253} entre 2, 5 y 49).

o. Hallar el resto de dividir 24^{253} entre 490.

c. $2^{-1} \pmod{55}$ y $2^{38} \pmod{55}$;

d. $123^{253} \pmod{490}$ (sug. descomponer módulo 2, 5 y 49).

c. $2^{-1} \equiv \frac{55+1}{2} \ (55) \equiv 28 \ (55)$

$\varphi(55) = \varphi(5)\cdot\varphi(11) = 4\cdot 10 = \boxed{40}$

Por T. de Fermat $\quad 2^{38} \equiv 2^{-2} \ (55)$

$\equiv (2^{-1})^2 \ (55)$

$\equiv 28^2 \ (55) \equiv 14 \ (55)$

$$\begin{array}{r} \overset{6}{28} \\ 28 \\ \hline 224 \\ 56 \\ \hline 784 \end{array} \quad \begin{array}{l} \underline{|\,55} \\ 14 \end{array}$$

$$\begin{array}{r} 784 \\ 234 \\ 220 \\ \hline 14 \end{array}$$

o. Hallar el resto de dividir 24^{253} entre 490.

$490 = 2 \cdot 5 \cdot 7^2$

$\varphi(490) = 4 \cdot 6 \cdot 7 = 168$

24 y 490 NO son coprimos

$\Rightarrow$ no puedo aplicar Fermat de manera directa.

$$x \equiv 24^{253} \ (490) \iff \begin{cases} x \equiv 24^{253} \ (2) \\ x \equiv 24^{253} \ (5) \\ x \equiv 24^{253} \ (49) \end{cases}$$

$$\iff \begin{cases} x \equiv 0 \ (2) \\ x \equiv (-1)^{253} \ (5) \equiv -1 \ (5) \\ x \equiv 24 \ (49) \end{cases} \iff x \equiv 24 \ (490)$$

Para calcular 24^{253} (49)

hay que reducir 253 mód $\varphi(49) = 42$.

$$\begin{array}{r|l} 253 & 42 \\ \hline 252 & 6 \\ \hline 1 & \end{array}$$

$253 \equiv 1\ (42)$

$\Rightarrow\ 24^{253} \equiv 24^{1}\ (49)$

Ejercicio 8. Se dice que un entero n es un *pseudoprimo de Carmichael* si n es compuesto y $a^n \equiv a \pmod{n}$ para todo $a \in \mathbb{Z}$.

a. Sea b un número entero positivo y coprimo con 561.

i) Demostrar que $b^2 \equiv 1 \pmod{3}$, $b^{10} \equiv 1 \pmod{11}$ y $b^{16} \equiv 1 \pmod{17}$.

ii) Hallar $b^{560} \pmod{3}$, $b^{560} \pmod{11}$ y $b^{560} \pmod{17}$.

iii) Probar que 561 es un pseudoprimo de Carmichael (*Sugerencia: hallar b^{561} dependiendo si b es coprimo o no con* 561).

$561 = 3 \cdot 11 \cdot 17$

i. Euler. ii. $b^{560}\ (3) \equiv (b^2)^{\frac{560}{2}}\ (3) \equiv 1 (3)$

$\boxed{2 \mid 560}$, $\boxed{10 \mid 560}$, $\boxed{16 \mid 560}$

$\Rightarrow\ b^{560} \equiv 1\ (3)$ $\qquad b^{560} \equiv 1\ (17)$

$b^{560} \equiv 1\ (11)$

iii. Si b coprimo con 561

$\Rightarrow\ b^{560} \equiv 1\ (561)$ por TCR.

$\Rightarrow\ \boxed{b^{561} \equiv b\ (561)}$

De 2 sabemos que si b es coprimo con 561 $\Rightarrow \begin{cases} b^{561} \equiv b\ (3) \\ b^{561} \equiv b\ (11) \\ b^{561} \equiv b\ (17) \end{cases}$

$\Leftrightarrow b^{561} \equiv b\ (3 \cdot 11 \cdot 17)$.

Pero si no fuese coprimo esos se siguen cumpliendo ya que me daría cero en los primos en común de b y 561. $\Rightarrow b^{561} \equiv b\ (561)$

$\forall\, b$.

b. Sea n un entero compuesto tal que $\varphi(n)|n-1$.

i) Probar que n es libre de cuadrados e impar.

ii) Utilizando la parte anterior y el Teorema Chino del resto probar que n es un pseudoprimo de Carmichael.

Def: n es libre de cuadrados si $n = p_1 \cdots p_k$ con primos distintos

ó es lo mismo $\boxed{\nexists\, p \,/\, p^2 | n}$