Primer parcial - primer semestre 2023

ii) (8 puntos) Calcule el resto de dividir $2^{2023} + 3^{2023}$ entre 25.

$$2^{2023} + 3^{2023} \equiv r \pmod{25} \quad \text{con} \quad 0 \leq r \leq 24$$

* $2^{2023} \pmod{25}$

$\text{mcd}(2,25) = 1$ entonces podemos aplicar el teorema Euler

$25 = 5^2$

$\varphi(25) = 25\left(1 - \frac{1}{5}\right) = 25 \cdot \frac{4}{5} = 20$

entonces por el teorema de Euler: $2^{20} \equiv 1 \pmod{25}$

$2023 = 20 \cdot 101 + 3$

$$2^{2023} \equiv 2^{20 \cdot 101 + 3} \pmod{25}$$
$$\equiv (2^{20})^{101} \cdot 2^3 \pmod{25}$$
$$\equiv 1^{101} \cdot 2^3 \pmod{25}$$
$$\equiv 2^3 \pmod{25}$$

$$\boxed{2^{2023} \equiv 8 \pmod{25}}$$

$(2^{20})^{101} \cdot 2^3 \equiv 1^{101} \cdot 2^3 \pmod{25}$

$2^{2023} \equiv 2^3 \pmod{25}$

* $3^{2023} \pmod{25}$

$\text{mcd}(3,25) = 1$ entonces podemos aplicar Euler

$\varphi(25) = 20$

entonces $3^{20} \equiv 1 \pmod{25}$

$$3^{2023} \equiv 3^{20 \cdot 101 + 3} \pmod{25}$$
$$\equiv (3^{20})^{101} \cdot 3^3 \pmod{25}$$
$$\equiv 3^3 \pmod{25}$$
$$\equiv 27 \pmod{25}$$
$$\equiv 2 \pmod{25}$$

$$\boxed{3^{2023} \equiv 2 \pmod{25}}$$

$$2^{2023} + 3^{2023} \equiv 8 + 2 \pmod{25}$$
$$\equiv 10 \pmod{25}$$

$\Rightarrow$ el resto de dividir $2^{2023} + 3^{2023}$ entre 25 es 10.

Ejercicio 5. – Practico 5

a. Determinar el último dígito de 3^{55} en base 10. Sugerencia: probar que $3^{55} \equiv a_0 \pmod{10}$; donde a_0 es el dígito buscado.

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

a) el último dígito de 3^{55} es el resto de dividir 3^{55} entre 10

$$3^{55} \equiv r \pmod{10} \quad \text{con} \quad 0 \leq r < 10$$

$\text{mcd}(3, 10) = 1$ entonces podemos aplicar el teorema de Euler

$10 = 2 \cdot 5$

$\varphi(10) = 10\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4$

entonces por Euler: $3^4 \equiv 1 \pmod{10}$

$55 = 4 \cdot 13 + 3$

$$3^{55} \equiv 3^{4 \cdot 13 + 3} \pmod{10}$$
$$\equiv (3^4)^{13} \cdot 3^3 \pmod{10}$$
$$\equiv 3^3 \pmod{10}$$
$$\equiv 27 \pmod{10}$$
$$\equiv 7 \pmod{10}$$

↑ último dígito de 3^{55}

b) resto en la división de 12^{1257} entre 5

$$12^{1257} \equiv r \pmod{5} \quad \text{con} \quad 0 \leq r < 5$$

$$12^{1257} \equiv 2^{1257} \pmod{5}$$

$2^1 \equiv 2 \pmod{5}$

$2^2 \equiv 4 \pmod{5}$

$2^3 \equiv 3 \pmod{5}$

$2^4 \equiv 1 \pmod{5}$

$1257 = 314 \cdot 4 + 1$

$2^{1257} \equiv 2^{4 \cdot 314 + 1} \pmod 5$

$\equiv (2^4)^{314} \cdot 2 \pmod 5$

$\equiv 2 \pmod 5$

entonces $12^{1257} \equiv 2 \pmod 5$

Parcial 2022 - segundo semestre

3) Calcular el resto de dividir 70^{151} entre 252.

$70^{151} \equiv r \pmod{252}$

$252 = 4 \cdot 63 = 4 \cdot 9 \cdot 7$

$70^{151} \equiv r \pmod{252} \overset{\text{TCR}}{\Longleftrightarrow}$ (4, 9 y 7 son divisores de 252)

$$\begin{cases} 70^{151} \equiv r \pmod 4 \\ 70^{151} \equiv r \pmod 9 \\ 70^{151} \equiv r \pmod 7 \end{cases}$$

* $r \equiv 70^{151} \pmod 7 \iff r \equiv 0 \pmod 7$

* $r \equiv 70^{151} \pmod 4 \iff r \equiv 0 \pmod 4$

$70 = 4 \cdot 17 + 2 \Rightarrow 70 \equiv 2 \pmod 4$

entonces $r \equiv 70^{151} \pmod 4$

$\equiv 2^{151} \pmod 4$

$= 2^{2+149} \pmod 4$

$\equiv 4 \cdot 2^{149} \pmod 4$

$\equiv 0 \pmod 4$

* $r \equiv 70^{151} \pmod 9 \Rightarrow r \equiv 7 \pmod 9$

$70 = 7 \cdot 9 + 7 \Rightarrow 70 \equiv 7 \pmod 9$

$\Rightarrow r \equiv 7^{151} \pmod 9$

$7^{151} \pmod 9$

$\text{mcd}(7,9) = 1$ entonces podemos aplicar Euler

$9 = 3^2$

$\varphi(9) = 9\left(1 - \frac{1}{3}\right) = 9 \cdot \frac{2}{3} = 6$

entonces por el teorema de Euler $7^6 \equiv 1 \pmod 9$

$151 = 6 \cdot 25 + 1$

$$\begin{aligned} 7^{151} &\equiv 7^{6\cdot 25+1} \pmod 9 \\ &\equiv (7^6)^{25} \cdot 7 \pmod 9 \\ &\equiv 7 \pmod 9 \end{aligned}$$

$$\left.\begin{cases} 70^{151} \equiv r \pmod 4 \iff r \equiv 0 \pmod 4 \\ 70^{151} \equiv r \pmod 7 \iff r \equiv 0 \pmod 7 \\ 70^{151} \equiv r \pmod 9 \iff r \equiv 7 \pmod 9 \end{cases}\right\} \text{TCR} \iff r \equiv 0 \pmod{28}$$

$$\begin{cases} r \equiv 0 \pmod{28} \\ r \equiv 7 \pmod 9 \end{cases}$$

$r \equiv 0 \pmod{28} \longrightarrow r = 28x \quad \text{con } x \in \mathbb{Z}$

$r \equiv 7 \pmod 9 \longrightarrow r = 9y + 7 \quad \text{con } y \in \mathbb{Z}$

$\Rightarrow 28x = 9y + 7$

$\Rightarrow 28x - 9y = 7$ ecuación diofántica

* $\text{mcd}(28,9) = 1 \Rightarrow$ tiene solución
* solución particular:

$28 - 9 \cdot 3 = 1$ Bezout

$28 \cdot 7 - 9 \cdot 3 \cdot 7 = 7$

solución particular: $\begin{cases} x_0 = 7 \\ y_0 = 21 \end{cases}$

* conjunto de soluciones:

$$28(7 + \underbrace{9k}_{\mathbb{Z}}) - 9(21 + \underbrace{28k}_{\mathbb{Z}}) = 7$$

$$\begin{cases} x = 7 + 9k \text{ con } k \in \mathbb{Z} \\ y = 21 + 28k \text{ con } k \in \mathbb{Z} \end{cases}$$

entonces: $r = 28x = 28(7 + 9k) = 196 + 252k$

$$\begin{cases} r \equiv 0 \pmod{28} \\ r \equiv 7 \pmod{9} \end{cases} \iff r = 196 + 252k \iff r \equiv 196 \pmod{252}$$

$r - 196 = 252k$

Parcial 2021 - segundo semestre

c) Un entero positivo n se dice admisible si verifica que $\frac{7n+i}{2+i}$ es entero para $i = 1, 2, 3$.

i) (3 pts.) ¿Cuántos enteros positivos admisibles verifican $n \leq 1200$?

ii) (3 pts.) Hallar el menor entero admisible que verifique $n > 1200$.

n admisible si $\frac{7n+1}{2+1}$, $\frac{7n+2}{2+2}$, $\frac{7n+3}{2+3}$ son enteros

si $3 \mid 7n+1$, $4 \mid 7n+2$, $5 \mid 7n+3$

si $\begin{cases} 7n+1 \equiv 0 \pmod 3 \\ 7n+2 \equiv 0 \pmod 4 \\ 7n+3 \equiv 0 \pmod 5 \end{cases}$ ← buscamos la cantidad de soluciones positivas con $n \leq 1200$

$$\begin{cases} 7n+1 \equiv 0 \pmod 3 \\ 7n+2 \equiv 0 \pmod 4 \\ 7n+3 \equiv 0 \pmod 5 \end{cases} \iff \begin{cases} 7n \equiv -1 \pmod 3 \\ 7n \equiv -2 \pmod 4 \\ 7n \equiv -3 \pmod 5 \end{cases} \iff \begin{cases} 7n \equiv 2 \pmod 3 \\ 7n \equiv 2 \pmod 4 \\ 7n \equiv 2 \pmod 5 \end{cases}$$

$x = 7n \iff \begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 2 \pmod 4 \\ x \equiv 2 \pmod 5 \end{cases}$

$\iff x \equiv 2 \pmod{3 \cdot 4 \cdot 5}$

$$\begin{cases} 7n \equiv 2 \pmod 3 \\ 7n \equiv 2 \pmod 4 \\ 7n \equiv 2 \pmod 5 \end{cases} \iff \boxed{7n \equiv 2 \pmod{60}}$$

$7n \equiv 2 \pmod{60}$

vamos a buscar el inverso de 7 modulo 60:

igualdad de Bezout para 7 y 60:

$$60 = 7 \cdot 8 + 4$$
$$7 = 4 \cdot 1 + 3$$
$$4 = 3 + 1$$

$$1 = 4 - 3$$
$$1 = 4 - (7 - 4)$$
$$1 = 2 \cdot 4 - 7$$
$$1 = 2(60 - 7 \cdot 8) - 7$$
$$1 = 2 \cdot 60 - 17 \cdot 7$$

Bezout: $2 \cdot 60 - 17 \cdot 7 = 1$

$$\Rightarrow 2 \cdot 60 - 17 \cdot 7 \equiv 1 \pmod{60}$$
$$\Rightarrow \underbrace{-17}_{\text{inverso de 7 módulo 60}} \cdot 7 \equiv 1 \pmod{60}$$

x inverso de 7 mod 60

$x \equiv -17 \pmod{60}$

$$7n \equiv 2 \pmod{60} \iff -17 \cdot 7n \equiv -17 \cdot 2 \pmod{60}$$
$$\iff n \equiv -34 \pmod{60}$$
$$\iff n \equiv 26 \pmod{60}$$

la cantidad de soluciones positivas tales que $n \leq 1200$ es

$$\frac{1200}{60} = 20$$

b) menor n admisible tal que $n > 1200$

$n = 26 + 20 \cdot 60 = 1226$

b. (7 puntos) Probar que si $\mcd(m,n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$.

Teorema 2.6.3. *Si* $\mcd(m,n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$.

Demostración. Como la tesis es obvia si m o n es 1, demostrémoslo para $m, n > 1$. La idea de la demostración es la siguiente: daremos dos conjuntos C y D tales que $\#C = \varphi(mn)$ y $\#D = \varphi(m)\varphi(n)$, y luego construiremos una función biyectiva $f : C \to D$ lo cual terminaría probado que $\#C = \#D$; es decir que $\varphi(mn) = \varphi(m)(n)$.

Sea $C = \{c \in \{0, \cdots, mn-1\} : \mcd(c, mn) = 1\}$; claramente $\#C = \varphi(mn)$. Además, tenemos que

$$\mcd(c, mn) = 1 \Leftrightarrow \mcd(c,m) = 1 \text{ y } \mcd(c,n) = 1. \tag{2.6.4}$$

Así que $C = \{c \in \{0, \cdots, mn\} : \mcd(c,m) = 1 \text{ y } \mcd(c,n) = 1\}$.

Sean $A = \{a \in \{0, \cdots, m-1\} : \mcd(a,m) = 1\}$ y $B = \{b \in \{0, \cdots, n-1\} : \mcd(b,n) = 1\}$; tenemos que $\#A = \varphi(m)$, $\#B = \varphi(n)$ y por lo tanto si $D = A \times B = \{(a,b) : a \in A,\ b \in B\}$ tenemos que $\#D = \varphi(m)\varphi(n)$.

Consideramos ahora la función $f : C \to D$ dada por $f(c) = (a,b)$ siendo a el resto de dividir c entre m y b el resto de dividir c entre n. Es decir $f(c) = (a,b)$ con $a \in \{0, \cdots, m-1\}$, $b \in \{0, \cdots, n-1\}$ y

~~$c \equiv a \pmod m$~~ $\quad \begin{cases} c \equiv a \pmod m \\ c \equiv b \pmod n \end{cases}$

Veamos primero que efectivamente, si $c \in C$ y $f(c) = (a,b)$ entonces $(a,b) \in D$. Como $c = mq + a$ y $c = nq' + b$ tememos (por la Proposición 1.2.6) que

$$\mcd(c,m) = \mcd(a,m) \text{ y } \mcd(c,n) = \mcd(b,n). \tag{2.6.5}$$

Por lo tanto si $\mcd(c,m) = 1$ y $\mcd(c,n) = 1$ tenemos que $\mcd(a,m) = 1$ y $\mcd(b,n) = 1$. Como además claramente $a \in \{0, \cdots, m-1\}$ y $b \in \{0, \cdots, n-1\}$ concluimos que $(a,b) \in D$.

Veamos ahora que la función f es biyectiva. Para ésto tenemos que ver que dado $(a,b) \in D$, existe un único $c \in C$ tal que $f(c) = (a,b)$ (la existencia de c nos da la sobreyectividad de f y la unicidad nos da la inyectividad de f). Tenemos que probar entonces que dado $(a,b) \in D$, existe un único $c \in C$ tal que

$$\begin{cases} c \equiv a \pmod m \\ c \equiv b \pmod n. \end{cases} \tag{2.6.6}$$

Como $\mcd(m,n) = 1$, por el Teorema Chino del Resto sabemos que el sistema

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n. \end{cases}$$

tiene solución x_0 y que además, todas las soluciones son $x \equiv x_0 \pmod{mn}$. Por lo tanto, existe un único $c \in \{0, \cdots, mn-1\}$ que verifica (2.6.6). Resta ver que efectivamente este $c \in C$: como $\mcd(a,m) = 1$, $\mcd(b,n) = 1$ y $c \equiv a \pmod m$, $c \equiv b \pmod n$, por (2.6.5) tenemos que

$$\mcd(c,m) = 1 \text{ y } \mcd(c,n) = 1$$

y por lo tanto $c \in C$.

Teorema: Si $\mcd(m,n) = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

* Si m o n valen 1 es obvio
* Supongamos que $m > 1$ y $n > 1$

idea: $\varphi(mn) = \varphi(m)\varphi(n)$

definir
- un conjunto C tal que $\#C = \varphi(mn)$
- un conjunto D tal que $\#D = \varphi(m)\varphi(n)$

construir:

$f : C \to D$ biyectiva

entonces $\#C = \#D \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

prueba:

① vamos a definir el conjunto C

$\varphi(mn)$ = cantidad de naturales $c < mn$ tq $mcd(c, mn) = 1$

$= \#\{c \in \{0, \dots, mn-1\} : mcd(c, mn) = 1\}$

$C = \{c \in \{0, \dots, mn-1\} : mcd(c, mn) = 1\}$

tenemos $\#C = \varphi(mn)$

② vamos a definir el conjunto D ($\#D = \varphi(m)\varphi(n)$)

$\varphi(m)$ = cantidad de naturales $a < m$ tq $mcd(a, m) = 1$

$= \#\{a \in \{0, \dots, m-1\} : mcd(a, m) = 1\}$

$A = \{a \in \{0, \dots, m-1\} : mcd(a, m) = 1\}$

tenemos $\#A = \varphi(m)$

$\varphi(n)$ = cantidad de naturales $b < n$ tq $mcd(b, n) = 1$

$= \#\{b \in \{0, \dots, n-1\} : mcd(b, n) = 1\}$

$B = \{b \in \{0, \dots, n-1\} : mcd(b, n) = 1\}$

tenemos $\#B = \varphi(n)$

definimos $D = A \times B = \{(a, b) : a \in \{0, \dots, m-1\}, b \in \{0, \dots, n-1\}, mcd(a, m) = 1, mcd(b, n) = 1\}$

tenemos $\#D = \#A \times \#B = \varphi(m)\varphi(n)$

③ definimos $f : C \to D$

$C = \{c \in \{0, \dots, mn-1\} : mcd(c, mn) = 1\}$

$D = \{(a, b) : a \in \underbrace{\{0, \dots, m-1\}}_{\text{posibles valores del resto al dividir entre } m}, b \in \{0, \dots, n-1\}, mcd(a, m) = 1, mcd(b, n) = 1\}$

$f : C \to D$

$f(c) = (a, b)$ donde $\begin{cases} a \text{ es el resto de dividir } c \text{ entre } m \\ b \text{ es el resto de dividir } c \text{ entre } n \end{cases}$

$$f(c) = (a,b) \quad \text{donde} \quad \begin{cases} c \equiv a \pmod m \\ c \equiv b \pmod n \end{cases}$$

hay que ver que si $c \in C$ entonces $f(c) = (a,b) \in D$
es decir hay que ver que

$$\boxed{\text{mcd}(c, mn) = 1 \Rightarrow \text{mcd}(a, m) = 1 \text{ y } \text{mcd}(b, n) = 1}$$

(a: resto de dividir c entre m, $a = c - qm$; $b = c - q'n$)

Tenemos que $\text{mcd}(c, mn) = 1 \Rightarrow \text{mcd}(c, m) = 1$ y $\text{mcd}(c, n) = 1$
$\Rightarrow \text{mcd}(c - qm, m) = 1$ y $\text{mcd}(c - q'n, n) = 1$
$\Rightarrow \text{mcd}(a, m) = 1$ y $\text{mcd}(b, n) = 1$

④ Vamos a probar que $f: C \to D$ es biyectiva

$$f(c) = (a,b) \quad \text{donde} \quad \begin{cases} c \equiv a \pmod m \\ c \equiv b \pmod n \end{cases}$$

para ver que f es biyectiva tenemos que ver que para todo $(a,b) \in D$ existe (sobre) un único (inye) $c \in C$ tal que $f(c) = (a,b)$

o sea dado $(a,b) \in D$ queremos ver que existe un único $c \in \{0, \dots, mn-1\}$ tal que

$$\begin{cases} c \equiv a \pmod m \\ c \equiv b \pmod n \end{cases} \quad (*)$$

como $\text{mcd}(m,n) = 1$, por el teorema chino del resto

$$\begin{cases} c \equiv a \pmod m \\ c \equiv b \pmod n \end{cases} \iff c \equiv x_0 \pmod{mn}$$

es decir existe un único $c \in \{0, \dots, mn-1\}$ que verifica $(*)$

para obtener que $c \in C$ falta ver que $\text{mcd}(c, mn) = 1$

pero:

$$\begin{cases} c \equiv a \pmod{m} \\ c \equiv b \pmod{n} \end{cases}$$

$\text{mcd}(a, m) = 1$

$\text{mcd}(b, n) = 1$

$\Rightarrow$ $\text{mcd}(c, m) = 1$

$\text{mcd}(c, n) = 1$

$\text{mcd}(m, n) = 1$

$\Rightarrow \text{mcd}(c, mn) = 1$