

PRIMER PARCIAL - 26 DE ABRIL DE 2023. DURACIÓN: 3 HORAS

Nº de parcial	Cédula	Apellido y nombre	Ej. 2A o 2B

Atención: Este parcial vale 40 puntos. Debe elegir entre uno de los ejercicios 2A o 2B y marcar la opción escogida en el casillero de arriba. Justifique todas las respuestas.

Ejercicio 1 (12 puntos).

- i) (8 puntos) Demuestre que para $a, b \in \mathbb{Z}^+$ se cumple que $\text{mcm}(a, b) \cdot \text{mcd}(a, b) = ab$.
(Sug. escribir $a = da', b = db'$ con $d = \text{mcd}(a, b)$ y $a', b' \in \mathbb{Z}^+$ coprimos.)
- ii) (4 puntos) Encontrar todos los $a, b \in \mathbb{Z}^+$ tales que $\text{mcm}(a, b) + \text{mcd}(a, b) = 47$.

Ejercicio 2A (8 puntos). Sean $a > 1, b > 1$ enteros con $\text{mcd}(a, b) = 1$. Probar que la ecuación diofántica $ax + by = ab$ no tiene solución con $x, y \in \mathbb{Z}^+$. (Sug. observe que $ab = a \cdot b + b \cdot 0$.)

Ejercicio 2B (8 puntos). Sea $p(x)$ un polinomio con coeficientes enteros que cumple que $p(4) = 7$ y $p(11) = 14$. Probar que si $x_0 \in \mathbb{Z}$ es raíz del polinomio $p(x)$ entonces $3 \mid x_0$.

Ejercicio 3 (10 puntos).

- i) (2 puntos) Encuentre un inverso de 17 módulo 25 y un inverso de 25 módulo 17.
- ii) (8 puntos) Encuentre todos los naturales $x < 1000$ que verifican el siguiente sistema de congruencias:

$$\begin{cases} 3x + 5 & \equiv 0 \pmod{17} \\ 3x + 18 & \equiv 0 \pmod{75} \end{cases}$$

Ejercicio 4 (10 puntos).

- i) (2 puntos) Defina la función φ de Euler y enuncie el Teorema de Fermat-Euler.
- ii) (8 puntos) Calcule el resto de dividir $2^{2023} + 3^{2023}$ entre 25.

PRIMER PARCIAL - 26 DE ABRIL DE 2023 (SOLUCIONES)

Ejercicio 1.

- i) Escribimos $a = da', b = db'$ con $d = \text{mcd}(a, b)$ y $a', b' \in \mathbb{Z}^+$ coprimos. Queremos probar que $\text{mcm}(a, b) = da'b'$. Por un lado tenemos $a|ab' = da'b'$ y $b|a'b = da'b'$ luego $da'b'$ es un múltiplo común de a y b por lo tanto $\text{mcm}(a, b) \leq da'b'$. Como $a|\text{mcm}(a, b)$ podemos escribir $\text{mcm}(a, b) = at$. Como también $b|\text{mcm}(a, b) = at$ resulta que $b'|at$ y dado que $\text{mcd}(a', b') = 1$, por el Lema de Euclides tenemos que $b'|t$, lo cual implica $ab' = da'b'|at = \text{mcm}(a, b)$ y en particular $da'b' \leq \text{mcm}(a, b)$. Juntando ambas desigualdades obtenemos la igualdad $\text{mcd}(a, b) = da'b'$.
- ii) Tenemos $da'b' + d = d(a'b' + 1) = 47$ así que o bien $d = 1$ y $a'b' = 46$, o bien $d = 47$ y $a'b' = 0$. La segunda opción es imposible pues $a', b' \geq 1$. Para la primera opción resulta $a = a', b = b'$ y $ab = 46 = 2 \cdot 23$. Luego las posibilidades son $(a, b) = (1, 46), (2, 23), (23, 2)$ o $(46, 1)$.

Ejercicio 2A.

Realizamos el cambio de variable $x' = x - 1 \geq 0$ e $y' = y - 1 \geq 0$. La ecuación diofántica se transforma en $a(x' + 1) + b(y' + 1) = ab$, o equivalentemente $ax' + by' = ab - a - b$ y esta ecuación no tiene soluciones con $x', y' \geq 0$ pues $ab - a - b$ es el número de Frobenius de a y b .

Solución alternativa: Observamos que $(x, y) = (b, 0)$ es una solución particular de la ecuación diofántica $ax + by = ab$ y como $\text{mcd}(a, b) = 1$, todas las soluciones enteras vienen dadas por:

$$\begin{cases} x = b + bt \\ y = 0 - at \end{cases}$$

para algún $t \in \mathbb{Z}$. Para que $x, y \in \mathbb{Z}^+$ precisamos que $b + bt \geq 1$ y $-at \geq 1$, o equivalentemente que $\frac{1-b}{b} \leq t \leq \frac{-1}{a}$. Pero como $\frac{1-b}{b} = \frac{1}{b} - 1 > -1$ y $\frac{-1}{a} < 0$ precisaríamos que $-1 < t < 0$ y esto es imposible para $t \in \mathbb{Z}$.

Ejercicio 2B.

Sea $x_0 \in \mathbb{Z}$ una raíz de $p(x)$, tenemos tres posibilidades $x \equiv 0, 1$ o $2 \pmod{3}$. Si $x_0 \equiv 1 \pmod{3}$ entonces $x_0 \equiv 4 \pmod{3}$, luego $0 \equiv p(x_0) \equiv p(4) \equiv 7 \equiv 1 \pmod{3}$ que es una contradicción. Si $x_0 \equiv 2 \pmod{3}$ entonces $x_0 \equiv 11 \pmod{14}$ y $0 \equiv p(x_0) \equiv p(11) \equiv 14 \equiv 2 \pmod{3}$ que es una contradicción. La única posibilidad es que $x_0 \equiv 0 \pmod{3}$.

Ejercicio 3.

- i) Consideramos la ecuación diofántica $17x + 25y = 1$. Aplicamos el AEE para obtener una solución particular: $25 = 1 \cdot 17 + 8$ y $17 = 2 \cdot 8 + 1$, luego $1 = 17 - 2 \cdot 8 = 17 - 2 \cdot (25 - 17) = 3 \cdot 17 - 2 \cdot 25$, obteniendo $17 \cdot 3 + 25 \cdot (-2) = 1$. Esta última ecuación implica $17 \cdot 3 \equiv 1 \pmod{25}$ y $25 \cdot (-2) \equiv 1 \pmod{17}$, por lo tanto 3 es un inverso de 17 módulo 25 y -2 es un inverso de 25 módulo 17.
- ii) La primer congruencia es equivalente a $3x \equiv 12 \pmod{17}$, simplificando por 3 (observar que $\text{mcd}(3, 17) = 1$) tenemos $x \equiv 4 \pmod{17}$. La segunda congruencia es equivalente a $3x \equiv -18 \pmod{75}$, simplificando por 3 (observar que $\text{mcd}(3, 75) = 3$ y $75/3 = 25$) tenemos $x \equiv -6 \pmod{25}$. Por lo tanto el sistema de congruencias original es equivalente al sistema:

$$\begin{cases} x \equiv 4 \pmod{17} \\ x \equiv -6 \pmod{25} \end{cases}$$

Con las notaciones vistas en el teórico, una solución viene dada por $x_0 = a_1 M_1 M'_1 + a_2 M_2 M'_2$ donde $a_1 = 4$, $M_1 = m_2 = 25$ y $M'_1 = -2$ (pues M'_1 es un inverso de 25 módulo 17 y usamos la parte i), $a_2 = -6$, $M_2 = m_1 = 17$ y $M'_2 = 3$ (pues M'_2 es un inverso de 17 módulo 25 y usamos la parte ii). Luego $x_0 = 4 \cdot 25 \cdot (-2) + (-6) \cdot 17 \cdot 3 = -200 - 306 = -506$. Como $17 \cdot 25 = 425$ y $-506 + 2 \cdot 425 = 344$, la solución del sistema viene dada por $x \equiv 344 \pmod{425}$, o sea $x = 344 + 425t$ con $t \in \mathbb{Z}$. Las soluciones con $0 \leq x \leq 999$, corresponden a los valores enteros de t tales que $-344 \leq 425t \leq 655$, o equivalentemente $-344/425 = -0, \dots \leq t \leq 655/425 = 1, \dots$. Como $t \in \mathbb{Z}$ tenemos $t \in \{0, 1\}$, que corresponden con las soluciones $x = 344$ y 769 .

Ejercicio 4.

- i) El Teorema de Fermat-Euler dice que si a y m son enteros coprimos entonces $a^{\varphi(m)} \equiv 1 \pmod{m}$, donde φ es la función de Euler que se define como $\varphi(m) = \#\{i \in \mathbb{Z} : 0 \leq i < m, \text{mcd}(i, m) = 1\}$.
- ii) Tenemos $\varphi(25) = 20$ y como $2023 = 101 \cdot 20 + 3$ entonces $a^{2023} = (a^{20})^{101} \cdot a^3 \equiv 1 \cdot a^3 = a^3$ si $\text{mcd}(a, 25) = 1$ por Fermat-Euler. Esto se aplica tanto para $a = 2$ como para $a = 3$, luego $2^{2023} + 3^{2023} \equiv 2^3 + 3^3 = 8 + 27 = 35 \equiv 10 \pmod{25}$. Luego $2^{2023} + 3^{2023}$ deja resto 10 en la división por 25.