

| Nro de prueba | Cédula | Apellido y nombre |
|---------------|--------|-------------------|
| | | |

Ejercicio 1 (10 puntos)

- 1) Definir número primo.
- 2) Probar que hay infinitos números primos.

Ejercicio 2 (15 puntos)

- 1)
 - i) Enunciar el Teorema de Bézout. (Denominado igualdad o identidad de Bézout.)
 - ii) Sean $a, b, c \in \mathbb{N}$, probar que:
 - a) si $\text{mcd}(a, b) = \text{mcd}(a, c) = 1$ entonces $\text{mcd}(a, bc) = 1$
 - b) si $\text{mcm}(a, b) = ab$ y $\text{mcm}(a, c) = ac$ entonces $\text{mcm}(a, bc) = abc$.
- 2)
 - i) Enunciar y probar el teorema que estudia las soluciones de una ecuación diofántica.
 - ii) Para cada una de las siguientes ecuaciones diofánticas, encuentre todas las soluciones enteras o demuestre que no tienen solución.
 - a) $4x + 6y = 11$
 - b) $3x + 5y = 8$.

Ejercicio 3 (15 puntos)

- 1) Definir la función φ de Euler
- 2) Enunciar y probar el Teorema de Euler
- 3) Calcular el resto de dividir 70^{151} entre 252.

Solución

- Ejercicio 1**
- 1) Ver notas (Definición 1.2.2. página 7).
 - 2) Ver notas (Corolario 1.7.2. página 21).

- Ejercicio 2**
- 1)
 - i) Ver notas (Teorema 1.2.8. página 10).
 - ii) Sean $a, b, c \in \mathbb{N}$, probar que:
 - a) si $\text{mcd}(a, b) = \text{mcd}(a, c) = 1$ entonces $\text{mcd}(a, bc) = 1$. Por el teorema enunciado en la parte anterior existen $m, n, p, s \in \mathbb{Z}$ tales que $am + bn = 1$ y $ap + cs = 1$ por lo que al multiplicar la ecuaciones obtenemos $a(amp + mcs + bnp) + bcns = 1$, es decir coeficiente $r, t \in \mathbb{Z}$ tales que $ar + bct = 1$ por lo que por el mismo teorema enunciado tenemos que $\text{mcd}(a, bc) = 1$.
 - b) si $\text{mcm}(a, b) = ab$ y $\text{mcm}(a, c) = ac$ entonces $\text{mcm}(a, bc) = abc$. Por la parte anterior probada y por la igualdad $ab = \text{mcd}(a, b) \cdot \text{mcm}(a, b)$ el resultado es evidente.
 - 2)
 - i) Ver notas (Teorema 1.5.3. página 18).
 - ii) Encuentre todas las soluciones enteras de las siguientes ecuaciones diofánticas o demuestre que no tienen soluciones.
 - a) $4x + 6y = 11$, $\text{mcd}(4, 6)$ no divide a 11 por lo que no existen soluciones por el teorema enunciado en la parte anterior.
 - b) $3x + 5y = 8$. Por ese mismo teorema tenemos que al ser $(1, 1)$ una solución particular evidente nos queda que $S = \{(1 + 5k, 1 - 3k) : k \in \mathbb{Z}\}$ es el conjunto de todas sus soluciones enteras.

- Ejercicio 3**
- 1) Ver notas (Definición 2.6.1. página 38).

- 2) Ver notas (Teorema 2.6.5. página 41).
 3) Para resolver el sistema podemos calcular la soluciones de

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

y tomar una solución que este comprendida en el conjunto $\{0, 1, \dots, 251\}$.

Primero podemos observar que $70 = 2 \times 5 \times 7$ y $252 = 2^2 \times 3^2 \times 7$. A partir de eso, resolver la ecuación

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

es equivalente a resolver el sistema

$$\begin{cases} x \equiv 70^{151} \pmod{9} \\ x \equiv 70^{151} \pmod{28} \end{cases}$$

Es fácil ver que la segunda ecuación es igual a $x \equiv 0 \pmod{28}$ debido a que $70 \equiv 14 \pmod{28}$ y $14^2 \equiv 0 \pmod{28}$. Por otro lado $\phi(9) = 6$, $70 \equiv 7 \pmod{9}$ y $151 = 6 \times 25 + 1$. Por lo tanto la primera ecuación es igual a $x \equiv 7 \pmod{9}$. Por lo tanto el sistema anterior es equivalente a resolver

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

Para resolver ese sistema, que sabemos que tiene solución por el Teorema Chino del resto, podemos resolver la ecuación diofántica

$$28n - 9m = 7$$

Es fácil ver que $(7, 21)$ es una solución, por lo que toda solución del sistema va a ser de la forma $x \equiv 196 \pmod{252}$. Finalmente deducimos que el resto de dividir 70^{151} entre 252 es 196.