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

Matemática Discreta 2
Curso segundo semestre 2024

PRIMER PARCIAL - 23 SETIEMBRE 2024.

Cédula de identidad	APELLIDO, Nombre	Número de lista

Ejercicio 1. (15 puntos)

1) Sean a y $b \in \mathbb{Z}$ enteros y d su máximo común divisor. Probar que si $d \mid c$ entonces la ecuación $ax + by = c$ tiene solución en el conjunto de los enteros $\mathbb{Z}$.

2) Probar o refutar con un contraejemplo la siguiente afirmación: "Si existe una solución a la ecuación $ax + by = c$ en el conjunto de lo enteros $\mathbb{Z}$ entonces $d \mid c$, siendo d el máximo común divisor de a y b".

3) Si (x_0, y_0) y (x_1, y_1) son soluciones de la ecuación $ax + by = c$, demostrar que $x_1 = x_0 + \frac{nb}{d}$ y $y_1 = y_0 + \frac{-na}{d}$ para algún $n \in \mathbb{Z}$, siendo d el máximo común divisor de a y b.

4) Probar que la ecuación $21x + 14y = 64$ no tiene solución o hallar una solución usando el método del algoritmo de Euclides extendido.

Solución: 1), 2) y 3) Teorema 1.5.3. notas. Pueden usar igualdad de Bézout sin demostrarla. En el item 4) $\mathrm{mcd}(21, 14) = 7$ no divide a 64 por lo que no hay solución por el contrarrecíproco de la parte 2).

Ejercicio 2. (10 puntos)

1) Mediante el algoritmo de Euclides extendido determinar $\mathrm{mcd}(210, 11)$ y hallar x e y que cumplan:

$$210x - 11y = \mathrm{mcd}(210, 11)$$

2) Determine $x \in \mathbb{Z}$ tal que $0 < x < 3000$, sea múltiplo de 11 y que tenga resto 1 cuando se lo divide separadamente por 2, 3, 5, y 7.

Solución:

1) Se cumple $210 = (-19)(-11)+1$; $-11 = (-11)\cdot 1+0$ por lo que $\mathrm{mcd}(210, 11) = 1$ y $210+19(-11) = 1$.

2) El problema se traduce en resolver el siguiente sistema: $\begin{cases} x \equiv 1 \ (\mathrm{mód}\ 2) \\ x \equiv 1 \ (\mathrm{mód}\ 3) \\ x \equiv 1 \ (\mathrm{mód}\ 5) \\ x \equiv 1 \ (\mathrm{mód}\ 7) \\ x \equiv 0 \ (\mathrm{mód}\ 11). \end{cases}$

en donde las primeras cuatro ecuaciones son equivalentes a $x \equiv 1 \ (\mathrm{mód}\ 2 \cdot 3 \cdot 5 \cdot 7)$ por lo que el sistema deviene: $\begin{cases} x \equiv 1 \ (\mathrm{mód}\ 210) \\ x \equiv 0 \ (\mathrm{mód}\ 11). \end{cases}$ Dado que $2 \cdot 3 \cdot 5 \cdot 7 = 210$. Para resolver este último sistema considero el teorema Chino del resto y por la parte $1)$ del ejercicio en donde obtengo una solución particular de la ecuación: $210x - 11y = -1$ (multiplicando por (-1)) me da equivalente a $x \equiv 1 + 210(-1) = -209 \equiv 2101 \ (\mathrm{mód}\ 210 \cdot 11)$. Es decir, $x \equiv 2101 \ (\mathrm{mód}\ 2310)$ y la solución es 2101.

Ejercicio 3. (15 puntos)

1) Definir la función φ de Euler.

2) Sean $m, n \in \mathbb{Z}^+$ coprimos. Consideramos los conjuntos $A = \{a \in \{0, \cdots, m-1\} : \text{mcd}(a, m) = 1\}$, $B = \{b \in \{0, \cdots, n-1\} : \text{mcd}(b, n) = 1\}$ y $C = \{c \in \{0, \cdots, mn-1\} : \text{mcd}(c, mn) = 1\}$, Construir una función biyectiva $f : C \to A \times B$ y concluir que $\varphi(mn) = \varphi(m)\varphi(n)$.

3) Enunciar el teorema de Euler.

4) Hallar el resto de dividir 195^{123} entre 140.

Solución: 1) Definición 2.6.1. notas. 2) Teorema 2.6.3. notas 3) Teorema 2.6.5 notas.

4) Buscamos r tal que $195^{123} \equiv r \pmod{140}$ y $0 \leq r \leq 139$

Como $195 = 140 + 55$, tenemos que $195^{123} \equiv r \pmod{140} \iff 55^{123} \equiv r \pmod{140}$, y, por el Teorema Chino del Resto, esto es equivalente a

$$\begin{cases} 55^{123} \equiv r \pmod{4} \\ 55^{123} \equiv r \pmod{5} \\ 55^{123} \equiv r \pmod{7} \end{cases}$$

Vamos a simplificar cada ecuación por separado.

- Dado que el resto al dividir 55 entre 4 es 3, tenemos que $55^{123} \equiv 3^{123} \pmod{4}$. Luego, como 4 y 3 son coprimos, podemos aplicar el teorema de Euler y obtenemos que $3^{\varphi(4)} \equiv 3^2 \equiv 1 \pmod{4}$. Además, como $123 = 2 \times 61 + 1$, tenemos que

  $$3^{123} \equiv (3^2)^{61}3 \equiv 3 \pmod{4}$$

  Entonces, la primera ecuación es equivalente a $r \equiv 3 \pmod{4}$.
- Dado que 55 es múltiplo de 5, tenemos que $55^{123} \equiv 0 \pmod{5}$ y, por lo tanto, la segunda ecuación del sistema es equivalente a $r \equiv 0 \pmod{5}$.
- Dado que el resto al dividir 55 entre 7 es 6, tenemos que $55^{123} \equiv 6^{123} \pmod{7}$. Luego, como 7 y 6 son coprimos, podemos aplicar el teorema de Euler y obtenemos que $6^{\varphi(7)} \equiv 6^6 \equiv 1 \pmod{7}$. Además, como $123 = 6 \times 20 + 3$, tenemos que

  $$6^{123} \equiv (6^6)^{20}6^3 \equiv 6^2 6 \equiv 6 \pmod{7}$$

  Entonces, la ecuación es equivalente a $r \equiv 6 \pmod{7}$.

Luego, tenemos que resolver el sistema

$$\begin{cases} r \equiv 3 \pmod{4} \\ r \equiv 0 \pmod{5} \\ r \equiv 6 \pmod{7} \end{cases}$$

Se tiene que 15 es solución particular de la primera y segunda ecuación. Entonces, por el Teorema Chino del resto obtenemos

$$\begin{cases} r \equiv 3 \pmod{4} \\ r \equiv 0 \pmod{5} \\ r \equiv 6 \pmod{7} \end{cases} \iff \begin{cases} r \equiv 15 \pmod{20} \\ r \equiv 6 \pmod{7} \end{cases}$$

Luego, como 55 es solución particular de este nuevo sistema concluímos, por el Teorema Chino del Resto, que

$$\begin{cases} r \equiv 15 \pmod{20} \\ r \equiv 6 \pmod{7} \end{cases} \iff \{ \ r \equiv 55 \pmod{140}$$

Obtuvimos, entonces que el resto de dividir 195^{123} entre 140 es 55.