Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería **Curso primer semestre 2025**
Instituto de Matemática y Estadística

PRIMER PARCIAL - 5 DE MAYO 2025.

Cédula de identidad	APELLIDO, Nombre	Número de lista

Ejercicio 1. (14 puntos)

1) Defina máximo común divisor entre dos enteros a y b.

2) Sean a y $b \in \mathbb{Z}$ con $a, b \neq 0$. Probar que $\mathrm{mcd}(a,b) = \min\{s > 0 : s = ax + by, x, y \in \mathbb{Z}\}$.

3) Sean a, b y $c \in \mathbb{Z}$ tal que $\mathrm{mcd}(a,b) = 1$. Probar que si $a \mid bc$ entonces $a \mid c$.

4) Hallar coeficientes de Bézout del máximo común divisor de 15 y 20 que sumados den 10. Es decir, hallar x_0, y_0, tal que $\mathrm{mcd}(15,20) = 15x_0 + 20y_0$ con $x_0 + y_0 = 10$. Justificar la respuesta.

Solución:

1) Ver Definición 1.2.4.

2) Ver Teorema 1.2.8.

3) Ver Lema 1.2.10.

4) Aplicando el método de Euclides vemos que una solución particular a la ecuación $5 = 15x + 20y$ es $x = -1$ e $y = 1$ por lo que la solución general viene dada por $\{(-1 + 4z, 1 + (-3)z) : z \in \mathbb{Z}$, por lo que $-1 + 4z + 1 + (-3)z = 10$ implica $z = 10$ y $x_0 = 39$, $y_0 = -29$.

Ejercicio 2. (12 puntos)

1) Sean $a, n \in \mathbb{Z}$ con $n > 0$. Probar que a es invertible módulo n, es decir, existe $x \in \mathbb{Z}$ tal que $ax \equiv 1 \pmod{n}$ si y sólo si $\mathrm{mcd}(a,n) = 1$.

2) Encontrar un inverso de 3 módulo 7.

3) Probar el siguiente criterio de divisibilidad por 7 para números de tres cifras: Un número abc escrito en base 10 es múltiplo de 7 si y sólo si $ab - 2 \cdot c$ es múltiplo de 7. Ejemplo: 343 es múltiplo de 7 ya que $34 - 2 \cdot 3 = 28$ y 28 es múltiplo de 7.

Solución:

1) Ver Corolario 2.4.5.

2) Es fácil ver que $3 \cdot 5 \equiv 15 \equiv 1 \pmod{7}$.

3) Probar que es múltiplo de 7 es equivalente a probar que es congruente con 0 módulo 7.

$$\begin{aligned} abc &\equiv a \cdot 100 + b \cdot 10 + c \pmod{7} \\ &\equiv 10 \cdot (a \cdot 10 + b) + c \pmod{7} \\ &\equiv 3 \cdot (a \cdot 10 + b) + c \pmod{7}. \end{aligned}$$

Luego, multiplicando por -2 a ambos lados, tenemos:

$$\begin{aligned} & 3 \cdot (a \cdot 10 + b) + c \equiv 0 \pmod 7 \\ \iff & a \cdot 10 + b - 2 \cdot c \equiv 0 \pmod 7 \\ \iff & ab - 2 \cdot c \equiv 0 \pmod 7. \end{aligned}$$

Otra forma: $abc = 10 \cdot ab + c \equiv 0 \pmod 7 \iff c \equiv -10 \cdot ab \pmod 7$. Por otro lado, $ab - 2 \cdot c \equiv ab - 2(-10 \cdot ab) \equiv ab + 20 \cdot ab \equiv 21 \cdot ab \equiv 0 \pmod 7$. Reciprocamente, $ab - 2 \cdot c \equiv 0 \pmod 7$ implica $10 \cdot ab - 20 \cdot c \equiv 0 \pmod 7$ es decir, $10 \cdot ab + c \equiv 0 \pmod 7$, es decir $abc \equiv 0 \pmod 7$.

Ejercicio 3. (14 puntos)

1) Enunciar y demostrar el Teorema Chino del Resto.

2) Resolver el siguiente sistema de congruencias: $\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 6 \\ 5x \equiv 1 \pmod 7. \end{cases}$

Solución:

1) Ver Teorema 2.5.1.

2) Resolvamos primero $\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 6. \end{cases}$. Como son coprimos los parámetros modulares, se transforma en la diofántica $5s - 6t = 1$ que tiene solución particular evidente $(-1, -1)$. Por lo que nos quedaria $x = 1 - 5 + 30K = -4 + 30k$ con $k \in \mathbb{Z}$, es decir, $x \equiv -4 \pmod{30}$, esto es $x \equiv 26 \pmod{30}$. Nos queda entonces resolver $\begin{cases} x \equiv 26 \pmod{30} \\ 5x \equiv 1 \pmod 7. \end{cases}$ Simplificamos el sistema multiplicandolo por el inverso módulo 7 ($5 \cdot 3 \equiv 1 \pmod 7$) y obtenemos $\begin{cases} x \equiv 26 \pmod{30} \\ x \equiv 3 \pmod 7. \end{cases}$ Finalmente volvemos a una diofántica: $30s - 7t = 3 - 26 = -23$ con solución particular evidente $(-1, -1)$ por lo que $x = 30(-1 + 7k) + 26 = -4 + 210k$ con $k \in \mathbb{Z}$. Esto es, $x \equiv -4 \pmod{210}$, es decir $x \equiv 206 \pmod{210}$.

Otra forma:

$$\begin{cases} x \equiv 1 \pmod 5, \\ x \equiv 2 \pmod 6 \\ 5x \equiv 1 \pmod 7. \end{cases}$$

De la última ecuación tenemos que x es un inverso de 5 módulo 7, o sea que $x = 3 + 7K$, sustituyendo en la segunda obtenemos

$$3 + 7K \equiv 2 \pmod 6 \iff K \equiv -1 \pmod 6$$

de modo que $K = -1 + 6H$, de donde $x = 3 + 7(-1 + 6H) = -4 + 42H$. Sustituyendo en la primer ecuación obtenemos

$$-4 + 42H \equiv 1 \pmod 5 \iff 2H \equiv 0 \pmod 5 \iff H \equiv 0 \pmod 5$$

de donde $H = 5L$ y $x = -4 + 42 \cdot 5L = -4 + 210L$.