PRIMER PARCIAL.

Ejercicio 1. (15 puntos)

a. (2 puntos) Defina máximo comun divisor entre dos enteros a y b.

b. (4 puntos) Mediante el algoritmo de Euclides extendido obtener el máximo comun divisor de 90 y 25 y coeficientes de Bézout x_0 y_0 tales que $\operatorname{mcd}(90, 25) = 90\, x_0 + 25\, y_0$.

c. (6 puntos) Dados a y $b \in \mathbb{Z}$, con $a, b \neq 0$ demostrar que $\operatorname{mcd}(a, b) = \operatorname{mcd}(b, a - bx)$ para todo $x \in \mathbb{Z}$. En caso de usar propiedades auxiliares se las debe enunciar claramente.

d. (3 puntos) Calcule $\operatorname{mcd}(12k + 7, 6k + 3)$ para todo $k \in \mathbb{Z}$.

Solución:

a. Ver notas Definición 1.2.4.

b. Efectuamos el algoritmo:

$$90 = 3 \cdot 25 + 15$$

$$25 = 1 \cdot 15 + 10$$

$$15 = 1 \cdot 10 + 5$$

$$10 = 2 \cdot 5 + 0$$

Por lo que se desprende que el $\operatorname{mcd}(90, 25) = 5$. Además:

$$5 = 15 - 1 \cdot 10 = 15 - 1 \cdot (25 - 1 \cdot 15) = 2 \cdot 15 - 1 \cdot 25 = 2(90 - 3 \cdot 25) - 1 \cdot 25 = 2 \cdot 90 - 7 \cdot 25$$

es decir, $x_0 = 2$ y $y_0 = -7$.

c. Ver notas Proposición 1.2.6.

d. Si efectuamos la división entera de $12k + 7$ entre $6k + 3$ obtenemos

$$12k + 7 = (6k + 3) \cdot 2 + 1$$

por lo que $\operatorname{mcd}(12k + 7, 6k + 3) = \operatorname{mcd}(6k + 3, 12k + 7 - (6k + 3) \cdot 2) = \operatorname{mcd}(6k + 3, 1) = 1$ para todo $k \in \mathbb{Z}$ (ver parte c, con $a = 12k + 7$, $b = 6k + 3$ y $x = 2$).

Ejercicio 2. (10 puntos) Resuelva el siguiente sistema de congruencias: $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 7 \\ x \equiv 4 \pmod{11}. \end{cases}$

Solución:

Al ser los módulos coprimos dos a dos, el Teorema chino del resto permite afirmar que el sistema tiene solución, y que esta es única módulo $3 \cdot 7 \cdot 11 = 231$.

Tenemos por las dos primeras ecuaciones que $x - 1 = 3s$ y $x - 2 = 7t$ con $s, t \in \mathbb{Z}$. Por lo que como $\operatorname{mcd}(3, 7) = 1$ tiene solución. Se cumple $3s + 1 = 7t + 2$ por lo que tenemos que resolver $3s + (-7)t = 1$. Una solución particular es evidente: $3(-2) + (-7)(-1) = 1$ por lo que el conjunto de soluciones es

$S = \{(-2+7k, -1+3k) : k \in \mathbb{Z}\}$ de esa forma $x = 3(-2+7k)+1 = -5+21k$ es decir $x \equiv -5 \pmod{21}$.

Ahora, lo resuelvo respecto a la última ecuación y me da: $x = 21s-5$ y $x = 11t+4$ es decir $21s-5 = 11t+4$, es decir, tengo que resolver la diofántica: $21s - 11t = 9$. La solución particular no es tan evidente por lo que empleamos el algoritmo de Euclides y nos da soluciones particulares $s_0 = -9$ y $t_0 = -18$. (esto último porque $1 = 10 - 9\cdot 1 = 10 - (-11 + 2\cdot 10) = -(21-11)+11 = -21 + 2\cdot 11$ entonces $21(-9) - 11(-18) = 9$).

De donde nos queda $x = 21s - 5 = 21(-9+11z) - 5 = -194 + 231z$ con $z \in \mathbb{Z}$. Es decir, $x \equiv 37 \pmod{231}$ siendo $231 = 3 \cdot 7 \cdot 11$.

Ejercicio 3. (15 puntos)

a. (6 puntos) Defina la función de Euler $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$y demuestre que $\varphi(p^n) = p^n - p^{n-1}$, para todo p primo y $n \in \mathbb{Z}^+$.

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

c. (2 puntos) Calcule $\varphi(162)$.

Solución:

a. Ver notas Definición 2.6.1 y Ejemplos 2.6.2.

b. Ver notas Teorema 2.6.3.

c. Usando lo anterior tenemos:

$$\varphi(162) = \varphi(3^4 \cdot 2) = \varphi(3^4)\varphi(2) = (3^4 - 3^{4-1})(2-1) = 81 - 27 = 54$$

o bien

$$\varphi(162) = 162 \cdot (1 - \frac{1}{3})(1 - \frac{1}{2}) = 162 \cdot \frac{2}{3} \cdot \frac{1}{2} = \frac{162}{3} = 54.$$