Capítulo 23

A. Resolviendo Congruencias Simples

1.

a) $60x \equiv 12 \pmod{24}$.

$$m = \frac{22}{\gcd(60,24)} = \frac{22}{12} = 2$$

b) $42x \equiv 24 \pmod{30}$

$$m = \frac{30}{\gcd(42,30)} = \frac{30}{6} = 5$$

c) $49x \equiv 30 \pmod{25}$

$$m = \frac{25}{\gcd(49,25)} = \frac{25}{1} = 25$$

d) $39x \equiv 14 \pmod{52}$

$$\text{No tiene solución, ya que: } \gcd(39,52) = 13, \text{ pero } 13 \nmid 14$$

e) $147x \equiv 47 \pmod{98}$

$$\text{No tiene solución, ya que: } \gcd(98,147) = 7, \text{ pero } 7 \nmid 47$$

f) $39x \equiv 26 \pmod{52}$

$$m = \frac{26}{\gcd(39,52)} = \frac{26}{13} = 2$$

2.

a) $12x \equiv 7 \pmod{25}$
La ecuación no se puede reducir ya que $\gcd(12,25) = 1$. $x \equiv 11 \pmod{25}$

b) $35x \equiv 8 \pmod{12}$.
La ecuación no se puede reducir ya que $\gcd(35,12) = 1$. $x \equiv 4 \pmod{12}$

c) $15x \equiv 9 \pmod{6}$
Como $\gcd(15,6) = 3$, la ecuación se reduce a $5x \equiv 3 \pmod{2}$. $x \equiv 1 \pmod{2}$

d) $42x \equiv 12 \pmod{30}$
Como $\gcd(42,30) = 6$, la ecuación se reduce a $7x \equiv 2 \pmod{5}$. $x \equiv 1 \pmod{5}$

e) $147x \equiv 49 \pmod{98}$
Como $\gcd(39,52) = 12 \Longrightarrow 3x \equiv 2 \pmod{4}$. $x \equiv 2 \pmod{4}$

f) $39x \equiv 25 \pmod{52}$
Como $\gcd(39,52) = 13 \Longrightarrow 3x \equiv 2 \pmod{4}$. $x \equiv 2 \pmod{4}$

3.
a) Explicar por qué $2x^2 \equiv 8 \pmod{10}$ posee las mismas soluciones que $x^2 \equiv 4 \pmod{5}$.

Por teorema, existe una solución módulo m. En donde $m = 10/\gcd(2,10) = 10/2 = 5$. Con esto, la ecuación se puede reducir a $x^2 \equiv 4 \pmod{5}$.

b) Explicar por qué $x \equiv 2 \pmod{5}$ y $x \equiv 3 \pmod{5}$ son todas las soluciones de $2x^2 \equiv 8 \pmod{10}$

$$\gcd(2,10) = 2 \Longrightarrow x^2 \equiv 4 \pmod{5} \Longleftrightarrow x^2 - 4 \equiv 0 \pmod{5} \Longleftrightarrow (x-2)(x+2) \equiv 0 \pmod{5}$$
$$\Longrightarrow x \equiv 2 \pmod{5} \text{ o } x \equiv 3 \pmod{5}$$

4. Resolver las siguientes congruencias cuadráticas

a) $6x^2 \equiv 9 \pmod{12}$.

$\gcd(6,15) = 3 \Longrightarrow 2x^2 \equiv 3 \pmod{5} \Longrightarrow x^2 \equiv 4 \pmod{5} \Longleftrightarrow (x+2)(x-2) \equiv 0 \pmod{5} \Longrightarrow x \equiv 2 \pmod{5}$ o $x \equiv 3 \pmod{5}$

b) $60x^2 \equiv 18 \pmod{24}$

$\gcd(60,18) = 6 \Longrightarrow 10x^2 \equiv 3 \pmod{4}$. La ecuación reducida no tiene solución ya que $\gcd(10,4) \nmid 3$

c) $30x^2 \equiv 18 \pmod{24}$

$\gcd(30,24) = 6 \Longrightarrow 5x^2 \equiv 3 \pmod{4} \Longrightarrow x^2 \equiv 3 \pmod{4}$. Esta ecuación no tiene soluciones en $\mathbb{Z}_4$

d) $4(x+1)^2 \equiv 14 \pmod{10}$

$\gcd(4,10) = 2 \Longrightarrow 2(x+1)^2 \equiv 7 \pmod{5} \Longleftrightarrow (x+1)^2 \equiv 1 \pmod{5} \Longleftrightarrow (x+1-1) \equiv 0 \pmod{5}$ o $(x+1+1) \equiv 0 \pmod{5} \Longrightarrow x \equiv 0 \pmod{5}$ o $x \equiv 3 \pmod{5}$

e) $4x^2 - 2x - 2 \equiv 0 \pmod{6}$

La ecuación es equivalente a $4x^2 + 4x + 4 \equiv 0 \pmod{6} \Longleftrightarrow 4(x^2 + x + 1) \equiv 0 \pmod{6} \Longleftrightarrow 2(x^2 + x + 1) \equiv 0 \pmod{3} \Longrightarrow x^2 + x + 1 \equiv 0 \pmod{3} \Longrightarrow x \equiv 1 \pmod{3}$

f) $3x^2 - 6x + 6 \equiv 0 \pmod{15}$

$3(x^2 - 2x + 2) \equiv 0 \pmod{15} \Longleftrightarrow 3(x^2 - 2x + 1 - 1 + 2) \equiv 0 \pmod{15} \Longleftrightarrow 3\big((x-1)^2 + 1\big) \equiv 0 \pmod{15} \Longleftrightarrow 3(x-1)^2 \equiv 12 \pmod{15} \longrightarrow (x-1)^2 \equiv 4 \pmod{5} \Longleftrightarrow x + 1 \equiv 0 \pmod{5}$ o $x - 3 \equiv 0 \pmod{5}$

$$x \equiv 4 \pmod{5} \text{ o } x \equiv 3 \pmod{5}$$

5. Resolver las siguientes congruencias

a) $x^4 \equiv 4 \pmod{6}$

Equivalente a $x^2 - 2 \equiv 0 \pmod{6}$ o $x^2 + 2 \equiv 0 \pmod{6} \Longleftrightarrow x^2 \equiv 2 \pmod{6}$ o $x^2 \equiv 4 \pmod{6}$

$x^2 \equiv 2 \pmod{6}$ no tiene solución. De la segunda ecuación se extrae que $x \equiv 2 \pmod{6}$ o $x \equiv 4 \pmod{6}$

b) $2(x-1)^4 \equiv 0 \pmod{8}$.

$\gcd(2,8) = 2 \Longrightarrow (x-1)^4 \equiv 0 \pmod{4} \Longrightarrow 2^2 \mid \big((x-1)^2\big)^2 \Longrightarrow (x-1) \equiv 0 \pmod{2} \Longleftrightarrow x \equiv 1 \pmod{2}$

c) $x^3 + 3x^2 + 3x + 1 \equiv 0 \pmod{8}$

$(x+1)^3 \equiv 0 \pmod{8} \Longrightarrow 2^3 \mid (x+1)^3 \Longrightarrow 2 \mid (x+1) \Longleftrightarrow x + 1 \equiv 0 \pmod{2} \Longleftrightarrow x \equiv 1 \pmod{2}$

d) $x^4 + 2x^2 + 1 \equiv 4 \pmod{5}$

$(x^2+1)^2 \equiv 4 \pmod{5} \Longleftrightarrow (x^2-1)(x^2+3) \equiv 0 \pmod{5} \Longleftrightarrow x^2 \equiv 1 \pmod{5}$ o $x^2 \equiv 2 \pmod{5}$

La ecuación $\bar{x}^2 = \bar{2}$ no posee solución en $\mathbb{Z}_5$. De la primera ecuación se obtiene que $x \equiv 1 \pmod 5$ o $x \equiv 4 \pmod 5$

6. Resolver las siguientes ecuaciones diofantinas (Si no tienen solución, argumentar).

a) $14x + 15y = 11$

$$14x \equiv 11 \pmod{15} \Longrightarrow x \equiv 4 \pmod{15}$$
$$15y \equiv 11 \pmod{14} \Longrightarrow x \equiv 11 \pmod{14}$$

b) $4x + 5y = 1$

$$4x \equiv 1 \pmod 5 \Longrightarrow x \equiv 4 \pmod 5$$
$$5y \equiv 1 \pmod 4 \Longrightarrow x \equiv 1 \pmod 4$$

c) $21x + 10y = 9$

$$21x \equiv 9 \pmod{10} \Longrightarrow x \equiv 9 \pmod{10}$$
$$10y \equiv 9 \pmod{21} \Longrightarrow x \equiv 3 \pmod{21}$$

d) $30x^2 + 24y = 18$

$$24y \equiv 18 \pmod{30} \Longrightarrow 4y \equiv 3 \pmod 5 \Longrightarrow x \equiv 2 \pmod 5$$
$$30x^2 \equiv 18 \pmod{24} \Longrightarrow 5x^2 \equiv 3 \pmod 4 \Longleftarrow x^2 \equiv 3 \pmod 4 \Longleftrightarrow \bar{x}^2 = \bar{3} \text{ no tiene solución en } \mathbb{Z}_4$$

C. Propiedades Elementales de Congruencias

Probar las siguientes propiedades para enteros a, b, c, d y enteros positivos m y n.

1. Si $a \equiv b \pmod n$ y $b \equiv c \pmod n$, entonces $a \equiv c \pmod n$

$nk_1 = (a - b)$ y $nk_2(b - c)$, entonces $nk_1 + nk_2 = (a - b) + (b - c) \Longrightarrow n \mid (a - c)$

2. Si $a \equiv b \pmod n$, entonces $a + c \equiv b + c \pmod n$

$nk = (a - c) \Longleftrightarrow nk = (a + c - (c + b)) \Longrightarrow a + c \equiv b + c \pmod n$

3. Si $a \equiv b \pmod n$, entonces $ac \equiv bc \pmod n$

$nk = (a - b) \Longleftrightarrow cnk = c(a - b) \Longrightarrow n \mid c(a - b) \Longrightarrow n \mid ac - bc$

4. $a \equiv b \pmod 1$

Directamente, 1 divide todo entero: $1 \mid a - b$

5. Si $ab \equiv 0 \pmod p$, donde p es primo, entonces $a \equiv 0 \pmod n$ o $b \equiv 0 \pmod n$

$p \mid ab$, por lema de Euclides $p \mid a$ o $p \mid b$, es decir $a \equiv 0 \pmod p$ o $b \equiv 0 \pmod p$

6. Si $a^2 \equiv b^2 \pmod p$, donde p es primo, entonces $a \equiv \pm b \pmod p$

$p \mid (a^2 - b^2) \Longleftrightarrow p \mid (a - b)(a + b)$, por lema de Euclides, $p \mid (a - b)$ o $p \mid (a + b)$, entonces $a \equiv \pm b \pmod p$

7. Si $a \equiv b \pmod m$m entonces $a + km \equiv b \pmod{}$

$m \mid (b - a) \Longrightarrow mk = (b - a) \Longleftrightarrow mk + a - b = 0 \Longleftrightarrow mk + a \equiv b \pmod m$

8. Si $ac \equiv bc \pmod n$ y $\gcd(c, n) = 1$, entonces $a \equiv b \pmod n$

$$ac - bc = nk$$
$$c(a - b) = kn$$

Como $\gcd c, n = 1$, entonces $n \mid (a - b)$, es decir $a \equiv b \pmod{n}$

9. Si $a \equiv b \pmod{n}$, entonces $a \equiv b \pmod{m}$, donde m es un factor de n.

$n \mid (a - b) \iff nk = (a - b) \iff mqk = (a - b) \iff m \mid (a - b) \iff a \equiv b \pmod{m}$

E. Consecuencias del Teorema de Fermat