2. Aritmética modular Ejercicios resueltos

Ejercicio 2.1 Probar, mediante congruencias, que $3^{2n+5} + 2^{4n+1}$ es divisible por 7 cualquiera que sea el entero $n \geq 1$.

SOLUCIÓN: Trabajando módulo 7 se tiene que

$$3^{2n+5} + 2^{4n+1} = 3^5 \cdot 3^{2n} + 2 \cdot 2^{4n} = 243 \cdot 9^n + 2 \cdot 16^n \equiv 5 \cdot 2^n + 2 \cdot 2^n = 7 \cdot 2^n \equiv 0$$

es decir, 7 divide a $3^{2n+5} + 2^{4n+1}$. ■

Ejercicio 2.2

a) Probar que el número inmediatamente posterior a cualquier potencia de 5 es múltiplo de 2 pero no de 4.

b) Probar, por inducción en n, que si denotamos por $p^m \parallel N$ a la **mayor** potencia del primo p que divide a N (así, por ejemplo, $2^3 \parallel 40$ ya que $2^3 = 8$ es un divisor de 40 pero $2^4 = 16$ no lo es), se verifica que $2^{n+2} \parallel 5^{2^n} - 1$ para cualquier $n \in \mathbf{Z}^+$.
Indicación: recuérdese que $a^{2k} - 1 = (a^k - 1)(a^k + 1)$.

SOLUCIÓN:

a) $\left.\begin{array}{l} 5 \equiv 1 \pmod 2 \\ 5 \equiv 1 \pmod 4 \end{array}\right\} \Longrightarrow$ para cualquier $n \in \mathbf{Z}^+$ es $\left\{\begin{array}{l} 5^n \equiv 1 \pmod 2 \\ 5^n \equiv 1 \pmod 4 \end{array}\right.$,
por lo que $\left\{\begin{array}{l} 5^n + 1 \equiv 0 \pmod 2 \\ 5^n + 1 \equiv 2 \pmod 4 \end{array}\right.$ es decir, el numero inmediatamente posterior a cualquier potencia de 5 es divisible por 2 pero no por 4.

b) Para $n = 1$ se tiene que $2^3 = 2^{1+2} \parallel 5^{2^1} - 1 = 24$.
Supongámoslo cierto para n y vamos a probarlo para $n+1$. Debemos probar que

$$2^{(n+1)+2} = 2^{n+3} \parallel 5^{2^{n+1}} - 1 = 5^{2\cdot 2^n} - 1 = (5^{2^n} - 1)(5^{2^n} + 1).$$

Dado que por hipótesis de inducción es $2^{n+2} \parallel 5^{2^n} - 1$ y además $2^1 \parallel 5^{2^n} + 1$, ya que se trata del número inmediatamente posterior a una potencia de 5, se deduce que $2^{n+3} \parallel 5^{2^{n+1}} - 1$, lo que prueba el resultado. ■

Ejercicio 2.3 Sean a, b y c tres enteros positivos tales que $a \mid b$. Si al dividir c entre a obtenemos un resto r y al dividir c entre b un resto s, ¿qué resto se obtiene de la división de s entre a?

a) Razonar el ejercicio haciendo uso del algoritmo de la divisibilidad y no de congruencias.

b) Repetirlo haciendo uso de congruencias y no del algoritmo de la divisibilidad.

SOLUCIÓN:

a) Sabemos que

$$\begin{array}{lllll} c = a \cdot q_1 + r & \text{con} & q_1 \in \mathbf{Z} & \text{y} & 0 \leq r < a \\ c = b \cdot q_2 + s & \text{con} & q_2 \in \mathbf{Z} & \text{y} & 0 \leq s < b \end{array}$$

por lo que

$$a \cdot q_1 + r = b \cdot q_2 + s \implies a \cdot q_1 - b \cdot q_2 = s - r$$

como $a \mid b$ podemos expresar b de la forma $b = a \cdot b'$ con $b' \in \mathbf{Z}$ y, por tanto

$$s - r = a \cdot q_1 - a \cdot b' \cdot q_2 = a \cdot (q_1 - b' \cdot q_2) = a \cdot q \quad \text{con} \quad q = q_1 - b' \cdot q_2 \in \mathbf{Z}$$

es decir, $s = a \cdot q + r$ con $0 \leq r < a$, por lo que el resto de dividir s entre a es también r.

b) Sabemos que $\begin{cases} c \equiv r \pmod{a} \\ c \equiv s \pmod{b} \end{cases}$

De la segunda ecuación tenemos que $c = s + bt$ con $t \in \mathbf{Z}$, que llevada a la primera nos da

$$s + bt \equiv r \pmod{a}$$

como, por otra parte $a \mid b$ se tiene que $b \equiv 0 \pmod{a}$, por lo que la ecuación anterior se reduce a

$$s \equiv r \pmod{a}$$

es decir, el resto de dividir s entre a es r. (Obsérvese que $0 \leq r < a$ por tratarse del resto de la división de c entre a). ■

Ejercicio 2.4 ¿Puede conocerse un entero positivo sabiendo que es menor que 100 y conociendo los restos de sus divisiones entre 3, 5 y 7?

SOLUCIÓN: Basta con resolver el sistema de congruencias

$$x \equiv a \pmod{3} \quad x \equiv b \pmod{5} \quad x \equiv c \pmod{7}$$

que tiene solución única en $\mathbf{Z}_{105}$.
Procediendo como en los ejercicios anteriores, la solución general viene dada por $x = -35a + 21b + 15c + 105t$ con $t \in \mathbf{Z}$. De entre todas las soluciones nos quedaremos con la que se encuentra en el rango $1 \leq x \leq 100$. Así, por ejemplo, si los restos son 2, 2 y 5 respectivamente, $x = -70+42+75+105t = 47+105t$, por lo que el número buscado es 47. ■

Ejercicio 2.5 Dado el sistema:

$$\begin{cases} x \equiv 4 \pmod{8} \\ x \equiv a \pmod{6} \\ x \equiv -1 \pmod{15} \end{cases}$$

a) Determinar todos los posibles valores del parámetro $a \in \mathbf{Z}$ que hacen que el sistema tenga solución.

b) Probar que la solución del sistema, en caso de tener solución, es independiente del parámetro a.

c) Resolver el sistema en los casos en que tiene solución.

SOLUCIÓN:

a) Las condiciones que se deben cumplir para que el sistema tenga solución son:

$$\text{mcd}\,(8,6) = 2 \,|\, (4-a) \Longrightarrow 2 \,|\, a \Longrightarrow a \equiv 0 \pmod 2$$
$$\text{mcd}\,(6,15) = 3 \,|\, (a+1) \Longrightarrow a+1 \equiv 0 \pmod 3 \Longrightarrow a \equiv 2 \pmod 3$$

De la segunda ecuación se obtiene que $a = 2+3u$, que llevada a la primera nos da $2+3u \equiv 0 \pmod 2 \iff u \equiv 0 \pmod 2$, es decir, $u = 2t$.
La solución del sistema vendrá dada por $a = 2+3(2t) = 2+6t$ cualquiera que sea $t \in \mathbf{Z}$. Así pues, el sistema tiene solución siempre que $a = 2+6t$ con $t \in \mathbf{Z}$.

b) Teniendo en cuenta que, para cualquier valor de parámetro $a = 2+6t$ que hace que el sistema tenga solución, la segunda ecuación se convierte en $x \equiv 2+6t \pmod 6$ que es equivalente a $x \equiv 2 \pmod 6$, dicha solución es independiente del valor del parámetro $a = 2+6t$.

c) El sistema ha quedado de la forma

$$x \equiv 4 \pmod 8 \quad x \equiv 2 \pmod 6 \quad x \equiv -1 \pmod{15}$$

equivalente a

$$\begin{array}{lll} x \equiv 4 \pmod{2^3} & x \equiv 2 \pmod 2 & x \equiv -1 \pmod 3 \\ & x \equiv 2 \pmod 3 & x \equiv -1 \pmod 5 \end{array}$$

y como sabemos que tiene solución, vuelve a ser equivalente a

$$x \equiv 4 \pmod{2^3} \quad x \equiv 2 \pmod 3 \quad x \equiv -1 \pmod 5$$

o lo que es lo mismo

$$x \equiv 4 \pmod 8 \quad x \equiv 2 \pmod 3 \quad x \equiv 4 \pmod 5$$

De la primera se obtiene que $x = 4+8u$, que llevada a la tercera nos queda

$$4+8u \equiv 4 \pmod 5 \iff 3u \equiv 0 \pmod 5 \iff u \equiv 0 \pmod 5$$

es decir, $u = 5v \Longrightarrow x = 4+8(5v) = 4+40v$.

Obligando ahora a que cumpla la segunda:

$$4+40v \equiv 2 \pmod 3 \iff v \equiv 1 \pmod 3$$

de donde $v = 1+3t$ y, por tanto $x = 4+40(1+3t) = 44+120t$.

La solución es, por tanto $x = 44+120t$ cualquiera que sea $t \in \mathbf{Z}$. ■

Ejercicio 2.6 Determinar los dígitos x e y del número $n = 59x7y8$ sabiendo que es divisible por 123.

SOLUCIÓN: Al ser divisible por 123 sabemos que

$$59x7y8 \equiv 0 \pmod{123} \implies 590708 + 1000x + 10y \equiv 0 \pmod{123}$$

es decir

$$62 + 16x + 10y \equiv 0 \pmod{123} \iff 31 + 8x + 5y \equiv 0 \pmod{123}$$

ya que 2 es primo con 123.

Por otra parte, dado que $0 \leq x, y \leq 9$ sabemos que

$$31 \leq 31 + 8x + 5y \leq 148$$

Como el único múltiplo de 123 que existe en dicho intervalo es el propio 123, se tiene que

$$31 + 8x + 5y = 123 \iff 8x + 5y = 92$$

Al ser $\text{mcd}\,(8, 5) = 1 = 8 \cdot 2 + 5 \cdot (-3)$, la ecuación tiene solución, siendo una solución particular

$$x_0 = 2 \cdot 92 = 184 \quad \text{y} \quad y_0 = -3 \cdot 92 = -276$$

La solución general viene dada por

$$\left.\begin{array}{l} x = 184 + 5t \\ y = -276 - 8t \end{array}\right\} \quad \forall\, t \in \mathbf{Z}$$

Como $0 \leq y \leq 9$ se tiene que

$$0 \leq -276 - 8t \leq 9 \iff 276 \leq -8t \leq 285$$

es decir

$$34'5 \leq -t \leq 35'625 \iff -35'625 \leq t \leq -34'5$$

siendo -35 el único número entero de dicho intervalo, por lo que $t = -35$, obteniéndose que

$$x = 9, \quad y = 4 \quad \text{y} \quad n = 599748 = 123 \cdot 4876$$ ■

Ejercicio 2.7 Juan saca a pasear a su perro cada 6 horas y Pedro cada 10. Si Juan lo ha sacado a las 8 de la mañana y Pedro a las 12,

a) ¿Cuál es la última hora de la mañana a la que puede sacar su perro Luis si quiere sacarlo cada 15 horas y no coincidir nunca ni con Juan ni con Pedro?

b) ¿A qué hora de la tarde debería sacarlo si quisiera coincidir con ambos? y ¿cuándo coincidirían?

SOLUCIÓN:

a) Los datos que nos dan para Juan y Pedro se traducen en

$$\begin{aligned} x &\equiv 8 \pmod 6 \iff x \equiv 2 \pmod 6 \\ x &\equiv 12 \pmod{10} \iff x \equiv 2 \pmod{10} \end{aligned}$$

La ecuación para Luis es $x \equiv a \pmod{15}$ y debe resultar incompatible con las dos anteriores.

Para ser incompatible con la de Juan $\operatorname{mcd}(15,6) = 3$ no debe dividir a $a-2$ y para ser incompatible con la de Pedro, $\operatorname{mcd}(15,10) = 5$ tampoco debe dividir a $a-2$.

Si lo sacase a las 12 ($a = 12$) no resultaría incompatible con la de Pedro y si lo hiciese a las 11 no lo sería con la de Juan, por lo que la última hora de la mañana a la que deberá sacar al perro son las 10 ya que 3 no divide a $10-2=8$ y 5 tampoco divide a 8, por lo que nunca coincidiría ni con Juan ni con Pedro.

b) Para que con $12 < a \leq 24$ resulte que $a-2$ sea divisible por 3 y por 5 ha de ser $a-2=15$ es decir, $a=17$, por lo que si lo saca a las 5 de la tarde habrá un momento en el que coincidan los tres.

El sistema quedaría entonces

$$\left.\begin{aligned} x &\equiv 8 \pmod 6 \iff x \equiv 2 \pmod 6 \\ x &\equiv 12 \pmod{10} \iff x \equiv 2 \pmod{10} \\ x &\equiv 17 \pmod{15} \iff x \equiv 2 \pmod{15} \end{aligned}\right\} \implies x \equiv 2 \pmod{30}$$

por lo que coincidirían, por primera vez a las 32 horas, es decir, mañana a las 8 de la mañana y volverían a hacerlo cada 30 horas. ■

Ejercicio 2.8 Para todo $n \in \mathbf{N}$, sea $A_n = 2^n + 4^n + 8^n$.

a) Probar que si $n \equiv m \pmod 3$ entonces $A_n \equiv A_m \pmod 7$.

b) Probar, sin hallar su expresión decimal, que el número cuya expresión en binario viene dada por 1000100010000, es divisible entre 7.

SOLUCIÓN:

a) Supongamos, sin pérdida de generalidad que $m > n$. Si $n \equiv m \pmod 3$ es $m = n + 3p$ con $p \in \mathbf{N}$. Entonces:

$$\begin{aligned} A_m - A_n &= 2^{n+3p} + 4^{n+3p} + 8^{n+3p} - 2^n - 4^n - 8^n = \\ &= 2^n(8^p - 1) + 4^n(8^{2p} - 1) + 8^n(8^{3p} - 1) \end{aligned}$$

Como $x^p - 1$ es divisible entre $x - 1$ cualquiera que sea $p \in \mathbf{N}$,

$$8^p - 1,\ 8^{2p} - 1 \text{ y } 8^{3p} - 1 \text{ son divisibles entre } 8 - 1 = 7$$

por lo que $A_m - A_n = \overset{\bullet}{7}$ y por tanto $A_n \equiv A_m \pmod 7$.

b) El número cuya expresión en binario es 1000100010000 es en sistema decimal $2^4 + 2^8 + 2^{12} = 2^4 + 4^4 + 8^4 = A_4$ y como $4 \equiv 1 \pmod 3$ se verifica que $A_4 \equiv A_1 \pmod 7$.

Como $A_1 = 2 + 4 + 8 = 14 = \overset{\bullet}{7}$, se verifica que A_4 es divisible por 7. ■

Ejercicio 2.9 Hallar tres números primos p_1, p_2 y p_3, con

$$5 < p_1 < p_2 < p_3 < 37$$

tales que $n = p_1 \cdot p_2 \cdot p_3$ y $m = 37 \cdot p_1 \cdot p_2 \cdot p_3$ sean números de Carmichael.

SOLUCIÓN: Al ser $p_1 < p_2 < p_3 < 37$ ambos números son libres de cuadrados, por lo que serán de Carmichael si

$$\begin{aligned} &n \equiv 1 \pmod{(p_1 - 1)} \\ &n \equiv 1 \pmod{(p_2 - 1)} \\ &n \equiv 1 \pmod{(p_3 - 1)} \\ &m = 37n \equiv 1 \pmod{(p_1 - 1)} \\ &m = 37n \equiv 1 \pmod{(p_2 - 1)} \\ &m = 37n \equiv 1 \pmod{(p_3 - 1)} \\ &m = 37n \equiv 1 \pmod{36} \end{aligned}$$

$$\left.\begin{aligned} &n \equiv 1 \pmod{(p_1 - 1)} \\ &m = 37n \equiv 1 \pmod{(p_1 - 1)} \end{aligned}\right\} \Longrightarrow 37 \equiv 1 \pmod{(p_1 - 1)} \Longrightarrow p_1 - 1 \,|\, 36$$

$$\left.\begin{array}{l} n \equiv 1 \pmod{(p_2-1)} \\ m = 37n \equiv 1 \pmod{(p_2-1)} \end{array}\right\} \Longrightarrow 37 \equiv 1 \pmod{(p_2-1)} \Longrightarrow p_2 - 1 \,|\, 36$$

$$\left.\begin{array}{l} n \equiv 1 \pmod{(p_3-1)} \\ m = 37n \equiv 1 \pmod{(p_3-1)} \end{array}\right\} \Longrightarrow 37 \equiv 1 \pmod{(p_3-1)} \Longrightarrow p_3 - 1 \,|\, 36$$

Los divisores de 36 son: 1, 2, 3, 4, 6, 9, 12, 18 y 36 por lo que los posibles valores de p_i son 2, 3, 4, 5, 7, 10, 13, 19 y 37. Al tratarse de primos mayores que 5 y menores que 37, sólo nos queda la posibilidad de que

$$p_1 = 7, \quad p_2 = 13 \quad \text{y} \quad p_3 = 19$$

es decir:

$$n = 7 \cdot 13 \cdot 19 = 1729 \quad \text{y} \quad m = 7 \cdot 13 \cdot 19 \cdot 37 = 63973.$$

Es fácil comprobar que también se verifica la última ecuación (no utilizada)

$$37n = 37 \cdot 1729 \equiv 1729 \equiv 1 \pmod{36}.$$ ■

Ejercicio 2.10 ¿Para qué valores de n es $\phi(n) \equiv 2 \pmod 4$?

SOLUCIÓN: Sabemos que

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \Longrightarrow \phi(n) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1).$$

Dado que $\phi(n)$ es par y no es múltiplo de 4, sólo pueden darse una de las siguientes posibilidades:

a) Si n es par $\Rightarrow$
$$\begin{cases} \text{Si } n = 2^\alpha & \Rightarrow \phi(n) = 2^{\alpha-1} \Rightarrow \alpha = 2 \Rightarrow n = 2^2 = 4 \\ \text{Si } n = 2^\alpha p^\beta & \Rightarrow \phi(n) = 2^{\alpha-1} p^{\beta-1}(p-1) \\ & \Rightarrow \alpha = 1,\ p - 1 \equiv 2 \pmod 4 \\ & \Rightarrow n = 2 \cdot p^\beta \text{ con } p \text{ primo tal que p=4a+3} \end{cases}$$

b) Si n es impar $n = p^\alpha$ con p primo tal que $p = 4a + 3$. ■