Respuestas a los problemas impares del capítulo 8

Congruencias

8.1 $31 \equiv 3 \pmod{m}$ si y sólo si $m|28$ si y sólo si $m = 1,\ 2,\ 4, 7,\ 14,\ 28$.

8.3 $52 = 2^2 + 2^4 + 2^5 = 4 + 16 + 32$, por lo tanto $17^{52} = 17^4 \cdot 17^{16} \cdot 17^{32}$. Ahora bien

$$\begin{aligned} 17 &\equiv 2 \pmod{5} \\ 17^2 &\equiv 4 \pmod{5} \\ 17^4 \equiv 16 &\equiv 1 \pmod{5} \\ 17^{16} \equiv 1^4 &\equiv 1 \pmod{5} \\ 17^{32} \equiv 1^2 &\equiv 1 \pmod{5} \end{aligned}$$

Por lo tanto $17^{52} \equiv 1 \pmod{5}$.

8.5 Si $a \equiv b \pmod{m}$, entonces $m|(a-b)$. Si además $n|m$, entonces $n|(a-b)$ y por lo tanto $a \equiv b \pmod{n}$.

8.7 $a - b + c - d + d - c + b - a = 0$ es divisible entre once, por lo tanto *abcddcba* es divisible entre 11.

Calendario perpetuo

8.9

$$\begin{aligned} t &= 1900 - 1600 = 300. \\ B(1900) &= \lfloor 300/4 \rfloor - \lfloor 300/100 \rfloor + \lfloor 300/400 \rfloor = 75 - 3 + 0 = 72. \\ f(3, 1900) &= 3 + 300 + 72 = 375 \equiv 4 \pmod{7} \\ S(1, 3, 1900) &= 4 + 0 = 4 \equiv 3 \pmod{7}. \end{aligned}$$

Por lo tanto el primero de marzo de 1900 fue jueves.

8.11
1. $t = n - 1900$.
2. $B(n) = \lfloor t/4 \rfloor$.
3. $f(3,\ n) = 4 + t + B(n) \pmod{7}$.
4. $f(m, n) = f(3, n) + g(m)$.
5. $S(d, m, n) = f(m, n) + (d - 1) \pmod{7}$.

Teorema chino del residuo

8.13 *a*) $3x \equiv 2 \pmod 7$ implica que $x = 3 + 7k$, $k \in \mathbb{Z}$.
b) $17x \equiv 14 \pmod{21}$ implica que $x = 7 + 21k$, $k \in \mathbb{Z}$.

8.15 $x \equiv 4 \pmod 7$ implica que $x = 4 + 7k$. Por otra parte, $x \equiv 3 \pmod{13}$ implica que

$$(4 + 7k) \equiv 3 \pmod{13}$$

y de ahí que

$$7k \equiv -1 \pmod{13}.$$

Por lo tanto $k = 11 + 13n$, $n \in \mathbb{Z}$. En conclusión,

$$x = 4 + 7(11 + 13n) = 81 + 91n, \ n \in \mathbb{Z}.$$

8.17 $x \equiv 3 \pmod 5$ implica que $x = 3 + 5r$. Por otra parte, $x \equiv 1 \pmod 2$ implica que

$$(3 + 5r) \equiv 1 \pmod 2$$

y de ahí que

$$5r \equiv -2 \pmod 2.$$

De modo que $r = 2 + 2k$, y por lo tanto,

$$x = 3 + 5(2 + 2k) = 13 + 10k.$$

Por último, $x \equiv 2 \pmod 7$ implica que $13 + 10k \equiv 2 \pmod 7$, y de ahí que $10k \equiv -11 \equiv 3 \pmod 7$, por lo tanto $k = 1 + 7n$, y de ahí que

$$x = 13 + 10(1 + 7n) = 23 + 70n.$$

8.19 *a*) $a = 2k$ implica que $a^2 = 4k^2$, por lo tanto $a^2 \equiv 0 \pmod 4$.
b) $a = 2k + 1$ implica que $a^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, por lo tanto $a^2 \equiv 1 \pmod 4$.

8.21 $a^3 - a = a(a^2 - 1) = a(a - 1)(a + 1)$. Como $a - 1, a, a + 1$ son tres enteros consecutivos, alguno de ellos debe ser múltiplo de tres, por lo tanto $a^3 \equiv a \pmod 3$.

Aritmética modular

8.23 $[a][b] = [ab] = [ba] = [b][a]$.

8.25 $[a]([b]+[c]) = [a][b+c] = [a(b+c)] = [ab+ac] = [ab]+[ac] = [a][b]+[a][c]$.

8.27

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

8.29 $[9][x] = [1] \Leftrightarrow 9x \equiv 1 \pmod{14} \Leftrightarrow 1 = 9x + 14y$. Utilizando el algoritmo de Euclides tenemos que $1 = -3(9) + 2(14)$. Por lo tanto $[x] = [-3] = [14 - 3] = [11]$ es el inverso de $[9]$ en $\mathbb{Z}_{14}$.

8.31 Por el teorema de Euler, $5^{58} \equiv 1 \pmod{59}$, por lo tanto $[5]^{-1} = [5^{57}]$. Ahora bien, $57 = 32 + 16 + 8 + 1$. Por lo tanto $5^{57} \equiv 5^{32} \cdot 5^{16} \cdot 5^8 \cdot 5^1 \pmod{59}$. Observemos además que

$$\begin{aligned} 5 &\equiv 5 \pmod{59} \\ 5^2 &\equiv 25 \pmod{59} \\ 5^4 &\equiv 625 \equiv 35 \pmod{59} \\ 5^8 &\equiv 1225 \equiv 45 \pmod{59} \\ 5^{16} &\equiv 2025 \equiv 19 \pmod{59} \\ 5^{32} &\equiv 361 \equiv 7 \pmod{59} \end{aligned}$$

Por lo tanto $5^{57} \equiv 7 \cdot 19 \cdot 45 \cdot 5 = 29925 \equiv 12 \pmod{59}$. De ahí que $[5]^{-1} = [12]$ en $\mathbb{Z}_{59}$.

8.33 $a^2 \equiv 1 \pmod{p} \Leftrightarrow p|(a^2 - 1) \Leftrightarrow p|(a-1)(a+1)$ $\Leftrightarrow p|(a-1)$ o $p|(a+1) \Leftrightarrow a \equiv 1 \pmod{p}$ o $a \equiv -1 \pmod{p}$.

Criptografía

8.35 $AVE = 012205 = M_1M_2M_3$, donde $M_1 = 01$, $M_2 = 22$, $M_3 = 05$. Ahora bien, $C_1 = 1^5 \pmod{85} \Rightarrow C_1 = 01$; $C_2 = 22^5 \pmod{85} \Rightarrow C_2 = 82$; $C_3 = 5^5 \pmod{85} \Rightarrow C_3 = 65$. Por lo tanto $C = 018265$.

8.37 $C_1 = 70$, $C_2 = 22$, $C_3 = 01$. Necesitamos calcular primero $M_1 = 70^{31} \pmod{91}$. Con este fin observemos que $31 = 16+8+4+2+1$. Ahora bien,

$$\begin{aligned} 70 &\equiv 70 \pmod{91} \\ 70^2 &\equiv 4900 \equiv 77 \pmod{91} \\ 70^4 &\equiv 5929 \equiv 14 \pmod{91} \\ 70^8 &\equiv 196 \equiv 14 \pmod{91} \\ 70^{16} &\equiv 196 \equiv 14 \pmod{91} \end{aligned}$$

Por lo tanto

$$70^{31} \equiv (14)(14)(14)(77)(70) \equiv 21 \pmod{91},$$

de ahí que $M_1 = 21$. Análogamente, $M_2 = 22^{31} \pmod{91} \Rightarrow M_2 = 22$. $M_3 = 1^{31} \pmod{91} \Rightarrow M_3 = 01$. Por lo tanto $M = 212201$, es decir, el mensaje es UVA.