

Ejercicio 1. Hallar el menor entero positivo congruente a:

$$7^{217^{38}} \pmod{34}.$$

Solución. Primero observamos que se trata del número $7^{(217^{38})}$ módulo 34. Como $\text{mcd}(7, 34) = 1$, podemos aplicar el Teorema de Euler y proceder a reducir 217^{38} módulo $\varphi(34) = 16$. Ya que $217 \equiv 9 \pmod{16}$, consideramos $9^{38} \pmod{16}$. De nuevo, $\text{mcd}(9, 16) = 1$, pues por el mismo Teorema consideramos: $38 \equiv 6 \pmod{8}$, pues volviendo para atrás y aplicando la tesis del Teorema de Euler tenemos primero: $9^{38} \equiv 9^6 = 81^3 \equiv 1 \pmod{16}$, luego: $7^{(217^{38})} \equiv 7^{(9^{38})} \equiv 7^1 = 7 \pmod{34}$. Así que el número buscado es 7.

Ejercicio 2.

a. ¿Qué es una ecuación diofántica?

Decidir cuándo tiene solución y qué forma tiene esta cuando existe. Probar ambas propiedades.

b. ¿Qué podemos decir sobre la existencia y el número de soluciones de la ecuación de congruencia:

$$ax \equiv b \pmod{m}?$$

Justificar.

c. Hallar todas las soluciones (módulo 64) de la ecuación de congruencia:

$$28x \equiv 44 \pmod{64}.$$

Solución. Las partes **a.** (Definición 1.5.2 y Teorema 1.5.3) y **b.** (Teorema 2.4.2) son de teórico, pero la prueba de la parte **b.** se basa en el resultado de la parte **a.**, con lo cual para la prueba de la parte **b.** basta mostrar la conexión que tiene con las ecuaciones diofánticas e interpretar el resultado sobre las soluciones.

c. Dado que $\text{mcd}(28, 64) = 4 \nmid 44$, existen exactamente 4 soluciones módulo 64. Dividiendo toda la ecuación entre 4 y aplicando la regla del teórico obtenemos que es equivalente a la ecuación $7x \equiv 11 \pmod{16}$. Esto nos lleva a la ecuación diofántica $7x - 16y = 11$. Resolviéndola llegamos a que $-3 \cdot 16 + 7 \cdot 7 = 1$, luego $16(-33) + 7(77) = 11$, de donde concluimos que una solución para x es 77. Para hallar el mínimo entero positivo x que es la solución, reducimos 77 módulo 16, obteniendo 13. Luego todas las soluciones de la ecuación de congruencia inicial módulo 64 son: $x = 13 + 16k$ siendo $k = 0, 1, 2, 3$, esto es: $x \in \{13, 29, 45, 61\}$.

Ejercicio 3. Hallar todas las soluciones en \mathbb{Z} del sistema:

$$\begin{cases} 3x \equiv 10 \pmod{11} \\ 2x \equiv 7 \pmod{9} \\ x \equiv 8 \pmod{15} \\ 5x \equiv 10 \pmod{12} \\ x \equiv 18 \pmod{20}. \end{cases}$$

Solución. Para la primera, segunda y la cuarta ecuación buscamos primero los inversos de los coeficientes del lado izquierdo. Solucionando las tres ecuaciones de congruencia: $3x \equiv 1 \pmod{11}$, $2x \equiv 1 \pmod{9}$, $5x \equiv 1 \pmod{12}$ obtenemos fácilmente que los inversos respectivos son: 4, 5, 5, respectivamente. De ahí, las tres ecuaciones de congruencia iniciales se reducen a: $x \equiv 40 \equiv 7 \pmod{11}$, $x \equiv 35 \equiv 8 \pmod{9}$ y $x \equiv 50 \equiv 2 \pmod{12}$. Con eso el sistema inicial es equivalente a:

$$\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 8 \pmod{9} \\ x \equiv 8 \pmod{15} \\ x \equiv 2 \pmod{12} \\ x \equiv 18 \pmod{20} \end{cases}$$

Tenemos entonces las siguientes implicaciones y equivalencias:

$$\left\{ \begin{array}{l} x \equiv 7 \pmod{11} \\ x \equiv 8 \pmod{9} \\ x \equiv 8 \pmod{15} \\ x \equiv 2 \pmod{12} \\ x \equiv 18 \pmod{20} \end{array} \right. \Rightarrow \begin{array}{l} x \equiv 2 \pmod{3} \\ (x \equiv 3 \pmod{5} \text{ y } x \equiv 2 \pmod{3}) \\ (x \equiv 2 \pmod{4} \text{ y } x \equiv 2 \pmod{3}) \\ (x \equiv 3 \pmod{5} \text{ y } x \equiv 2 \pmod{4}) \end{array}$$

luego a la primera y la segunda ecuación las debemos preservar intactas y de las restantes es suficiente tomar las ecuaciones $x \equiv 3 \pmod{5}$ y $x \equiv 2 \pmod{4}$, o, lo que es lo mismo, la última ecuación de las de arriba. Así nos queda el sistema equivalente:

$$\left\{ \begin{array}{l} x \equiv 7 \pmod{11} \\ x \equiv 8 \pmod{9} \\ x \equiv 18 \pmod{20} \end{array} \right.$$

Resolviendo obtenemos: $x = 18 + 20k \equiv 7 \pmod{11}$ reduciendo: $9k \equiv 0 \pmod{11}$ de donde k debe ser un múltiplo de 11. Luego tenemos: $x = 18 + 20 \cdot 11s \equiv 8 \pmod{9}$, reduciendo: $4s \equiv 8 \pmod{9}$, luego $s \equiv 2 \pmod{9}$, ya que 4 es invertible módulo 9, pues $\text{mcd}(4, 9) = 1$. Recolectando: $x = 18 + 20 \cdot 11(2 + 9p) = 458 + 20 \cdot 11 \cdot 9p$, para todo $p \in \mathbb{Z}$. Dicho de otro modo: $x \equiv 458 \pmod{20 \cdot 11 \cdot 9}$, la solución buscada.

Ejercicio 4.

- Describir el método de Diffie - Hellman para acuerdo de clave.
- Donald y Mickey, para garantizar la seguridad del gobierno de su país, se ponen de acuerdo en utilizar Diffie - Hellman y fijan el primo $p = 73$ y $g = 11$. Donald elige el número secreto $n = 71$ y Mickey le envía $g^m = 23$. ¿Cuál es la clave secreta que acuerdan Donald y Mickey?
- Asignamos valores a algunos caracteres según la tabla siguiente:

A	B	C	D	E	J	L	M	N	O	P	S	R
0	1	2	3	4	5	6	7	8	9	10	11	12

Definimos el criptosistema afín de la siguiente manera: para $a, b \in \mathbb{Z}$, con $1 \leq a \leq 12$, y $0 \leq b \leq 12$, consideramos la función de encriptado $E : \mathbb{Z}_{13} \rightarrow \mathbb{Z}_{13}$ tal que $E(x) = ax + b \pmod{13}$. Sea $0 \leq W < 73$ la clave acordada por Donald y Mickey. Escribamos $W = a \cdot 13 + b$ con $0 \leq a < 13$ y $0 \leq b < 13$. El encriptado se hace letra a letra usando la función E definida arriba. Encriptar la palabra DJNP.

- Supongamos que somos espías rusos y que Donald le envió a Mickey un mensaje encriptado según el criptosistema anterior (desconociendo los valores de a y b de la función de encriptado). Espías ayudantes han descubierto que el mensaje original (sin encriptar) tiene como segunda letra A y como cuarta letra E . El mensaje encriptado es $OCEJM$.
 - Hallar la función de encriptado (o sea hallar los valores de a y b) que usan Donald y Mickey.
 - Desencriptar el mensaje $OCEJM$.

Solución.

- Ver Sección 5.2.1 de las notas de teórico.

b. Queremos calcular $23^{71} \pmod{73}$. Por el teorema de Fermat tenemos que $23^{72} \equiv 1 \pmod{73}$, por lo tanto $23^{71} \cdot 23 \equiv 1 \pmod{73}$. O sea que 23^{71} es el inverso de 23 módulo 73 (o sea: $23^{71} \equiv (23)^{-1} \pmod{73}$). Necesitaríamos resolver la ecuación diofántica lineal: $23 \cdot x + 73 \cdot y = 1$. Usando el algoritmo de Euclides extendido obtenemos que el inverso es $x = 54$. O sea $23^{71} \equiv 54 \pmod{73}$.

c. Como $54 = 4 \cdot 13 + 2$ (de forma única, pues estamos escribiendo en base 13), entonces $a = 4$ y $b = 2$. La palabra encriptada es BOND.

- Usando que A se transforma en C y que E se transforma en J podemos deducir que $a = 4$ y $b = 2$.
 - Con el $a = 4$ y el $b = 2$ hallado arriba, se tiene que el mensaje desencriptado es JAMES.

Ejercicio 5.

- a. Sea p un primo y k un entero positivo. Si g es un número par y raíz primitiva de p^k , probar que $g + p^k$ es raíz primitiva de $2p^k$.
- b. Hallar explícitamente todos los homomorfismos de $U(54)$ en el grupo dihedral D_{12} .

Solución. La parte **a.** es de teórico (Lema 4.1.13).

b. Dado que $54 = 2 \cdot 3^3$, por el Teorema 4.1.15, $n = 54 = 2 \cdot 3^3$, y por lo tanto el grupo $U(54)$ es cíclico, con lo cual para determinar un morfismo $f : U(54) \rightarrow D_{12}$ basta definir $f(g) = k$ donde $o(k) | o(g)$, siendo g un generador de $U(54)$. Para hallar un generador de $U(54)$, veremos que 2 es raíz primitiva módulo 27, luego por la parte **a.** tendremos $U(54) = \langle 2 + 3^3 \rangle = \langle 29 \rangle$.

Siendo $\varphi(27) = 18 = 2 \cdot 3^2$, para demostrar que 2 es raíz primitiva módulo 27, basta probar que 2^9 y 2^6 no son congruentes con 1 módulo 27. Calculamos que $2^6 \equiv 10 \not\equiv 1$ y $2^9 \equiv -1 \not\equiv 1$ módulo 27.

Ahora basta definir $f(29) = k$ de modo que $o(k) | 18$. Los posibles órdenes de los elementos en D_{12} , por el Teorema de Lagrange, son 1, 2, 3, 4, 6, 8, 12 (son los divisores de $|D_{12}| = 24$, omitiendo el 24, ya que D_{12} no es cíclico, obsérvese que las simetrías tienen orden 2 y las potencias de la rotación mínima ρ tienen órdenes 3, 4 o 6). De estos posibles órdenes los que dividen a 18 son 1, 2, 3 y 6, luego las imágenes $f(29) = k$ pueden ser:

- la identidad;
- cualquiera de las 12 simetrías y la rotación ρ^6 (tienen orden 2);
- las rotaciones ρ^2 y ρ^{10} (de orden 6); y
- por último: ρ^4 y ρ^8 (de orden 3).

En total son 18 homomorfismos.