1. Hallar todos los $x \in \mathbb{Z}$ que satisfacen los siguientes sistemas de congruencias:

(a) $\begin{cases} x \equiv 2 \ (6) \\ x \equiv -1 \ (15) \end{cases}$ (b) $\begin{cases} x \equiv 5 \ (2) \\ x \equiv 3 \ (4) \end{cases}$ (c) $\begin{cases} x \equiv 3 \ (4) \\ x \equiv 2 \ (3) \\ x \equiv 3 \ (5) \end{cases}$ (d) $\begin{cases} x \equiv 5 \ (2) \\ 3x \equiv 1 \ (4) \\ x \equiv 2 \ (3) \\ x \equiv 3 \ (5). \end{cases}$

2. Hallar el menor entero positivo n que satisface simultáneamente las siguientes condiciones:

(a) el resto de n en la división por 10 es 3,

(b) el resto de $3n$ en la división por 7 es 2, y

(c) el resto de $4n$ en la división por 9 es 5.

3. En un grupo de 20 amigos se reparten alfajores entre todos y sobran 7 alfajores. Tres amigos se van, devuelven su parte y se vuelve a repartir el total de alfajores entre los amigos que quedan. Sobran 5 alfajores. ¿Cuántos alfajores, como mínimo, había para repartir?

4. La producción diaria de huevos en una granja es inferior a 75. Cierto día el recolector informó que la cantidad de huevos recogida es tal que contando de a 3 sobran 2, contando de a 5 sobran 4 y contando de a 7 sobran 5. El capataz dijo que eso era imposible. ¿Quién tiene razón? Justificar.

5. Hallar el resto de la división de a por p en los casos:

(a) $a = 2^{21}$, $p = 13$;

(b) $a = 3^8$, $p = 5$;

(c) $a = 3^{256}$, $p = 127$;

(d) $a = 5 \cdot 7^{2451} + 3 \cdot 65^{2345} - 23 \cdot 8^{138}$, $p = 13$.

6. Probar que si $(a, 1001) = 1$ entonces 1001 divide a $a^{720} - 1$.

7. Hallar todos los primos positivos p tales que $p \mid 2^p + 5$.

8. Hallar todos los enteros positivos a tales que $(4a^{62} - a, 11a) \neq a$.

9. Probar que para todo primo $p > 3$ se cumple que $p \mid 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$.

10. Sea p un primo distinto de 2 y de 5. Probar que existe un número de la forma $99\ldots99$ que es múltiplo de p.

11. Sean p y q primos positivos. Probar que si q divide a $2^p - 1$, entonces $q \equiv 1 (p)$.
[Ayuda: Probar primero que q divide a $(2^p - 1, 2^{q-1} - 1) = 2^{(p,q-1)} - 1$].

12. Probar la recíproca del teorema de Wilson: si $p > 1$ satisface $(p-1)! \equiv -1 \, (p)$ entonces p es primo.

Recordatorio: los anillos $\mathbb{Z}_m$. Dado un entero $m > 1$, definimos una relación de equivalencia en $\mathbb{Z}$ por: a está relacionado con b si y sólo si $a \equiv b \ (m)$. Denotamos por $\mathbb{Z}_m$ al conjunto de clases de equivalencia, y la clase de un entero a se denota por $[a]$ (también usamos $\overline{a}$).

13. Probar que $\mathbb{Z}_m$ es un anillo conmutativo con unidad.

14. Decimos que un elemento x de un anillo R es *inversible* si existe un elemento $y \in R$ tal que $xy = 1 = yx$. Sea $m > 1$ un entero. Probar que:

(a) Un elemento $[a] \in \mathbb{Z}_m$ es inversible si y sólo si $(a, m) = 1$.

(b) El anillo $\mathbb{Z}_m$ es un cuerpo si y sólo si m es primo.

15. Decimos que un elemento no nulo x de un anillo R es un *divisor de cero* si existe un elemento no nulo $y \in R$ tal que $xy = 0$. Dado un entero $m > 1$, probar que m es primo si y sólo si el anillo $\mathbb{Z}_m$ no tiene divisores de cero.

16. Probar que en $\mathbb{Z}_m$ vale que

$$\sum_{k=0}^{m-1} [k] = \begin{cases} [0] & \text{si } m \text{ es impar,} \\ [\frac{m}{2}] & \text{si } m \text{ es par.} \end{cases}$$

Ejercicios complementarios

17. (a) En $\mathbb{Z}_7$, probar que $\{[3]^n : n \in \mathbb{N}\} = \mathbb{Z}_7 - \{[0]\}$.

(b) En $\mathbb{Z}_{11}$, calcular $\{[3]^n : n \in \mathbb{N}\}$. De ser posible, hallar un elemento $[a] \in \mathbb{Z}_{11}$ tal que $\{[a]^n : n \in \mathbb{N}\} = \mathbb{Z}_{11} - \{[0]\}$.

(c) Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 1\,(7)$ y todos los $n \in \mathbb{N}$ tales que $3^n \equiv 4\,(7)$.

(d) Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 1\,(11)$ y todos los $n \in \mathbb{N}$ tales que $3^n \equiv 9\,(11)$.

(e) Hallar todos los $n \in \mathbb{N}$ tales que $3^n \equiv 53\,(77)$.

18. Un elemento $[a] \in \mathbb{Z}_n$ es un *cuadrado* si existe $[b] \in \mathbb{Z}_n$ tal que $[a] = [b]^2$ en $\mathbb{Z}_n$.

(a) Calcular los cuadrados de $\mathbb{Z}_n$ para $n = 2$, 3, 4, 5, 6, 7, 8, 9, 11 y 13.

(b) Probar que si $[a]$ y $[b] \in \mathbb{Z}_n$ son cuadrados, entonces $[a][b]$ es un cuadrado.

(c) Probar que si $[a]$ es un elemento inversible de $\mathbb{Z}_n$ tal que $[a] = [b]^2$, entonces $[b]$ es inversible y $[a]^{-1}$ es un cuadrado.

(d) Sea p primo positivo. En $\mathbb{Z}_p$, probar que si $[a]^2 = [b]^2$ entonces $[a] = [b]$ ó $[a] = -[b]$. Deducir que si p es impar, entonces hay exactamente $\frac{p-1}{2}$ cuadrados no nulos en $\mathbb{Z}_p$.

(e) Sea p primo positivo impar. Probar que, en $\mathbb{Z}_{2p}$, si $[a]^2 = [b]^2$ entonces $[a] = [b]$ ó $[a] = -[b]$.

(f) Probar que si $n \in \mathbb{N}$ es impar y n no es primo, entonces existen $[a]$ y $[b] \in \mathbb{Z}_n$ con $[a]^2 = [b]^2$ y $[a] \neq \pm[b]$.

19. Sea p un número primo impar. Probar que

(a) $((\frac{p-1}{2})!)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

(b) La ecuación $x^2 \equiv -1 \pmod{p}$ tiene solución si y sólo si p es un primo de la forma $4k + 1$.
[Ayuda: usar el pequeño teorema de Fermat].

(c) Usar el punto anterior para dar una prueba alternativa a un ejercicio del práctico anterior:

"Si a y b son enteros entonces $a^2 + b^2$ es divisible por 7 si y sólo si a y b son divisibles por 7."

Puede plantear una generalización a dicho ejercicio y probarla?

20. Mostrar que las ecuaciones $a^2 + 10b^2 = 2$, $a^2 - 10b^2 = 3$, $7x^4 + 2y^3 = 3$, $2x^3 + 27y^4 = 21$, $7x^5 + 3y^4 = 2$ y $15x^2 - 7y^2 = 1$ no tienen soluciones en los números enteros.

21. Recordemos que la función de Eüler φ se define de la siguiente manera: si m es un número natural, $\varphi(m)$ se define como la cantidad de números naturales menores o iguales que m y coprimos con m:

$$\varphi(m) = |\{n \in \mathbb{N} \mid n \leq m,\ (n, m) = 1\}|.$$

Por ejemplo, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(12) = 4$, $\varphi(15) = 8$. Algunas propiedades son:

- Si p es un número primo y $k \in \mathbb{N}$ entonces $\varphi(p^k) = p^{k-1}(p-1)$.
- Si $(m, n) = 1$ entonces $\varphi(mn) = \varphi(m)\varphi(n)$.
- Teorema de Fermat-Eüler: sean $m \in \mathbb{N}$ y $a \in \mathbb{Z}$ con $(a, m) = 1$. Entonces $a^{\varphi(m)} \equiv 1\,(m)$.

Resolver los siguientes ejercicios:

(a) Calcular $\varphi(36)$, $\varphi(400)$, $\varphi(10^n)$ para $n \in \mathbb{N}$.

(b) Sea $m \in \mathbb{N}$, $m > 1$. Probar que

$$\varphi(m) = m \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right),$$

donde p recorre todos los primos positivos que dividen a m.

(c) Sea $m \in \mathbb{N}$, $m > 2$. Probar que $\varphi(m)$ es par.

(d) Hallar el resto que se obtiene al dividir 2^{2021} por 125.