Práctico 6

Congruencia de enteros
Aritmética modular

Álgebra I
2022, FaMAF - UNC

Objetivos

- Aprender a operar en congruencias.
- Usar congruencias para resolver problemas de divisibilidad.
- Resolver ecuaciones y sistemas de ecuaciones en congruencias.
- Aprender el Pequeño Teorema de Fermat y sus corolarios, el Teorema de Euler y el Teorema de Wilson, y su uso en la resolución de problemas en congruencias (Ejercicios **17)**-**22)**).

Ejercicios

1) Demostrar las siguientes congruencias, aclarando las propiedades que usa en cada paso:

(a) $4! \equiv 4\,(5)$ (b) $36^5 \equiv -1\,(37)$ (c) $6^n + 8 \equiv 4\,(5)$ $(n \in \mathbb{N})$.

2) Calcular el resto de la división de x por n sin realizar la división en los siguientes casos

(a) $x = 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101$ y $n \in \{5, 7\}$.
(b) $x = 2^{210}$ y $n = 6$.
(c) $x = 1^6 + 2^6 + 3^6 + 4^6 + 5^6 + 6^6 + 7^6 + 8^6$ y $n = 9$.
(d) $x = \sum_{i=1}^{100} i!$ y $n = 50$.

3) Hallar la cifra de las unidades y la de las decenas del número 7^{15}.

4) Probar el Ejercicio 3) del Práctico 4 usando congruencias y sin usar inducción.

5) Sean $m, n \in \mathbb{Z}$.

(a) Probar que $m^2 \equiv 0(3)$ ó $m^2 \equiv 1(3)$.
(b) Hallar los restos posibles en la división de m^{15} por 3.
(c) Probar 3 divide a $m^2 + n^2$ si y sólo si 3 divide a m y a n.

6) (a) Probar las reglas de divisibilidad por 2, 3, 4, 5, 8, 9 y 11 que no hayan sido probadas en el teórico.
(b) Decir por cuáles de los números 2, 3, 4, 5, 8, 9 y 11 son divisibles los números 12342, 5176, 314573 y 899.

7) Calcular el resto de 3^n dividido 7 para $n = 1, 2, 3, ...$ y así hasta que deduzcas unas fórmula general en función de n.

8) Resolver las siguientes ecuaciones:

(a) $2x \equiv -21\ (8)$ (b) $2x \equiv -12\ (7)$ (c) $3x \equiv 5\ (4)$.

9) Resolver la ecuación $221\,x \equiv 85\ (340)$. Hallar todas las soluciones x tales que $0 \leq x < 340$.

10) Decimos que $x \in \mathbb{Z}_m$ es *inversible* si existe $y \in \mathbb{Z}_m$ tal que $xy \equiv 1\,(m)$. Probar que $a \in \mathbb{Z}_m$ es inversible si y sólo si $(a, m) = 1$.

11) Decimos que $x \in \mathbb{Z}_m$ es *divisor de cero* si existe $y \in \mathbb{Z}_m$ tal que $xy \equiv 0\,(m)$. Probar que $a \in \mathbb{Z}_m$ es divisor de cero si y sólo si $(a, m) \neq 1$.

12) Dar todos los pares $(x, y) \in \mathbb{Z}_6 \times \mathbb{Z}_6$ tales que $x + 2y \equiv 0\ (7)$.

13) Sea p un primo y a un entero no divisible por p. ¿Cuántos pares (x, b) con $0 \leq x, b \leq p-1$ hay tales que $ax \equiv b\ (p)$?

14) Sean a, b, $m \in \mathbb{Z}$, $d > 0$, tales que $d \mid a$, $d \mid b$ y $d \mid m$. Probar que x_0 es solución de la ecuación $a \cdot x \equiv b\,(m)$ si y sólo si x_0 es solución la ecuación

$$\frac{a}{d} \cdot x \equiv \frac{b}{d}\ \left(\frac{m}{d}\right).$$

15) Dar el conjunto de soluciones de los siguientes sistemas de congruencias:

(a) $\begin{cases} x \equiv 11\ (15) \\ x \equiv\ 8\ (12) \end{cases}$ (b) $\begin{cases} x \equiv 11\ (15) \\ x \equiv\ 7\ (12) \end{cases}$ (c) $\begin{cases} x \equiv 1\ (3) \\ x \equiv 2\ (5) \\ x \equiv 3\ (7) \end{cases}$ (d) $\begin{cases} 4x \equiv 14\ (15) \\ 5x \equiv 40\ (12) \end{cases}$

16) 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?

17) Hallar el resto de la división de a por p en los casos:

(a) $a = 3^{210}$, $p = 13$; (b) $a = 25^{63}$, $p = 127$;

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

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

20) Sea a un entero tal que $(18a^{49} - 14, 104) = 26$. Calcular el resto en la división de a por 13.

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

Más ejercicios...

Si ya hizo los ejercicios anteriores continue con la siguiente guía. Los ejercicios que siguen son similares y le pueden servir para practicar antes de los exámenes.

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

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

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

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

Resolver los siguientes ejercicios:

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

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

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

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

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

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

23) Hallar todos los x que satisfacen:

(a) $x^2 \equiv 1\ (4)$ (c) $x^2 \equiv 2\ (5)$ (e) $x^3 \equiv 1\ (7)$

(b) $x^2 \equiv x\ (12)$ (d) $x^2 \equiv 0\ (12)$ (f) $x^4 \equiv 1\ (5)$.

24) Sean a, b, c números enteros, ninguno divisible por 3. Probar que $a^2 + b^2 + c^2$ es divisible por 3.

25) (a) Probar que el resto de dividir n^2 por 4 es igual a 0 si n es par y 1 si n es impar.

(b) Probar que si las longitudes de los lados de un triángulo rectángulo son números enteros, entonces las longitudes de los catetos no pueden ser ambas impares.

26) (a) ¿Para cuáles valores de $n \in \mathbb{N}$ es $2^n + 1$ divisible por 3?

(b) ¿Para cuáles valores de $n \in \mathbb{N}$ es $10^n - 1$ divisible por 11?

27) Probar que, para todo $n \in \mathbb{Z}$, el número $n^2 + 4n + 6$ no es múltiplo de 5.

28) Sean m, n números enteros.

(a) Probar que $m^2 + n^2$ es múltiplo de 7 si y sólo si m y n son múltiplos de 7.

(b) Probar que $m^2 + 5n^2$ es múltiplo de 11 si y sólo si m y n son múltiplos de 11.

29) Dado $t \in \mathbb{Z}$, decimos que t es *inversible módulo* m si existe $h \in \mathbb{Z}$ tal que $th \equiv 1\,(m)$.

(a) ¿Es 5 inversible módulo 17?

(b) Probar que t es inversible módulo m si y sólo si $(t, m) = 1$.

(c) Determinar los inversibles módulo m, para $m = 11, 12, 16$.

30) Hallar el resto de la división de a por p en los casos:

(a) $a = 3^8$, $p = 5$; (c) $a = 3^{256}$, $p = 127$;

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

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

32) 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.