Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería **Segundo semestre 2024**
Instituto de Matemática y Estadística

PRÁCTICO 5: CONGRUENCIAS

Ejercicio 1.

a. Si $a \equiv 22 \pmod{14}$, hallar el resto de dividir a por 2, por 7 y por 14.

b. Verifique que se cumplen las siguientes congruencias: $5! \equiv 12 \pmod{36}$; $i! \equiv 0 \pmod{36}$, $\forall\, i \geq 6$.

c. Hallar, para cada $n \in \mathbb{N}$, el resto de dividir $S_n = \displaystyle\sum_{i=1}^{n} (-1)^i \cdot i!$ por 36.

Ejercicio 2. Suponga que $a \equiv b \pmod{m}$, para cierto entero m fijo. Probar las siguientes propiedades:

a. $\lambda a \equiv \lambda b \pmod{m}$, para todo $\lambda \in \mathbb{Z}$.

b. $a^n \equiv b^n \pmod{m}$ para todo $n \in \mathbb{N}$.

c. Si $a \equiv 3 \pmod{5}$, hallar el resto de dividir $4a^3$ entre 5.

d. Usando las propiedades anteriores, probar que si $p(x) = \lambda_n x^n + \lambda_{n-1} x^{n-1} + \ldots + \lambda_1 x + \lambda_0$, es un polinomio con coeficientes enteros λ_i, entonces $p(a) \equiv p(b) \pmod{m}$.

e. Si $a \equiv 3 \pmod{5}$, hallar el resto de dividir $33a^3 + 3a^2 - 197a + 2$ por 5.

Ejercicio 3. [Pequeño Teorema de Fermat]

a. Probar que si a y b son enteros y p un número primo, entonces: $(a+b)^p \equiv a^p + b^p \pmod{p}$. Sugerencia: usar el teorema del binomio. ¿Vale el resultado si p no es primo?

b. Probar el denominado “pequeño Teorema de Fermat”: $a^p \equiv a \pmod{p}$, para todo a entero y p primo. Sugerencia: usar inducción.

c. Calcular el resto de dividir 327^{101} entre 101.

Ejercicio 4.

a. Demostrar que $10^n \equiv (-1)^n \pmod{11}$, para todo $n \in \mathbb{N}$.

b. Enunciar y probar un criterio de divisibilidad entre 11. Sugerencia: expresar el número en base 10 y usar la parte anterior.

c. Hallar el dígito $d \in \{0, 1, \ldots, 9\}$, de modo que el número $2\mathbf{d}653874$ sea múltiplo de 11.

Ejercicio 5.

a. Determinar el último dígito de 3^{55} en base 10. Sugerencia: probar que $3^{55} \equiv a_0 \pmod{10}$; donde a_0 es el dígito buscado.

b. Hallar el resto de la división de 12^{1257} entre 5.

Ejercicio 6.

a. Hallar el inverso de 2 módulo 141.

b. Probar que 2 es invertible módulo n si y solamente si n es impar. En tal caso, hallar el inverso.

c. Resolver la ecuación $2x + 1 \equiv 0 \pmod{69}$.

Ejercicio 7. Resolver cada una de las congruencias siguientes:

a. $3x \equiv 7 \pmod{16}$.

b. $2x + 8 \equiv 5 \pmod{33}$.

c. $3x+9 \equiv 8x+61 \pmod{64}$.

d. $6x - 1 \equiv 5 \pmod{12}$.

e. $9x + 3 \equiv 5 \pmod{18}$.

Ejercicios complementarios

Ejercicio 8. El número de la cédula uruguaya tiene la forma $x_1x_2 \dots x_7$-x_8; donde cada $x_i,\ i = 1, 2 \dots 8$, es un dígito de 0 a 9. El dígito verificador x_8 se calcula de la siguiente manera. Sea

$$c = \sum_{i=1}^{7} a_i \cdot x_i,$$

donde $(a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (2, 9, 8, 7, 6, 3, 4)$. Entonces x_8 es: $r \equiv -c \pmod{10},\ 0 \leq r < 10$.

a. Verificar que el dígito verificador de su cédula se obtiene mediante la fórmula dada arriba.

b. Investigar si el dígito verificador detecta el error de copiar mal un dígito (de los primeros 7).

c. Probar que el dígito verificador detecta el error de intercambiar dos dígitos consecutivos de los $x_1, x_2, \dots, x_7$ (en el sentido del ejercicio anterior).

d. Escribir un programa para comprobar si una secuencia de 8 dígitos es un número de cédula o no.

Ejercicio 9. Sea $n \in \mathbb{N}$ cuya representación en base 10 es $a_k a_{k-1} \cdots a_2 a_1 a_0$.

a. Probar que $n \equiv 2a_1 + a_0 \pmod{4}$.

b. Probar que $n \equiv 4a_2 + 2a_1 + a_0 \pmod{8}$.

c. Proponer una generalización del resultado para congruencia módulo 2^i, con $i < k$. Probar esta generalización, o refutarla mediante un contraejemplo.

Ejercicio 10.

a. Probar que para todo $a \in \mathbb{Z}$ se cumple: $a^2 \equiv 0 \pmod{4}$ o $a^2 \equiv 1 \pmod{4}$.

b. Muestre que el número 342634535100234547254362 2 no es cuadrado perfecto ni cubo perfecto. Sugerencia: para la 1a parte use congruencia módulo 4, y para la 2a use congruencia módulo 9.

c. Probar que ningún número de la sucesión $a_1 = 11,\ a_2 = 111,\ a_3 = 1111,\ a_4 = 11111, \ldots$ es un cuadrado perfecto.

Ejercicio 11. Sea $p(x)$ un polinomio con coeficientes enteros, tal que: $p(0) = 1$, $p(1) = 2$ y $p(2) = 5$. Probar que $p(x)$ no tiene raíces enteras. Sugerencia: si $p(a) = 0$, podemos factorizar: $p(x) = (x - a)q(x)$, para algún polinomio q. Si $a \in \mathbb{Z}$, esto implica que $x - a$ divide a $p(x)$, para todo $x \in \mathbb{Z}$.

Ejercicio 12. Probar lo siguiente:

a. La ecuación $x^2 - 1 \equiv 0 \pmod{7}$ tiene exactamente 2 soluciones distintas.

b. La ecuación $x^2 - 1 \equiv 0 \pmod{35}$ tiene al menos 4 soluciones distintas. Probar además que son las únicas soluciones posibles.