Universidad de la República
Facultad de Ingeniería
Instituto de Matemática y Estadística

Matemática Discreta 2
Curso 2018

PRÁCTICO 4: CONGRUENCIAS

Ejercicio 1. Probar las siguientes propiedades:

a. $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$ y $ac \equiv bd \pmod{n}$.

b. $b \equiv c \pmod{n}$ y $a \in \mathbb{Z} \Rightarrow a + b \equiv a + c \pmod{n}$.

c. $a \equiv b \pmod{n}$ y $m|n \Rightarrow a \equiv b \pmod{m}$.

d. $a \equiv b \pmod{m}$ y $n \in \mathbb{Z} \Rightarrow na \equiv nb \pmod{m}$. ¿Vale el recíproco?

e. $a \equiv b \pmod{m}$ y $n \in \mathbb{N} \Rightarrow a^n \equiv b^n \pmod{m}$.

f. $ac \equiv bc \pmod{m}$ y $d = \text{mcd}(c, m) \Rightarrow a \equiv b \pmod{m/d}$.

Ejercicio 2.

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

b. Si $a \equiv 13 \pmod{5}$, hallar el resto de dividir a $33a^3 + 3a^2 - 197a + 2$ por 5.

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

Ejercicio 3.

a. Probar que si a y b son enteros y p un número primo entonces

$$(a + b)^p \equiv a^p + b^p \pmod{p}$$

¿Vale el resultado si p no es primo?

b. Probar (por inducción) el Teorema de Fermat: $a^p \equiv a \pmod{p}$, para todo a entero y todo primo p.

Ejercicio 4.

a. Hallar todos los $a \in \mathbb{Z}$ tales que $a^3 \equiv 3 \pmod{11}$.

b. Probar que no existe ningún entero a tal que $a^3 \equiv -3 \pmod{13}$.

c. Probar que $a^2 \equiv -1 \pmod{5} \Leftrightarrow a \equiv 2 \pmod{5}$ o $a \equiv 3 \pmod{5}$.

d. Probar que $a^7 \equiv a \pmod{7}$ para todo $a \in \mathbb{Z}$.

Ejercicio 5. Encontrar las soluciones (módulo 35) de la ecuación

$$x^2 - 1 \equiv 0 \pmod{35}.$$

Ejercicio 6. 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. Enunciar y demostrar un resultado similar a los anteriores para 2^k.

Ejercicio 7.

a. Demostrar que $10^n \equiv (-1)^n \pmod{11}$.

b. Enunciar y probar un criterio de divisibilidad entre 11.

c. Hallar el dígito d, de modo que el número $2d653874$ sea múltiplo de 11.

Ejercicio 8. Demostrar que $4^n \equiv 4 \pmod 6$ para todo entero $n \geq 1$.

Ejercicio 9.

a. Probar que para todo $a \in \mathbb{Z}$ se cumple que

$$a^2 \equiv 0 \pmod 4 \qquad \text{o} \qquad a^2 \equiv 1 \pmod 4.$$

b. Averiguar si 345674535600234567654346 2 es un cuadrado perfecto.

c. Probar que ningún número de la sucesión

$$a_1 = 11, \quad a_2 = 111, \quad a_3 = 1111, \qquad a_n = 11\ldots11$$

es un cuadrado perfecto.

Ejercicio 10.

El código ISBN de libros tiene la forma $x_1x_2\ldots x_9$-x_{10} donde cada $x_i, i = 1, 2\ldots10$ es un dígito de 0 a 9, mientras x_{10} también puede ser igual al símbolo X. El símbolo x_{10} se llama el *símbolo verificador* y se calcula de la siguiente manera. Sea

$$c = \sum_{i=1}^{9} i \cdot x_i$$

y sea r el resto: $r \equiv c \pmod{11},\ 0 \leq r < 11$. Entonces

$$x_{10} = \begin{cases} r, & \text{si} \quad 0 \leq r \leq 9 \\ X, & \text{si} \quad r = 10 \end{cases}$$

a. Probar que $\sum_{i=1}^{10} i \cdot x_i \equiv 0 \pmod{11}$.

b. Probar que el dígito verificador detecta el error de intercambiar exactamente dos dígitos de los $x_1, x_2, \ldots, x_9$ (si intecambiamos exactamente dos de esos dígitos, obtenemos un dígito verificador diferente).

Ejercicio 11.

El número de la cédula uruguaya tiene la forma $x_1x_2\ldots x_7$-x_8 donde cada $x_i, i = 1, 2\ldots8$ 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 $x_1, x_2, \ldots, x_7$ (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 12. 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. $9x + 3 \equiv 5 \pmod{18}$.

Ejercicio 13.

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

b. Hallar $71^{10} \pmod{141}$.

Ejercicio 14.

a. Determinar el último dígito de 3^{55}.

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

Ejercicio 15.

a. Probar $2^{5n} \equiv 1 \pmod{31}$ para todo $n \in \mathbb{N}$.

b. Hallar el resto de la división de 2^{51833} por 31.

c. Sea $k \in \mathbb{N}$. Sabiendo que $2^k \equiv 39 \pmod{31}$, hallar el resto de la división de k por 5.

d. Hallar el resto de la división de $43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999}$ por 31.

Ejercicio 16.

a. Probar que el inverso de 10 módulo 7 es -2.

b. Sea $n = 10x + y$, probar que $n \equiv 0 \pmod{7}$ si y solo si $x - 2y \equiv 0 \pmod{7}$.

c. Utilizando lo anterior enunciar y demostrar un criterio de divisibilidad entre 7.