Práctico 4
Matemática Discreta I – Año 2022/1
FAMAF

(1) *a)* Calcular el resto de la división de 1599 por 39, sin tener que hacer la división.

b) Lo mismo con el resto de 914 al dividirlo por 31.

(2) Hallar el resto en la división de x por 5 y por 7 para:

a) $x = 1^8 + 2^8 + 3^8 + 4^8 + 5^8 + 6^8 + 7^8 + 8^8$,

b) $x = 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101$.

(3) Sea $n \in \mathbb{Z}$. Probar que el resto de dividir n^2 por 4 es igual a 0 si n es par, y 1 si n es impar.

(4) Sean a, b, c números enteros, ninguno divisible por 3. Probar que

$$a^2 + b^2 + c^2 \equiv 0 \pmod 3.$$

(5) Sea $n \in \mathbb{N}$. Probar las siguientes afirmaciones.

a) Todo número de la forma $4^n - 1$ es divisible por 3.

b) Todo número de la forma $7 \cdot 5^{2n} - 24 \cdot 2^{3n}$ es divisible por 17.

c) Todo número de la forma $3^{3n+1} + 2^{3n+4}$ es divisible por 19.

(6) *a)* Probar las reglas de divisibilidad por 2, 3, 4, 5, 8, 9 y 11.

b) Decir por cuáles de los números del 2 al 11 son divisibles los siguientes números:

12342 5176 314573 899.

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

(8) Sean $a, b \in \mathbb{Z}$. Si $m, d \in \mathbb{N}$ cumplen que $d \mid a$, $d \mid b$ y $d \mid m$, probar que la ecuación $ax \equiv b\,(m)$ admite solución si y sólo si la ecuación

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

admite solución.

(9) Resolver las siguientes ecuaciones:

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

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

(11) *a)* Encontrar todas las soluciones de la ecuación $36\,x \equiv 8\ (20)$, usando el método visto en la clase teórica.

b) Dar todas las soluciones x de la ecuación anterior tales que $-8 < x < 30$.

(12) *a)* Encontrar todas las soluciones de la ecuación $21\,x \equiv 6\ (30)$, usando el método visto en la clase teórica.

b) Dar todas las soluciones x de la ecuación anterior tales que $0 < x < 35$.

(13) Sea $t \in \mathbb{Z}$, 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 $m = 11, 12, 16$.

(14) Sean a, b números enteros, y m un entero positivo. Si $x_0 = m \cdot q + r$, con $q \in \mathbb{Z}$ y $0 \leq r < m$, probar que x_0 es una solución de la ecuación $ax^2 \equiv b\,(m)$ si y sólo si r también lo es.

(15) *a)* Encontrar las soluciones enteras de la ecuación $x^2 \equiv 94\,(13)$ en el intervalo $[10, 35]$.

b) Demostrar que la ecuación $52\,x^2 \equiv 24\,(17)$ no tiene soluciones enteras.

c) Probar que la ecuación $2\,x^2 \equiv 3\,(19)$ tiene una única solución en el intervalo $[30, 45)$.

(16) Encontrar el resto en la división de a por b en los siguientes casos:

a) $a = 11^{13} \cdot 13^8$, $b = 12$. *b)* $a = 4^{1000}$, $b = 7$.

c) $a = 123^{456}$, $b = 31$. *d)* $a = 7^{83}$, $b = 10$.

(17) Hallar el resto en la división de a por b en los siguientes casos:

a) $a = 2^{21}$, $b = 13$. *b)* $a = 7^{241}$, $b = 17$.

c) $a = 424^{97}$, $b = 11$. *d)* $a = 8^{25}$, $b = 127$.

e) $a = 623^{1229} \cdot 67^{345}$, $b = 17$.

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

§ **Ejercicios de repaso.** Los ejercicios marcados con ($\star$) son de mayor dificultad.

(19) Dada la ecuación de congruencia $14\,x \equiv 10\,(26)$, hallar todas las soluciones en el intervalo $[-20, 10]$. Hacerlo con el método usado en la teórica.

(20) Dada la ecuación de congruencia $21\,x \equiv 15\,(39)$, hallar todas las soluciones en el intervalo $[-10, 30]$. Hacerlo con el método usado en la teórica.

(21) *a)* Probar que no existen enteros no nulos tales que $x^2 + y^2 = 3z^2$.

b) Probar que no existen números racionales no nulos a, b, r tales que $3(a^2 + b^2) = 7r^2$.

(22) ($\star$) Probar que todo número impar a satisface:

$$a^4 \equiv 1(16), \quad a^8 \equiv 1(32), \quad a^{16} \equiv 1(64).$$

¿Se puede asegurar que $a^{2^n} \equiv 1(2^{n+2})$?

(23) ($\star$) ¿Para qué valores de n es $10^n - 1$ divisible por 11?

(24) ($\star$) Probar que para ningún $n \in \mathbb{N}$ se puede partir el conjunto

$$\{n, n+1, \ldots, n+5\}$$

en dos partes disjuntas no vacías tales que los productos de los elementos que las integran sean iguales.

(25) ($\star$) El número 2^{29} tiene nueve cifras y todas distintas. ¿Cuál dígito falta? (No está permitido el uso de calculadora).

(26) Sea p primo impar. Probar que las únicas raíces cuadradas de 1 módulo p, son 1 y -1 módulo p. Es decir, probar que si $x^2 \equiv 1 \pmod p$, entonces $x \equiv \pm 1 \pmod p$.

(27) ($\star$) Sea p un primo impar de la forma $p = d \cdot 2^s + 1$, donde d es impar. Dado a entero tal que $0 < a < p$, probar que

(i) $a^d \equiv 1 \pmod p$, **o**

(ii) $a^{2^r \cdot d} \equiv -1 \pmod p$, para algún r tal que $0 \leq r < s$.

Dicho de otra forma: probar que

$$a^d \equiv 1 \pmod p \quad \text{o} \quad a^d \equiv -1 \pmod p \quad \text{o} \quad a^{2d} \equiv -1 \pmod p \quad \text{o} \cdots$$
$$\text{o} \quad a^{2^{s-2}d} \equiv -1 \pmod p \quad \text{o} \quad a^{2^{s-1}d} \equiv -1 \pmod p.$$

(Ayuda: observar que $a^{2^i d}$ es el cuadrado de $a^{2^{i-1}d}$; y que por el Teorema de Fermat $a^{2^s d} = a^{p-1} \equiv 1 \pmod p$. Utilizar el resultado del ejercicio (26)).