Práctico 4
Matemática Discreta I – Año 2021/1
FAMAF

(1) *a)* Calcular el resto de la división de 1599 por 39 sin tener que hacer la división.
(Ayuda: $1599 = 1600 - 1 = 40^2 - 1$).

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

(2) Sea $n \in \mathbb{N}$. Probar que todo número de la forma $4^n - 1$ es divisible por 3.

(3) 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) *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:

$$12342 \qquad 5176 \qquad 314573 \qquad 899.$$

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

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

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

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

(8) Hallar todos los x que satisfacen:

a) $x^2 \equiv 1\ (4)$ *b)* $x^2 \equiv x\ (12)$ *c)* $x^2 \equiv 2\ (3)$
d) $x^2 \equiv 0\ (12)$ *e)* $x^4 \equiv 1\ (16)$ *f)* $3x \equiv 1\ (5)$

(9) Sean a, b, $m \in \mathbb{Z}$, $d > 0$ tales que $d \mid a$, $d \mid b$ y $d \mid m$. Probar que la ecuación $a \cdot x \equiv b\,(m)$ tiene solución si y solo si la ecuación

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

tiene solución.

(10) Resolver las siguientes ecuaciones:

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

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

(12) *a)* Encontrar todas las soluciones de la ecuación en congruencia

$$36\,x \equiv 8 \quad (20)$$

usando el método visto en clase.

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

(13) *a)* Encontrar todas las soluciones de la ecuación en congruencia

$$21\,x \equiv 6 \quad (30)$$

usando el método visto en clase.

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

(14) Encontrar todas las soluciones de los siguientes sistemas de ecuaciones en congruencia

a) $\begin{array}{l} 4x \equiv 7 \pmod{11} \\ 7x \equiv 8 \pmod{12} \end{array}$

b) $\begin{array}{l} x \equiv -1 \pmod{7} \\ x \equiv 3 \pmod{10} \\ x \equiv -2 \pmod{11}. \end{array}$

c) $\begin{array}{l} x \equiv -1 \pmod{2} \\ x \equiv 5 \pmod{9} \\ x \equiv -3 \pmod{7}. \end{array}$

(15) 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 $m = 11, 12, 16$.

(16) Encontrar los enteros cuyos cuadrados divididos por 19 dan resto 9.

(17) Probar que todo número impar a satisface: $a^4 \equiv 1(16)$, $a^8 \equiv 1(32)$, $a^{16} \equiv 1(64)$. ¿Se puede asegurar que $a^{2^n} \equiv 1(2^{n+2})$?

(18) 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)* $a = 7^{83}$; $b = 10$.

(19) Obtener el resto en la división de 2^{21} por 13; de 3^8 por 5 y de 8^{25} por 127.

(20) *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 $3(a^2 + b^2) = 7r^2$.

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

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

§ **Ejercicios de repaso.** Los ejercicios marcados con $^{(*)}$ son de mayor dificultad.

(23) 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.

(24) 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.

(25) Hallar todos los enteros que satisfacen simultáneamente:

$$x \equiv 1 \ (3); \qquad x \equiv 1 \ (5); \qquad x \equiv 1 \ (7).$$

(26) $^{(*)}$ ¿Para qué valores de n es $10^n - 1$ divisible por 11?

(27) $^{(*)}$ Probar que para ningún $n \in \mathbb{N}$ se puede partir el conjunto $\{n, n+1, \dots, n+5\}$ en dos partes disjuntas no vacías tales que los productos de los elementos que las integran sean iguales.

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

(29) $^{(*)}$ Sea $p = d \cdot 2^s + 1$ donde d es impar. Dado a entero tal que $0 < a < p$, probar que

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

Dicho de otra forma: probar que

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

(*Ayuda:* observar $a^{2^i d}$ es el cuadrado de $a^{2^{i-1}d}$ y por el Teorema de Fermat $a^{2^s \cdot d} = a^{n-1} \equiv 1 \pmod n$. Utilizar el resultado del ejercicio (22)).