

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.
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) 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) $x = 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101$.
- (4) 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.
- (5) Sean a, b, c números enteros, ninguno divisible por 3. Probar que
$$a^2 + b^2 + c^2 \equiv 0 \pmod{3}.$$
- (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:

123425176314573899.
- (7) Hallar la cifra de las unidades y la de las decenas del número 7^{15} .
- (8) Hallar todos los $x \in \mathbb{Z}$ que satisfacen:

a) $x^2 \equiv 1 \pmod{4}$
d) $x^2 \equiv 1 \pmod{5}$

b) $x^2 \equiv x \pmod{12}$
e) $x^4 \equiv 1 \pmod{16}$

c) $x^2 \equiv 2 \pmod{3}$
f) $x^2 \equiv 9 \pmod{19}$
- (9) 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 $ax \equiv b \pmod{m}$ tiene solución si y sólo si la ecuación
$$\frac{a}{d} x \equiv \frac{b}{d} \pmod{\left(\frac{m}{d}\right)}$$
tiene solución.
- (10) Resolver las siguientes ecuaciones:

a) $2x \equiv -21 \pmod{8}$

b) $2x \equiv -12 \pmod{7}$

c) $3x \equiv 5 \pmod{4}$

- (11) Resolver la ecuación $221x \equiv 85 \pmod{340}$. Hallar todas las soluciones x tales que $0 \leq x < 340$.
- (12) a) Encontrar todas las soluciones de la ecuación $36x \equiv 8 \pmod{20}$, usando el método visto en la clase teórica.
b) Dar todas las soluciones x de la ecuación anterior tales que $-8 < x < 30$.
- (13) a) Encontrar todas las soluciones de la ecuación $21x \equiv 6 \pmod{30}$, usando el método visto en la clase teórica.
b) Dar todas las soluciones x de la ecuación anterior tales que $0 < x < 35$.
- (14) Sea $t \in \mathbb{Z}$, decimos que t es *invertible módulo m* si existe $h \in \mathbb{Z}$ tal que $th \equiv 1 \pmod{m}$.
a) ¿Es 5 invertible módulo 17?
b) Probar que t es invertible módulo m si y sólo si $(t, m) = 1$.
c) Determinar los invertibles módulo m , para $m = 11, 12, 16$.
- (15) 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) $a = 7^{83}$, $b = 10$.
- (16) 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) $a = 8^{25}$, $b = 127$.
- (17) Probar que si $(a, 1001) = 1$ entonces 1001 divide a $a^{720} - 1$.
- (18) Sea p primo impar.
a) 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 $x \equiv \pm 1 \pmod{p}$.
b) Sea $p = d \cdot 2^s + 1$, 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 $0 \leq r < s$.

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

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

- (20) Dada la ecuación de congruencia $21x \equiv 15(39)$, 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) (★) 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) (★) ¿Para qué valores de n es $10^n - 1$ divisible por 11?
- (24) (★) 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.
- (25) (★) El número 2^{29} tiene nueve cifras y todas distintas. ¿Cuál dígito falta? (No está permitido el uso de calculadora).