Práctico 4
Matemática Discreta I – Año 2018
FAMAF

1. Sea $n \in \mathbb{N}$. Probar que todo número de la forma $4^n - 1$ es divisible por 3.
2. Probar que el resto de dividir n^2 por 4 es igual a 0 si n es par y 1 si n es impar.
3. Probar las reglas de divisibilidad por 2, 3, 4, 5, 8, 9 y 11.
4. *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.
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 el último dígito del número
$$1^2 + 2^2 + 3^2 + \ldots + 98^2 + 99^2.$$
9. Probar que 35 divide $3^{6n} - 2^{6n}$, para cualquier entero positivo.
10. Hallar todos los x que satisfacen:

    a) $x^2 \equiv 1 \pmod{4}$, *c*) $x^2 \equiv 2 \pmod{3}$, *e*) $x^4 \equiv 1 \pmod{16}$,
    b) $x^2 \equiv x \pmod{12}$, *d*) $x^2 \equiv 0 \pmod{12}$, *f*) $3x \equiv 1 \pmod{5}$.

11. Resolver las siguientes ecuaciones:

    a) $2x \equiv -21 \pmod{8}$, *b*) $2x \equiv -12 \pmod{7}$, *c*) $3x \equiv 5 \pmod{4}$.

12. Resolver la ecuación $221x \equiv 85 \pmod{340}$. Hallar todas las soluciones x tales que $0 \leq x < 340$.

13. Resolver la ecuación en congruencia $36\,x \equiv 8 \pmod{20}$. Dar todas las soluciones x de la ecuación anterior tales que $-8 < x < 30$.

14. Dado $t \in \mathbb{Z}$, decimos que t es *inversible módulo* m si existe $h \in \mathbb{Z}$ tal que $th \equiv 1 \pmod{m}$.

    a) ¿Es 5 inversible módulo 17?

    b) Probar que t es inversible módulo m, si y sólo si $\text{mcd}(t, m) = 1$.

    c) Probar que si $\text{mcd}(a, m) = 1$ entonces la ecuación $ax \equiv b \pmod{m}$ tiene solución para x.

    d) Determinar los inversibles módulo m, para $m = 11, 12, 16$.

15. Sea p un número primo impar. Probar

    a) $(p-1)! \equiv (p-1) \equiv -1 \pmod{p}$.

    b) (El pequeño teorema de Fermat) Sea a un entero que no es divisible por p, entonces $a^{p-1} \equiv 1 \pmod{p}$.

    c) $((\frac{p-1}{2})!)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

    d) La ecuación $x^2 \equiv -1 \pmod{p}$ tiene solución si y sólo si p es un primo de la forma $4k+1$.

    [Hint: usar el pequeño teorema de Fermat].

    e) Usar el punto anterior para dar una prueba alternativa a un ejercicio del práctico anterior:

    "Si a y b son enteros entonces $a^2 + b^2$ es divisible por 7 si y sólo si a y b son divisibles por 7."

    ¿Puede plantear una generalización a dicho ejercicio y probarla?

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

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

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. Probar que si a es un entero coprimo con 561, entonces $561 \mid a^{560} - 1$. El número 561 es el número de Carmichael mas pequeño que existe.

21. ¿Para qué valores de n es $10^n - 1$ divisible por 11?

22. Hallar todos los enteros que satisfacen simultáneamente:

    $x \equiv 1 \pmod{3}, \qquad x \equiv 1 \pmod{5}, \qquad x \equiv 1 \pmod{7}.$

23. Hallar el menor entero positivo que satisface simultáneamente las siguientes congruencias:

    $x \equiv 2 \pmod{3}, \qquad x \equiv 3 \pmod{5}, \qquad x \equiv 5 \pmod{2}.$

24. Hallar 4 enteros consecutivos divisibles por 5, 7, 9 y 11 respectivamente.

25. La producción diaria de huevos en una granja es inferior a 75. Cierto día el recolector informó que la cantidad de huevos recogida era tal que contando de a 3 sobraban 2, contando de a 5 sobraban 4 y contando de a 7 sobraban 5. El capataz, dijo que eso era imposible ¿Quién tenía razón? Justificar.

26. (Raíz primitiva módulo n) Sea n un entero positivo. Un entero g se dice una *raíz primitiva módulo* n si $\forall a \in \mathbb{Z}$ tal que $\mathrm{mcd}(a,n) = 1$, existe $k \in \mathbb{N}$ tal que $a \equiv g^k \pmod{n}$. El número k en la definición anterior es llamado el *logarítmo discreto de* a *en la base* g *módulo* n. Hallar una raíz primitiva para los siguientes números: 5, 6, 12 y 15.