Práctico 4
Matemática Discreta I – Año 2019/1
FAMAF

Soluciones

1. *a*) Calcular el resto de la división de 1599 por 39 sin tener que hacer la división. (Ayuda: $1599 = 1600 - 1 = 40^2 - 1$).
   Rta: $1599 \equiv 1^2 - 1 \pmod{39}$, por lo tanto el resto es 0.

   b) Lo mismo con el resto de 914 al dividirlo por 31.
   Rta: $914 = 30^2 + 14 \equiv (-1)^2 + 14 \pmod{31}$, por lo tanto el resto es 15.

2. Sea $n \in \mathbb{N}$. Probar que todo número de la forma $4^n - 1$ es divisible por 3.
   Rta: $4^n - 1 \equiv 1^n - 1 \equiv 0 \pmod{3}$ por lo tanto $3|4^n - 1$.

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.
   Rta: Si $n = 2k$, se tiene $n^2 = 4k^2$, por lo tanto $4|n^2$. Si $n = 2k + 1$, tenemos $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$ y vale el resultado.

4. *a*) Probar las reglas de divisibilidad por 2, 3, 4, 5, 8, 9 y 11.
   Rta:
   Regla del 2. Si $n = \sum_{j=0}^{k} a_j 10^j, n \equiv \sum_{j=1}^{k} a_j 0^j + a_0$ (2) por lo tanto es divisible por 2 si y solo si su dígito de unidades lo es, o sea si termina en 0, 2, 4, 6, 8.
   Regla del 3 y 9. Como $10 \equiv 1$ (3), $\sum_{j=0}^{k} a_j 10^j \equiv \sum_{j=0}^{k} a_j 1^j$ (3). Por lo tanto $3|n$ si y sólo si 3 divide a la suma de sus dígitos. Notar que lo mismo pasa con 9 por ser $10 \equiv 1$ (9).
   Regla del 4 y 8. $10^j \equiv 0$ (4) si $j > 1$ y $10^j \equiv 0$ (8) si $j > 2$. Por lo tanto, al tomar congruencia de n módulo 4 u 8, sólo quedan las dos últimas cifras en el primer caso y las 3 últimas en el segundo. Es decir $4|n$ si y sólo si $4|10a_1 + a_0$ y $8|n$ si y sólo si $8|100a_2 + 10a_1 + a_0$.
   Regla del 11. $10 \equiv -1$ (11) $\Rightarrow n = \sum_{j=0}^{k} a_j 10^j \equiv \sum_{j=0}^{k} a_j (-1)^j$ Entonces $11|n$ si y sólo si 11 divide a la suma de los dígitos que están en lugar par menos la suma delos dígitos que están en lugar impar.

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

   12342 5176 314573 899.

Rta: $12342 = 2 \cdot 3 \cdot 11^2 \cdot 17$, $5176 = 2^3 \cdot 647$, $314573 = 7 \cdot 44939$, 899 no es divisible por ninguno de ellos.

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

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

Rta: Si ninguno es divisible por 3 tenemos que $x^2 \equiv 1\ (3)$ para $x =, a, b, c$, por lo tanto la suma de los cuadrados será congruente a 3 módulo 3 y esto dice que $3|a^2 + b^2 + c^2$.

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

Rta: Para encontrar dichas cifras tenemos que tomar congruencia módulo 100. $7^{15} = (7^2)^7 7 = (50 - 1)^7 7 \equiv (50 \cdot 7 - 1)7(100)$ donde hemos usado la fórmula binomial para $(50 - 1)^7$ y el hecho que $50^n \equiv 0(100)$ para $n > 1$. Finalmente $(50 \cdot 7 - 1)7 \equiv (50 - 1)7 \equiv 343 \equiv 43(100)$.

7. Hallar el resto en la división de x por 5 y por 7 para:

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

Rta: Sabemos que si $(a, 5) = 1$ se tiene $a^4 \equiv 1(5)$, luego cada sumando salvo 5^8 es congruente a 1 módulo 5. Su suma da entonces $7 \equiv 2(5)$.

También sabemos que $a^7 \equiv a(7) \forall a$, por lo cual la suma es congruente a $\sum_{i=1}^{8} i^2$ módulo 8. Esto es $1 + 4 + 2 + 2 + 4 + 1 + 0 + 1 = 15 \equiv 1(7)$.

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

Rta: $x = 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101 \equiv 3 \cdot 1 \cdot 2 \cdot 1 \cdot 1 \equiv 6 \equiv 1(5)$

$x = 3 \cdot 11 \cdot 17 \cdot 71 \cdot 101 \equiv 3 \cdot 4 \cdot 3 \cdot 1 \cdot 3 \equiv 108 \equiv 3(7)$.

8. Hallar todos los x que satisfacen:

a) $x^2 \equiv 1 \quad (4)$

Rta: Resolvemos primero para $0 \leq x \leq 3$ y luego sumamos un múltiplo de 4. Esto es $x = 1$ o $x = 3$ y por lo tanto $x = 1 + 4k$ o $x = 3 + 4k$, lo cual también se puede escribir como $x = 4k \pm 1$.

b) $x^2 \equiv x \quad (12)$

Rta: Soluciones menores que 12: $x = 0, 1, 4, 9, 11$. Luego el conjunto solución es $\{12k, 12k \pm 1, 12k + 4, 12k - 3\}$.

c) $x^2 \equiv 2 \quad (3)$

Rta: No tiene soluciones pues $0^2 = 0, 1^2 = 1, 2^2 \equiv 1(3)$.

d) $x^2 \equiv 0 \quad (12)$

Rta: Soluciones menores que 12: $\{0, 6, \}$. Luego las soluciones son $\{12k, 12k + 6\}$.

e) $x^4 \equiv 1 \quad (16)$

Rta: Notemos que x debe ser impar. Podemos tomar $-8 \leq x \leq 8$, es decir $x \in \{-7, -5, -3, -1, 1, 3, 5, 7\}$. Los cuadrados son $\{49, 25, 9, 1, 1, 9, 25, 49\}$ que son congruentes módulo 16 a $\{1, 9, 9, 1, 1, 9, 9, 1\}$ A su vez cuando elevamos estos al cuadrado, como $9^2 = 81 \equiv 1 \quad (16)$ Tenemos que todo número impar es solución de la ecuación.

Alternativamente podríamos elevar $2k + 1$ a la cuarta con la fórmula binomial $\sum_{j=0}^{4} \binom{4}{j} (2k)^j 1^{4-j} = 1 + 4 \cdot 2k + 6 \cdot 4k^2 + 4 \cdot 4k^3 + 16k^4 = 1 + 8(k + 3k^2) + 16(k^3 + k^4) \equiv 1 + 8(k + 3k^2) \quad (16)$. Si observamos que $k(1+3k)$ siempre es par ya que es uno de los factores es par, tenemos que $(2k+1)^4 \equiv 1 + 16(3k+1)k/2 \equiv 1 \quad (16)$.

f) $3x \equiv 1(5)$

Rta: Probamos con $x = 0, 1, 2, 3, 4$ y vemos que $3 \cdot 2 = 6 \equiv 1 \quad (5)$. Luego las soluciones son $x = 5k + 2$.

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 sólo si la ecuación

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

tiene solución.

Rta: La ecuación $\frac{a}{d} \cdot x \equiv \frac{b}{d}(\frac{m}{d})$ tiene solución si y sólo si $\frac{m}{d} | \frac{a}{d} \cdot x - \frac{b}{d}$ si y sólo si $\frac{a}{d} \cdot x - \frac{b}{d} = \frac{m}{d} q$ como $d \neq 0$ multiplicando por d, esto ocurre si y sólo si $m | a \cdot x - b$, es decir, $a \cdot x \equiv b(m)$.

10. Resolver las siguientes ecuaciones:

a) $2x \equiv -21(8)$

Como el módulo es par, no hay solución pues el miembro de la derecha es par y el de la izquierda es impar.

b) $2x \equiv -12(7)$

Rta: $x = 1 + 7k, k \in \mathbb{Z}$.

c) $3x \equiv 5(4)$.

Rta: $x = 3 + 4k, k \in \mathbb{Z}$.

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

    Rta: Notemos que 221, 85 y 340 son divisibles por 17 Sus respectivos cocientes son 13, 5 y 20. Por el ejercicio 9 podemos entonces resolver $13x \equiv 5(20)$. Las soluciones de esta ecuación deben ser múltiplos de 5 y menores que 20. Comprobamos que 5 es la única solución menor que 20. las restantes son de la forma $20k + 5$. Tenemos que el conjunto buscado es: $\{5, 25, 45, \ldots, 305, 325\} = \{5 + 20k, \}_{k=1}^{20}$.

12. (i) Encontrar todas las soluciones de la ecuación en congruencia

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

    usando el método visto en clase.

    Rta: $(36, 20) = 4 \Rightarrow 36 - 20 = 16, 20 - 16 = 4, \Rightarrow 2 \cdot 20 - 36 = 4$. Por lo tanto $(-2)36 = 8 - 4 \cdot 20$, Esto es $x = -2 + 20k$.

    Alternativa: La ecuación es equivalente a $9x \equiv 2\ (5)$ el único resto que la satisface es 3. Las soluciones de esta ecuación son $5k + 3, k \in \mathbb{Z}$. Entre los restos módulo 20, la única que satisface la ecuación original es $3 + 5 \cdot 3 = 18$ y a esta se le deben sumar los múltiplos de 20.

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

    Rta: $\{-2, 18\}$.

13. (i) Encontrar todas las soluciones de la ecuación en congruencia

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

    usando el método visto en clase.

    Rta: La ecuación es equivalente a: $7x \equiv 2\ (10)$. Ahora bien $1 = (7, 10)$ y $1 = (-7) \cdot 7 + 5 \cdot 10$, por lo tanto $2 = (-14) \cdot 7 + 10 \cdot 10$. Haciendo congruencia módulo 10 obtenemos: $2 \equiv (-14) \cdot 7 \equiv 6 \cdot 7\ (10)$. Luego la ecuación tiene como soluciones $x = 10k + 6$, con k entero.

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

    Rta: 6, 16, 26.

14. 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?

    Rta: Si, $5 \cdot 7 \equiv 1\ (17)$

b) Probar que t es inversible módulo m, si y sólo si $(t, m) = 1$.

Rta: Si t es inversible módulo m sea h tal que $th \equiv 1(m)$. Esto es $th - 1 = mq$, y por lo tanto $1 = th - mq$, lo cual dice que $(t, m) = 1$. Recíprocamente si $(t, m) = 1$ existen enteros h y q tales que $1 = th + mq$ y esto nos dice que m divide a $1 - th$ o sea $th \equiv 1(m)$.

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

Rta: $\{1, 2, 3, \dots, 9, 10\}, \{1, 5, 7, 11\}, \{1, 3, 5, 7, 9, 11, 13, 15\}$.

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

Rta: Si resolvemos $x^2 \equiv 9\ (3)$ vemos que 3 y 16 son los únicos restos que son solución. Luego, todas las soluciones buscadas son $19k \pm 3$.

16. 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 $a^{2^n} \equiv 1\ (2^{n+2})$?

Rta: Si $n = 1$, $a^2 - 1$ es divisible por 8 ya que $a^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k = 4k(k+1)$ y $2|k(k+1)$.

Si $a^{2^n} \equiv 1\ (2^{n+2})$ entonces 2^{n+2} divide a $a^{2^n} - 1$ multiplicando por $a^{2^n} + 1$, que es par, tenemos que 2^{n+1+2} divide a $(a^{2^n} - 1)(a^{2^n} + 1) = a^{2^{n+1}} - 1$.

17. Encontrar el resto en la división de a por b en los siguientes casos:

a) $a = 11^{13} \cdot 13^8; b = 12$; *Rta:* $11^{13} \cdot 13^8 \equiv (-1)^{13} \cdot 1^8 \equiv 11\ (12)$.

b) $a = 4^{1000}; b = 7$; *Rta:* $4^{1000} = (4^6)^{166} 4^4 \equiv (4^2)^2 \equiv 2^2\ (12)$.

c) $a = 123^{456}; b = 31$; *Rta:* $123^{456} \equiv (-1)^{456} \equiv 1\ (31)$.

d) $a = 7^{83}; b = 10$. *Rta:* $7^{83} = (7^4)^{20} 7^3 \equiv 1^{20} 343 \equiv 3\ (10)$.

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

Rta: $2^{21} = 2^{13} 2^8 \equiv 2 \cdot 2^8\ (13)$ Como $2^3 2^9 = 2^{12} \equiv 1\ (13)$, se tiene $8 2^9 \equiv 1\ (13)$ y esto dice que $2^9 \equiv 5\ (13)$ ya que $8 \cdot 5 = 3 \cdot 13 + 1$.

$3^8 = 3^4 \cdot 3^4 \equiv 1 \cdot 1\ (13)$.

$8^{25} = 2^{75}$ como $2^7 = 128 \equiv 1\ (127)$; tenemos que $2^{75} = (2^7)^{10} 2^5 \equiv 2^5\ (127)$. Por lo tanto $8^{25} \equiv 32\ (127)$

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

Rta: Si x, y, z fuesen solución y tuvieran un factor común t es claro que también $x/t, y/t.z/t$ cumpliría las condiciones. Luego podemos asumir que x, y, z no tienen factor en común salvo ± 1.

Si tomamos congruencia módulo 3 en ambos miembros vemos que la suma de dos cuadrados módulo 3 sólo puede ser 0si ambos números son divisibles por 3. Luego $x = 3a, y = 3b$, y por lo tanto $x^2 = 9a^2, y^2 = 9b^2$. Podemos simplificar la ecuación y obtenemos $3a^2 + 3b^2 = z^2$. Tomando congruencia módulo 3 nuevamente tenemos que 3 divide a z^2 y por lo tanto divide a z. Esto contradice el hecho que x, y, z no tenían factor común.

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

Rta: Aquí también podemos asumir que a, b, r no tienen factores en común. Tomando congruencia módulo 3 vemos que 3 divide a r o sea $r = 3t, r^2 = 9t^2$. Reemplazando y simplificando tenemos $a^2+b^2 = 3t^2$, que sabemos por el inciso anterior que no tiene solución.

20. Probar que si $(a, 1001) = 1$ entonces 1001 divide a $a^{720} - 1$.
Rta: Notemos que $1001 = 7 \cdot 11 \cdot 13$. Por lo tanto $(a, 1001) = 1$ implica $(a, 7) = (a, 11) = (a, 13) = 1$. Entonces $a^6 \equiv 1\ (7); a^{10} \equiv 1\ (11)$ y $a^{12} \equiv 1\ (13)$. Por lo tanto $a^{720} = ((a^6)^{10})^{12} \equiv 1\ (7 \cdot 11 \cdot 13)$.

(*): ejercicios opcionales de mayor dificultad.

21. (*) ¿Para qué valores de n es $10^n - 1$ divisible por 11?
Rta: Como $10 \equiv -1\ (11)$, se tiene $10^n - 1 \equiv (-1)^n - 1\ (11)$. Entonces $10^n - 1$ es divisible por 11 si y solo si n es par.

22. (*) 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.
Rta: Notemos que si fuera posible dicha partición. el $n + 2$ dividiría a ambos productos y uno de ellos no lo contiene. Entonces $n + 2$ debe dividir a $(n + 2 - 2)(n+2-1)(n+2+1)(n+2+2)(n+2+3)$. Esto nos dice que $n+2$ debe dividir a $(-1)(-2) \cdot 1 \cdot 2 \cdot 3 = 12$. Las posibilidades para $n+2$ son entonces: 1, 2, 3, 4, 6,12. Pero 1 y 2 dan $n \leq 0$ y las restantes dan $n \in \{1, 2, 4, 10\}$. Las primera no puede ser pues en el conjunto {1,2,3,4,5,6} hay un único elemento divisible por 5, que debería ser divisor de ambos productos de la partición. La misma razón dice que n no puede ser 2 ni 4. Finalmente si $n = 10$, el conjunto sería $\{10, 11, 12, 13, 14, 15\}$

que posee un único elemento divisible por 7 (el 14) y vale el mismo razonamiento que antes con 7 en lugar de 5.

Alternativamente: Notemos que 7 divide a lo sumo a uno de los 6 números. Si $\prod_{i=0}^{5}(n+i) = u_1 u_2$ con $u_1 = u_2$, entonces 7 no divide a ninguno de los factores ya que si divide a un factor de u_1 divide a un factor de u_2. Tenemos así que las congruencias módulo 7 dan los 6 restos posibles y su producto 720 es congruente a 6 módulo 7. Pero entonces $u_1^2 = u_1 u_2 \equiv 720 \equiv 6$ (7) se tendría que 6 es un cuadrado módulo 7 lo cual es falso.

23. (*) El número 2^{29} tiene nueve dígitos y todos son distintos. ¿Cuál dígito falta? (No está permitido el uso de calculadora).

    Rta: Primero nos planteamos la siguiente pregunta, ¿Cuánto suman sus dígitos? Si $2^{29} = \sum_{i=0}^{8} a_i 10^i$, entonces $\sum_{i=0}^{8} a_i = \sum_{i=0}^{9} i - d$, donde d es el dígito que falta. Esto es $\sum_{i=0}^{8} a_i = 45 - d$. Además $2^{29} = \sum_{i=0}^{8} a_i 10^i \equiv \sum_{i=0}^{8} a_i$ (9). Entonces si calculamos esta congruencia podemos obtener d: $2^{29} = (2^6)^4 2^5 \equiv 2^5$ (9) y $2^5 \equiv 5$ (9) por lo tanto $d \equiv -5$ (9) o sea $d = 4$ es el dígito faltante.