Álgebra I
Práctica 4 - Números enteros (Parte 1)

Divisibilidad

1. Decidir cuáles de las siguientes afirmaciones son verdaderas $\forall\, a, b, c \in \mathbb{Z}$

   (a) $a \cdot b \mid c \Rightarrow a \mid c \;$ y $\; b \mid c$
   (b) $4 \mid a^2 \Rightarrow 2 \mid a$
   (c) $2 \mid a \cdot b \Rightarrow 2 \mid a \;$ ó $\; 2 \mid b$
   (d) $9 \mid a \cdot b \Rightarrow 9 \mid a \;$ ó $\; 9 \mid b$
   (e) $a \mid b + c \Rightarrow a \mid b \;$ ó $\; a \mid c$
   (f) $a \mid c \;$ y $\; b \mid c \Rightarrow a \cdot b \mid c$
   (g) $a \mid b \Rightarrow a \leq b$
   (h) $a \mid b \Rightarrow |a| \leq |b|$
   (i) $a \mid b + a^2 \Rightarrow a \mid b$
   (j) $a \mid b \Rightarrow a^n \mid b^n, \forall\, n \in \mathbb{N}$

2. Hallar todos los $n \in \mathbb{N}$ tales que

   (a) $3n - 1 \mid n + 7$
   (b) $3n - 2 \mid 5n - 8$
   (c) $2n + 1 \mid n^2 + 5$
   (d) $n - 2 \mid n^3 - 8$

3. Sean $a, b \in \mathbb{Z}$.

   (a) Probar que $a - b \mid a^n - b^n$ para todo $n \in \mathbb{N}$ y $a \neq b \in \mathbb{Z}$.
   (b) Probar que si n es un número natural par y $a \neq -b$, entonces $a + b \mid a^n - b^n$.
   (c) Probar que si n es un número natural impar y $a \neq -b$, entonces $a + b \mid a^n + b^n$.

4. Sea a un entero impar. Probar que $2^{n+2} \mid a^{2^n} - 1$ para todo $n \in \mathbb{N}$.

5. Sea $n \in \mathbb{N}$.

   (a) Probar que si n es compuesto, entonces $2^n - 1$ es compuesto.
   (Los primos de la forma $2^p - 1$ para p primo se llaman *primos de Mersenne*, por Marin Mersenne, monje y filósofo francés, 1588-1648. Se conjetura que existen infinitos primos de Mersenne, pero aún no se sabe. Se conocen a la fecha 51 primos de Mersenne (Enero 2021). El más grande producido hasta ahora es $2^{82.589.933} - 1$, que tiene 24.862.048 dígitos, y es el número primo más grande conocido a la fecha.)
   (b) Probar que si $2^n + 1$ es primo, entonces n es una potencia de 2.
   (Los números de la forma $\mathcal{F}_n = 2^{2^n} + 1$ se llaman *números de Fermat*, por Pierre de Fermat, juez y matemático francés, 1601-1665. Fermat conjeturó que cualquiera sea $n \in \mathbb{N}_0$, $\mathcal{F}_n$ era primo, pero esto resultó falso: los primeros $\mathcal{F}_0 = 3,\ \mathcal{F}_1 = 5,\ \mathcal{F}_2 = 17,\ \mathcal{F}_3 = 257,\ \mathcal{F}_4 = 65537$, son todos primos, pero $\mathcal{F}_5 = 4294967297 = 641 \times 6700417$. Hasta ahora no se conocen más primos de Fermat que los 5 primeros mencionados.)

6. (a) Probar que el producto de n enteros consecutivos es divisible por $n!$.
   (b) Probar que $\binom{2n}{n}$ es divisible por 2.

7. Probar que las siguientes afirmaciones son verdaderas para todo $n \in \mathbb{N}$

   (a) $99 \mid 10^{2n} + 197$
   (b) $9 \mid 7 \cdot 5^{2n} + 2^{4n+1}$
   (c) $56 \mid 13^{2n} + 28n^2 - 84n - 1$
   (d) $256 \mid 7^{2n} + 208n - 1$

Algoritmo de División

8. Calcular el cociente y el resto de la división de a por b en los casos:

   (a) $a = 133, \quad b = -14$.
   (b) $a = 13, \quad b = 111$.
   (c) $a = 3b + 7, \quad b \neq 0$.
   (d) $a = b^2 - 6, \quad b \neq 0$.
   (e) $a = n^2 + 5, \quad b = n + 2 \ (n \in \mathbb{N})$.
   (f) $a = n + 3, \quad b = n^2 + 1 \ (n \in \mathbb{N})$.

9. Sabiendo que el resto de la división de un entero a por 18 es 5, calcular el resto de

   (a) la división de $a^2 - 3a + 11$ por 18.
   (b) la división de a por 3.
   (c) la división de $4a + 1$ por 9.
   (d) la división de $7a^2 + 12$ por 28.

10. (a) Si $a \equiv 22 \ (14)$, hallar el resto de dividir a a por 14, por 2 y por 7.
    (b) Si $a \equiv 13 \ (5)$, hallar el resto de dividir a $33a^3 + 3a^2 - 197a + 2$ por 5.
    (c) Hallar, para cada $n \in \mathbb{N}$, el resto de la división de $\displaystyle\sum_{i=1}^{n} (-1)^i \cdot i!$ por 12.

11. (a) Probar que $a^2 \equiv -1 \ (5) \Leftrightarrow a \equiv 2 \ (5)$ ó $a \equiv 3 \ (5)$.
    (b) Probar que no existe ningún entero a tal que $a^3 \equiv -3 \ (7)$.
    (c) Probar que $a^7 \equiv a \ (7)$ para todo $a \in \mathbb{Z}$.
    (d) Probar que $7 \mid a^2 + b^2 \Leftrightarrow 7 \mid a$ y $7 \mid b$.
    (e) Probar que $5 \mid a^2 + b^2 + 1 \Rightarrow 5 \mid a$ ó $5 \mid b$ ¿Vale la implicación recíproca?

12. (a) Probar que $2^{5k} \equiv 1 \ (31)$ para todo $k \in \mathbb{N}$.
    (b) Hallar el resto de la división de 2^{51833} por 31.
    (c) Sea $k \in \mathbb{N}$. Sabiendo que $2^k \equiv 39 \ (31)$, hallar el resto de la división de k por 5.
    (d) Hallar el resto de la división de $43 \cdot 2^{163} + 11 \cdot 5^{221} + 61^{999}$ por 31.

13. Se define por recurrencia la sucesión $(a_n)_{n \in \mathbb{N}}$:

$$a_1 = 3, \quad a_2 = -5 \ \text{ y } \ a_{n+2} = a_{n+1} - 6^{2n} \cdot a_n + 21^n \cdot n^{21} \text{ para todo } n \in \mathbb{N}.$$

    Probar que $a_n \equiv 3^n (\text{mod } 7)$ para todo $n \in \mathbb{N}$.

Sistemas de numeración

14. (a) Hallar el desarrollo en base 2 de

    i. 1365 ii. 2800 iii. $3 \cdot 2^{13}$ iv. $13 \cdot 2^n + 5 \cdot 2^{n-1}$

    (b) Hallar el desarrollo en base 16 de 2800.

15. Sea $a = (a_d a_{d-1} \dots a_1 a_0)_2$ un número escrito en base 2 (o sea escrito en bits). Determinar simplemente cómo son las escrituras en base 2 del número $2a$ y del número $a/2$ cuando a es par, o sea las operaciones "multiplicar por 2" y "dividir por 2" cuando se puede. Esas operaciones se llaman *shift* en inglés, o sea corrimiento, y son operaciones que una computadora hace en forma sencilla.

16. Enunciar y demostrar criterios de divisibilidad por 8 y por 9.

17. (a) Sea $k \in \mathbb{N}$, $k = (aaaa)_7$. Probar que $8 \mid k$.
    (b) Sea $k \in \mathbb{N}$, $k = (\underbrace{a \dots a}_{d})_7$. Determinar para qué valores de $d \in \mathbb{N}$ se tiene que $8 \mid k$.

Máximo común divisor

18. En cada uno de los siguientes casos calcular el máximo común divisor entre a y b y escribirlo como combinación lineal entera de a y b:

    (a) $a = 2532$, $b = 63$.
    (b) $a = 131$, $b = 23$.
    (c) $a = n^4 - 3$, $b = n^2 + 2$ $(n \in \mathbb{N})$.

19. Sean $a, b \in \mathbb{Z}$. Sabiendo que el resto de dividir a a por b es 27 y que el resto de dividir b por 27 es 21, calcular $(a : b)$.

20. Sea $a \in \mathbb{Z}$.

    (a) Probar que $(5a + 8 : 7a + 3) = 1$ o 41. Exhibir un valor de a para el cual da 1, y verificar que efectivamente para $a = 23$ da 41.
    (b) Probar que $(2a^2 + 3a - 1 : 5a + 6) = 1$ o 43. Exhibir un valor de a para el cual da 1, y verificar que efectivamente para $a = 16$ da 43.
    (c) Probar que $(a^2 - 3a + 2 : 3a^3 - 5a^2) = 2$ ó 4, y exhibir un valor de a para cada caso.
    (Para este ítem es **indispensable** mostrar que el máximo común divisor nunca puede ser 1).

21. Sean $a, b \in \mathbb{Z}$ coprimos. Probar que $7a - 3b$ y $2a - b$ son coprimos.

22. Sean $a, b \in \mathbb{Z}$ con $(a : b) = 2$. Probar que los valores posibles para $(7a + 3b : 4a - 5b)$ son 2 y 94. Exhibir valores de a y b para los cuales da 2 y para los cuales da 94.

23. (a) Determinar todos los $a, b \in \mathbb{Z}$ coprimos tales que $\dfrac{b+4}{a} + \dfrac{5}{b} \in \mathbb{Z}$.
    (b) Determinar todos los $a, b \in \mathbb{Z}$ coprimos tales que $\dfrac{9a}{b} + \dfrac{7a^2}{b^2} \in \mathbb{Z}$.
    (c) Determinar todos los $a \in \mathbb{Z}$ tales que $\dfrac{2a+3}{a+1} + \dfrac{a+2}{4} \in \mathbb{Z}$.

Primos y factorización

24. Probar que existen infinitos primos positivos congruentes a 3 módulo 4.
    Sugerencia: probar primero que si $a \in \mathbb{N}$ satisface $a \equiv 3 \pmod 4$, entonces existe p primo con $p \equiv 3 \pmod 4$ tal que $p \,|\, a$. Luego probar que si existieran sólo finitos primos congruentes a 3 módulo 4, digamos $p_1, p_2, \ldots, p_n$, entonces $a = -1 + 4 \displaystyle\prod_{i=1}^{n} p_i$ sería mayor que 1 y no es divisible por ningún primo congruente a 3 módulo 4.

25. Sea p primo positivo.

    (a) Probar que si $0 < k < p$, entonces $p \mid \dbinom{p}{k}$.
    (b) Probar que si $a, b \in \mathbb{Z}$, entonces $(a + b)^p \equiv a^p + b^p \pmod p$.

26. Decidir si existen enteros a y b no nulos que satisfagan

    (a) $a^2 = 3b^3$
    (b) $7a^2 = 8b^2$

27. Sea $n \in \mathbb{N}$, $n \geq 2$. Probar que si p es un primo positivo entonces $\sqrt[n]{p} \notin \mathbb{Q}$.

28. Sean p y q primos positivos distintos. Probar que $p^{113} \cdot q^{201} \mid a^{378}$ si y sólo si $p\,q \mid a$.

29. Determinar cuántos divisores positivos tienen 9000, $15^4 \cdot 42^3 \cdot 56^5$ y $10^n \cdot 11^{n+1}$. ¿ Y cuántos divisores en total ?

30. Hallar la suma de los divisores positivos de $2^4 \cdot 5^{123}$ y de $10^n \cdot 11^{n+1}$.

31. Hallar el menor número natural n tal que $6552\,n$ sea un cuadrado, es decir, que exista $k \in \mathbb{N}$ tal que $6552\,n = k^2$.

32. Sean $a, b \in \mathbb{N}$, $a, b \geq 2$. Probar que si ab es un cuadrado en $\mathbb{N}$ y $(a : b) = 1$, entonces tanto a como b son cuadrados en $\mathbb{N}$.

33. Hallar todos los $n \in \mathbb{N}$ tales que

    (a) $(n : 945) = 63$, $(n : 1176) = 84$ y $n \leq 2800$

    (b) $(n : 1260) = 70$ y n tiene 30 divisores positivos

34. Hallar el menor número natural n tal que $(n : 3150) = 45$ y n tenga exactamente 12 divisores positivos.

35. (a) Sea $k \in \mathbb{N}$. Probar que $(2^k + 7^k : 2^k - 7^k) = 1$.

    (b) Sea $k \in \mathbb{N}$. Probar que $(2^k + 5^{k+1} : 2^{k+1} + 5^k) = 3$ ó 9, y dar un ejemplo para cada caso.

    (c) Caracterizar para cada $k \in \mathbb{N}$ el valor que toma $\big(12^k - 1 : 12^k + 1286\big)$.

36. Sean $a, b \in \mathbb{Z}$. Probar que si $(a : b) = 1$ entonces $(a^2 \cdot b^3 : a + b) = 1$.

37. Sean $a, b \in \mathbb{Z}$ tales que $(a : b) = 5$.

    (a) Calcular los posibles valores de $(ab : 5a - 10b)$ y dar un ejemplo para cada uno de ellos.

    (b) Para cada $k \in \mathbb{N}$, calcular $(a^{k-1}b : a^k + b^k)$.

38. (a) Sean $a, b \in \mathbb{Z}$ tales que $(a : b) = 3$. Calcular los posibles valores de $\big(a^2 + 15b + 57 : 4050\big)$ y dar un ejemplo para cada caso.

    (b) Sean $a, b \in \mathbb{Z}$. Sabiendo que $b \equiv 6 \pmod{24}$ y que $(a : b) = 13$, calcular $(5a^2 + 11b + 117 : 624)$.

39. Hallar todos los $n \in \mathbb{N}$ tales que

    (a) $[n : 130] = 260$.

    (b) $[n : 420] = 7560$.

40. Hallar todos los $a, b \in \mathbb{N}$ tales que

    (a) $(a : b) = 10$ y $[\,a : b\,] = 1500$.

    (b) $3 \mid a$, $(a : b) = 20$ y $[a : b] = 9000$.