Propiedades de números enteros
(lista de problemas para examen)

Denotamos por $\mathbb{Z}$ al conjunto de los números enteros y por $\mathbb{N}$ al conjunto de los números enteros positivos:

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

Valor absoluto de números enteros

1. Definición (valor absoluto de números enteros). El *valor absoluto* (o *módulo*) de un número entero a se define de la siguiente manera:

$$|a| := \begin{cases} a, & \text{si } a \geq 0; \\ -a, & \text{si } a < 0. \end{cases}$$

2. Algunas propiedades simples del valor absoluto. Demuestre las siguientes propiedades suponiendo que $a, b \in \mathbb{Z}$:

1. $|a| \geq 0$.
2. $a \leq |a|$.
3. $|ab| = |a|\,|b|$.
4. $|-a| = |a|$.
5. $-a \leq |a|$.
6. $-|a| \leq a$.
7. $-|a| \leq a \leq |a|$.

3. Igualdad $|a| = b$ con $b \geq 0$. Sean $a, b \in \mathbb{Z}$, y $b \geq 0$. Demuestre que

$$|a| = b \qquad \Longleftrightarrow \qquad (a = b \quad \vee \quad a = -b).$$

4. Igualdad $|a| = |b|$. Sean $a, b \in \mathbb{Z}$. Demuestre que

$$|a| = |b| \qquad \Longleftrightarrow \qquad (a = b \quad \vee \quad a = -b).$$

5. Desigualdad $|a| \leq b$. Sean $a, b \in \mathbb{Z}$, $b \geq 0$. Demuestre que

$$|a| \leq b \qquad \Longleftrightarrow \qquad (-b \leq a \quad \wedge \quad a \leq b).$$

6. Propiedad subaditiva del valor absoluto (también se conoce como la desigualdad triangular). Sean $a, b \in \mathbb{Z}$. Demuestre que

$$|a + b| \leq |a| + |b|.$$

7. Un hecho sobre números enteros positivos (sin demostración).
Sea $m \in \mathbb{Z}$ tal que $m > 0$. Entonces $m \geq 1$.

8. Teorema (sobre el valor absoluto de números enteros no nulos).
Sea $a \in \mathbb{Z}$ tal que $a \neq 0$. Demuestre que $|a| \geq 1$.

Divisibilidad

9. Definición (divisibilidad de números enteros). Sean $a, b \in \mathbb{Z}$. Se dice que a *divide* a b y se escribe $a \mid b$ si existe $k \in \mathbb{Z}$ tal que $b = ka$. En este caso se dice también que b es un *múltiplo* de a, y que a es un *divisor* de b.

10. Propiedad transitiva de la divisibilidad. Sean $a, b, c \in \mathbb{Z}$ tales que $a \mid b$ y $b \mid c$. Demuestre que $a \mid c$.

11. Teorema sobre la divisibilidad de la suma de productos. Sean $a, b, m, n, d \in \mathbb{Z}$, $d \mid a$, $d \mid b$. Demuestre que $d \mid (ma + nb)$.

Las siguientes dos afirmaciones se pueden obtener como casos particulares del teorema anterior, pero se recomienda demostrarlas de manera independiente.

12. Corolario sobre la divisibilidad de la suma y resta. Sean $a, b, d \in \mathbb{Z}$ tales que $d \mid a$ y $d \mid b$. Demuestre que $d \mid (a + b)$ y $d \mid (a - b)$.

13. Corolario sobre la divisibilidad de un múltiplo. Sean $a, d, n \in \mathbb{Z}$, $d \mid a$. Demuestre que $d \mid (na)$.

14. Corolario sobre la divisibilidad de un sumando. Sean $d, a_1, \ldots, a_n \in \mathbb{Z}$ tales que

$$d \mid a_1, \quad d \mid a_2, \quad \ldots, \quad d \mid a_{n-1}, \quad d \mid (a_1 + \cdots + a_n).$$

Entonces $d \mid a_n$.

15. Sean $a, b, c \in \mathbb{Z}$, $a \mid b$. Demuestre que $(ac) \mid (bc)$.

16. Sean $a, b \in \mathbb{Z}$. Demuestre que

$$a \mid b \quad \Longleftrightarrow \quad a \mid (-b).$$

17. Sean $a, b \in \mathbb{Z}$. Demuestre que

$$a \mid b \quad \Longleftrightarrow \quad (-a) \mid b.$$

18. Sean $a, b \in \mathbb{Z}$. Demuestre que

$$a \mid b \quad \Longleftrightarrow \quad |a| \mid |b|.$$

19. Notación (múltiplos enteros de un número entero). Sea $n \in \mathbb{Z}$. Entonces el conjunto de los múltiplos enteros de n se denota por $n\mathbb{Z}$:

$$n\mathbb{Z} \coloneqq \big\{a \in \mathbb{Z}\colon \quad \exists k \in \mathbb{Z} \quad a = nk\big\}.$$

20. Múltiplos enteros de cero. Encontrar todos los números enteros que son múltiplos de 0.

21. Múltiplos enteros de uno. Encontrar todos los números enteros que son múltiplos de 1.

22. Notación (el conjunto de los divisores enteros de un número entero). Sea $a \in \mathbb{Z}$. Denotemos por $\mathcal{D}(a)$ al conjunto de los divisores enteros de a:

$$\mathcal{D}(a) \coloneqq \{b \in \mathbb{Z}: \quad b \mid a\}.$$

23. Sea $n \in \mathbb{Z}$. Demuestre que

$$\mathcal{D}(n) = \mathcal{D}(-n).$$

24. Sea $n \in \mathbb{Z}$. Demuestre que

$$\mathcal{D}(n) = \mathcal{D}(|n|).$$

25. Divisores enteros de cero. Halle $\mathcal{D}(0)$.

26. Teorema sobre la divisibilidad y comparación de valores absolutos. Sean $a, b \in \mathbb{Z}$ tales que $a \mid b$ y $b \neq 0$. Demuestre que $|a| \leq |b|$.

27. Sean $a, b \in \mathbb{Z}$ tales que $a \mid b$ y $b > 0$. Demuestre que $|a| \leq b$.

28. Divisores enteros de uno. Halle $\mathcal{D}(1)$.

29. Sea x un número entero que divide a cualquier número entero. Demuestre que $x = 1$ o $x = -1$.

30. Sean $a, b \in \mathbb{Z}$ tales que $a \mid b$ y $b \mid a$. Demuestre que $a = b$ o $a = -b$.

31. Usando la inducción matemática demuestre que $6 \mid (19^n + 5)$ para cada $n \in \mathbb{N}$.

División con resto

32. Teorema sobre la división con resto. Sean $a, b \in \mathbb{Z}$, $b > 0$. Entonces existe un único par $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ tales que $a = bq + r$ y $0 \leq r < b$.

Indicación: en el examen se puede incluir solamente la demostración de la unicidad en el teorema anterior.

33. Divisibilidad y resto. Sean $a, b \in \mathbb{Z}$, $b > 0$. Demuestre que $b \mid a$ si y sólo si, el resto al dividir a entre b es 0.

Máximo común divisor

34. Definición. Escriba la definición del máximo común divisor.

35. Sean $a, b \in \mathbb{Z}$ no ambos cero. Demuestre que

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(|a|, |b|).$$

36. Sea $a \in \mathbb{Z}$, $a > 0$. Demuestre que $\mathrm{mcd}(a, 0) = a$.

37. Sean $a, b \in \mathbb{Z}$, $a \mid b$, $a > 0$. Demuestre que $\mathrm{mcd}(a, b) = a$.

38. Sea $a \in \mathbb{Z}$, $a \neq 0$. Demuestre que $\mathrm{mcd}(a, 0) = |a|$.

39. Sean $a, b \in \mathbb{Z}$, $a \mid b$, $a \neq 0$. Demuestre que $\mathrm{mcd}(a, b) = |a|$.

40. Teorema sobre MCD que sirve como una base del algoritmo de Euclides. Sean $a, b, q, r \in \mathbb{Z}$ tales que $a \neq 0$ o $b \neq 0$, y $a = bq + r$. Demuestre que $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$.

41. Algoritmo de Euclides. Describa el algoritmo de Euclides con fórmulas matemáticas.

Los siguientes dos problemas de programación no se incluyen en el examen.

42. Programación: algoritmo de Euclides con un ciclo while. En algún lenguaje de programación escriba una función de dos argumentos enteros a, b que calcule y regrese el máximo común divisor de a y b. Utilice un ciclo de tipo `while` y la idea del algoritmo de Euclides.

43. Programación: algoritmo de Euclides en forma recursiva. En algún lenguaje de programación escriba una función de dos argumentos enteros a, b que calcule y regrese el máximo común divisor de a y b. Utilice la recursión.

Algoritmo extendido de Euclides. Coeficientes de Bézout

44. Lema para entender el cálculo de los coeficientes de Bézout. Supongamos que

$$r_1 = au_1 + bv_1, \qquad r_2 = au_2 + bv_2, \qquad r_1 = r_2q + r_3.$$

Encuentre u_3, v_3 tales que

$$r_3 = au_3 + bv_3.$$

45. Algoritmo extendido de Euclides. Describa con fórmulas el algoritmo extendido de Euclides.

Dados $a, b \in \mathbb{Z}$ no ambos cero, el algoritmo extendido de Euclides construye una terna (d, u, v) de números enteros tal que $d = \operatorname{mcd}(a, b)$ y $au + bv$. En algunos de los siguientes problemas utilizamos la existencia de u y v.

46. Sean $a, b \in \mathbb{Z}$ no ambos cero y sea $d = \operatorname{mcd}(a, b)$. Demuestre que si $m \in \mathbb{Z}$ tal que $m \mid a$ y $m \mid b$, entonces $m \mid d$. Indicación: utilizar u y v proporcionados por el algoritmo extendido de Euclides.

47. Descripción del conjunto de los divisores comunes de dos números enteros. Sean $a, b \in \mathbb{Z}$ no ambos cero y sea $d = \operatorname{mcd}(a, b)$. Demuestre que

$$\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(d).$$

48. Sean $a, b, u, v, d \in \mathbb{Z}$ tales que $d > 0$, $d \mid a$, $d \mid b$, $au + bv = d$. Demuestre que $\operatorname{mcd}(a, b) = d$.

49. Descripción del conjunto de las combinaciones lineales enteras de dos números enteros. Sean $a, b \in \mathbb{Z}$ no ambos cero y sea $d = \operatorname{mcd}(a, b)$. Demuestre que

$$\big\{x \in \mathbb{Z}\colon \quad \exists j, k \in \mathbb{Z} \quad x = aj + bk\big\} = \big\{x \in \mathbb{Z}\colon \quad \exists q \in \mathbb{Z} \quad x = dq\big\}.$$

En otras palabras, las combinaciones lineales enteras de a y b son los múltiplos enteros de d, y viceversa.

50. El máximo común divisor es el mínimo elemento positivo entre las combinaciones lineales enteras. Sean $a, b \in \mathbb{Z}$ no ambos cero y sea $d = \operatorname{mcd}(a, b)$. Demuestre que d es el mínimo elemento del conjunto

$$\big\{x \in \mathbb{N}\colon \quad \exists s, t \in \mathbb{Z} \quad x = as + bt\big\}.$$

51. Sean $a, b \in \mathbb{Z}$ no ambos cero, y sea $k \in \mathbb{N}$. Demuestre que $\operatorname{mcd}(ka, kb) = k \operatorname{mcd}(a, b)$.

Varios problemas sobre la divisibilidad y MCD

52. Aplique el algoritmo extendido de Euclides a los números 36, 42, luego resuelva en números enteros x, y la ecuación

$$36x + 42y = 24.$$

53. Encuentre $\mathrm{mcd}(8, 18)$, luego demuestre que la siguiente ecuación no tiene ninguna solución en números enteros:

$$8x + 18y = 27.$$

54. Sean $a, b \in \mathbb{Z}$ no ambos cero y sea $d = \mathrm{mcd}(a, b)$. Demuestre que la ecuación $ax+by = c$ tiene solución en números enteros si, y sólo si, $d \mid c$.

55. Sean $a, b, c \in \mathbb{Z}$, $d = \mathrm{mcd}(a, b)$, $a \mid c$, $b \mid c$. Demuestre que $(ab) \mid (cd)$.

56. Sean $a, b \in \mathbb{Z}$ tales que $a^2 \mid b^2$. Demuestre que $a \mid b$.

57. Sea $a \in \mathbb{N}$ tal que $a \neq k^2$ para todo $k \in \mathbb{N}$. Demuestre $\sqrt{a} \notin \mathbb{Q}$, esto es, no existe ningún par (m, n) de números naturales tal que $a = \frac{m^2}{n^2}$.

Primos relativos

58. Definición (primos relativos). Sean $a, b \in \mathbb{Z}$ no ambos cero. Decimos que a y b son *primos relativos* (o *coprimos*) si $\mathrm{mcd}(a, b) = 1$.

Por el algoritmo extendido de Euclides, si a y b son primos relativos, entonces existen $u, v \in \mathbb{Z}$ tales que $au + bv = 1$. El siguiente problema muestra que la afirmación inversa también es cierta.

59. Sean $a, b \in \mathbb{Z}$ tales que existen $u, v \in \mathbb{Z}$ con $au+bv = 1$. Demuestre que $\mathrm{mcd}(a, b) = 1$.

60. Sean $a, b, c \in \mathbb{Z}$ tales que $a \mid bc$ y $\mathrm{mcd}(a, b) = 1$. Demuestre que $a \mid c$.

61. Sean $a, b, s, t \in \mathbb{Z}$, $d = \mathrm{mcd}(a, b)$, $as + bt = d$. Demuestre que $\mathrm{mcd}(s, t) = 1$.

62. Sean $a, b, m, n \in \mathbb{Z}$, $d = \mathrm{mcd}(a, b)$, $a = md$, $b = nd$. Demuestre que $\mathrm{mcd}(m, n) = 1$.

63. Sean $a, b, c \in \mathbb{Z}$ tales que $c \mid a$ y $\mathrm{mcd}(a, b) = 1$. Demuestre que $\mathrm{mcd}(c, b) = 1$.

64. Sean $a, b \in \mathbb{Z}$ tales que $\mathrm{mcd}(a, b) = 1$. Demuestre que $\mathrm{mcd}(a + b, a - b)$ es 1 o 2.

65. Sean $a, b \in \mathbb{Z}$ tales que $\mathrm{mcd}(a, b) = 1$. Demuestre que para cada $n \in \mathbb{N}$, $\mathrm{mcd}(a, b^n) = 1$. Indicación: utilice la inducción matemática sobre n.

Números primos, el teorema fundamental de la aritmética

66. ¿Cuándo un número se llama *primo*? Escribir la definición.

67. Lema sobre el menor divisor entero mayor que 1 de un número entero mayor que 1. Sea $a \in \mathbb{Z}$, $a > 1$. Entonces el menor elemento del conjunto

$$\{d \in \mathbb{Z}: \quad d > 1 \quad \wedge \quad d \mid a\}$$

es un número primo.

68. Teorema de Eratóstenes. Sea $a \in \mathbb{N}$, $a > 1$. Supongamos que para cada p primo tal que $p^2 \leq a$ se tiene que $p \nmid a$. Demuestre que a es primo.

69. Utilizando el algoritmo llamado la *criba de Eratóstenes* encuentre todos los números primos menores que 100.

70. Demuestre que el conjunto de números primos no es finito.

71. Sea $a \in \mathbb{Z}$ y sea p un primo. Demuestre que $p \mid a$ o $\mathrm{mcd}(p, a) = 1$.

72. Sean $a, b \in \mathbb{Z}$ y sea p un primo. Supongamos que $p \mid (ab)$. Demuestre que $p \mid a$ o $p \mid b$.

73. Sean $a_1, \ldots, a_n \in \mathbb{Z}$ y sea p un primo. Supongamos que $p \mid (a_1 \cdots a_n)$. Demuestre que existe un $k \in \{1, \ldots, n\}$ tal que $p \mid a_k$.

74. Sean p_1, p_2 primos, $p_1 \neq p_2$. Demuestre que $\mathrm{mcd}(p_1, p_2) = 1$.

75. Sean d, p_1, p_2 algunos números primos tales que $d \mid (p_1 p_2)$. Demuestre que $d = p_1$ o $d = p_2$.

76. Sean $d, p_1, \ldots, p_n$ algunos números primos tales que $d \mid (p_1 \cdots p_n)$. Demuestre que existe un $k \in \{1, \ldots, n\}$ tal que $d = p_k$.

77. Teorema fundamental de aritmética, la parte de existencia. Sea $a \in \mathbb{Z}$, $a > 1$. Demuestre que existen números primos $p_1, p_2, \ldots, p_k$ tales que

$$a = p_1 p_2 \cdots p_k.$$

78. Teorema fundamental de aritmética, la parte de unicidad. Sean $p_1, \ldots, p_m$ y $q_1, \ldots, q_n$ algunos números primos tales que

$$p_1 \leq \ldots \leq p_m, \qquad q_1 \leq \ldots \leq q_n, \qquad p_1 \cdots p_m = q_1 \cdots q_n.$$

Demuestre que $m = n$, $p_1 = q_1, \ldots, p_n = q_n$.

79. Pequeño teorema de Fermat. Sean a un número entero y p un número primo. Demuestre que

$$p \mid (a^p - a).$$

Sugerencia: usar la inducción matemática (sobre a) y expandir $(a+1)^p$ por la fórmula de la potencia del binomio.