Demostraciones que utilizan la identidad de Bézout

(ejercicios)

1. Definición de la divisibilidad (repaso).
Sean $m, n \in \mathbb{Z}$. Decimos que m *divide a* n y escribimos $\underbrace{\qquad}_{?}$,

si existe un número $s \in \underbrace{\qquad}_{?}$ tal que $\underbrace{\qquad}_{?}$.

2. Conjunto de los divisores enteros de un número entero dado (repaso).
Dado un número entero m, denotamos por $\mathcal{D}(m)$ al conjunto de sus divisores enteros:

$$\mathcal{D}(r) := \{s \in \mathbb{Z}: \quad \underbrace{\qquad}_{?}\}.$$

3. Un teorema sobre propiedades de la divisibilidad (repaso).
Sean $a, b, u, v, d \in \mathbb{Z}$ tales que $d \mid a$ y $d \mid b$. Entonces $d \mid au + bv$.

Demostración. Las condiciones $d \mid a$ y $d \mid b$ significan que existen $j, k \in \mathbb{Z}$ tales que

$$a = \underbrace{\qquad}_{?}, \qquad b = \underbrace{\qquad}_{?}.$$

De estas igualdades obtenemos $au + bv = \underbrace{\qquad}_{?} + \underbrace{\qquad}_{?} = d\,\big(\,\underbrace{\qquad\qquad}_{?}\,\big)$.

Como $\underbrace{\qquad\qquad}_{?} \in \mathbb{Z}$, hemos demostrado que $au+bv$ es un múltiplo entero de $\underbrace{\qquad}_{?}$. $\square$

4. Divisibilidad y comparación de valores absolutos (repaso).
Sea $m \in \mathbb{Z}$ tal que $m \mid (-83)$. Entonces $|m| \leqslant \underbrace{\qquad}_{?}$, esto es, $\underbrace{\qquad}_{?} \leqslant m \leqslant \underbrace{\qquad}_{?}$.

5. La intersección y la unión de dos conjuntos (ejemplo).
Sean $A = \{-8, 2, 5\}$, $B = \{2, 4, 5, 9\}$. Entonces

$$A \cap B = \underbrace{\qquad\qquad}_{?}, \qquad\qquad A \cup B = \{-8, 2, 4, 5, 9\}.$$

6. Divisores comunes de dos números enteros (repaso). Sean $a, b \in \mathbb{Z}$. Entonces el conjunto de los divisores comunes de a y b se puede expresar a través de $\mathcal{D}(a)$ y $\mathcal{D}(b)$ de la siguiente manera:

$$\big\{s \in \mathbb{Z}\colon \quad s \mid a \quad \wedge \quad s \mid b\big\} = \mathcal{D}(a) \underbrace{\qquad}_{?} \mathcal{D}(b).$$

7. Definición del máximo común divisor de dos números enteros no ambos cero (repaso). Sean $a, b \in \mathbb{Z}$ tales que $a \neq 0$ o $b \neq 0$. Entonces $\mathrm{mcd}(a, b)$ se define como el elemento máximo del conjunto $\underbrace{\qquad\qquad\qquad\qquad}_{?}$.

8. Ejemplo de demostración con la identidad de Bézout. Supongamos que a, b son números enteros y

$$26 \mid a, \qquad 26 \mid b, \qquad 7a - 20b = 26.$$

Demostrar que $\mathrm{mcd}(a, b) = 26$.

Demostración. Primera parte. Las condiciones $26 \mid a$ y $26 \mid b$ significan que 26 es un divisor común de a y b. En otras palabras, 26 es un elemento del conjunto

$$\underbrace{\qquad}_{?} \ \underbrace{\qquad}_{\text{¿}\cap/\cup\text{?}} \ \underbrace{\qquad}_{?}. \tag{1}$$

Todavía nos falta demostrar que 26 es el *máximo elemento* del conjunto (1).

Segunda parte. Supongamos que d es algún elemento de este conjunto:

$$d \in \underbrace{\qquad\qquad\qquad\qquad}_{?}.$$

Entonces $d \mid a$ y $d \mid b$. Por lo tanto, $d \mid (7a - 20b)$.
Pero estamos suponiendo que $7a - 20b = \underbrace{\qquad}_{?}$. Por lo tanto, $d \mid \underbrace{\qquad}_{?}$.

Esto implica que $|d| \leqslant \underbrace{\qquad}_{?}$, esto es, $\underbrace{\qquad}_{?} \leqslant d \leqslant \underbrace{\qquad}_{?}$.

En particular, la desiguldad derecha dice que $d \leqslant \underbrace{\qquad}_{?}$.

Resumen: 26 es *un* elemento del conjunto $\underbrace{\qquad\qquad\qquad\qquad}_{?}$,

y cualquier elemento d de este conjunto es $\leqslant 26$.

Por lo tanto, d es el $\underbrace{\qquad\qquad\qquad\qquad}_{?}$ común divisor de a y b. □

9. Ejercicio. Supongamos que m, n son números enteros y

$$38 \mid m, \qquad 38 \mid n, \qquad 23m - 10n = 38.$$

Demuestre que $\mathrm{mcd}(m, n) = 38$.

Demostración. Primera parte. Las condiciones $\underbrace{\qquad}_{?}$ y $\underbrace{\qquad}_{?}$ dicen que

38 es un divisor $\underbrace{\qquad}_{?}$ de los números $\underbrace{\qquad}_{?}$ y $\underbrace{\qquad}_{?}$.

En otras palabras, 38 es elemento del conjunto

$$\underbrace{\qquad\qquad\qquad}_{?}.$$

Falta demostrar que 38 es el $\underbrace{\qquad\qquad}_{?}$ elemento de este conjunto.

Segunda parte. Supongamos que d es algún elemento del conjunto $\underbrace{\qquad\qquad\qquad}_{?}$,

y demostremos que $d \leqslant 38$.
Notamos que d divide a cada uno de los números $\underbrace{\qquad}_{?}$ y $\underbrace{\qquad}_{?}$.
Por lo tanto, d divide a su combinación lineal entera $23m - 10n$.
Pero el último número es $\underbrace{\qquad}_{?}$, así que $d \mid \underbrace{\qquad}_{?}$.
Esto implica que $|d| \leqslant \underbrace{\qquad}_{?}$, esto es, $\underbrace{\qquad}_{?} \leqslant d \leqslant \underbrace{\qquad}_{?}$. En particular, $d \leqslant 38$.

Resumen de dos partes: 38 es un elemento del conjunto $\underbrace{\qquad\qquad\qquad}_{?}$,

y cualquier elemento de este conjunto es $\leqslant 38$.
Por lo tanto, ...

□

10. Teorema. Sean a, b, u, v, d algunos números enteros tales que $d > 0$,

$$d \mid a, \qquad d \mid b, \qquad au + bv = d.$$

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

Se recomienda escribir la demostración del teorema en una hoja de papel razonando de la misma manera como en el ejemplo y ejercicio anteriores.

11. Otro ejemplo de demostración que utiliza coeficientes de Bézout.
Sea m un número entero tal que $4 \mid 9m$. Demostrar que $4 \mid m$.

Demostración. La condición $4 \mid 9m$ significa que existe un número $k \in \mathbb{Z}$ tal que

$$9m = \underbrace{\qquad}_{?}. \tag{2}$$

Por otro lado, notamos que 9 y 4 son números primos relativos, esto es, $\mathrm{mcd}(9, 4) = \underbrace{\qquad}_{?}$.

Se encuentran fácilmente dos números u y v tales que

$$4u + 9v = 1. \tag{3}$$

Por ejemplo, $u = -2$, $v = 1$. Multiplicamos la igualdad (3) por m:

$$4um + 9vm = m.$$

Ahora sustituimos $9m$ por la fórmula (2):

$$4um + \underbrace{\qquad\qquad}_{?} = m.$$

Factorizamos 4:

$$4 \left(\underbrace{\qquad\qquad}_{?} \right) = m.$$

Como el número entre los paréntesis es entero, hemos demostrado que $\underbrace{\qquad\qquad}_{?}$. □

De manera similar se resuelve el siguiente ejercicio, y luego de manera similar se demuestra el teorema (utilizando la existencia de coeficientes de Bézout). Se recomienda encontrar una hoja de papel y escribir las demostraciones con cuidado.

12. Ejercicio. Sea $q \in \mathbb{Z}$ tal que $(-8) \mid 15q$. Demuestre que $(-8) \mid q$.

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

Inicio de la demostración. Como $\mathrm{mcd}(a, b) = 1$, existen $u, v \in \mathbb{Z}$ tales que

$$au + bv = 1.$$

□