

FECHA DE ENTREGA: JUEVES 3 DE NOVIEMBRE

Nota. Cada inciso se calificará por separado en la escala del 0 al 10.

Definición Sean $a, b \in \mathbb{Z}$. Decimos que a divide a b o que b es divisible por a si existe un elemento $q \in \mathbb{Z}$ tal que $b = aq$, en cuyo caso escribimos, $a|b$.

1. Demostrar que

- (1) Si $0|a$ entonces $a = 0$.
- (2) $1|n$, para todo $n \in \mathbb{Z}$.
- (3) Si $m|n$ y $n|p$ entonces $m|p$.
- (4) Si $m|n$ y $m|p$ entonces $m|rn + sp$, para todos r y s en $\mathbb{Z}$.
- (5) Si $a|b$ y $b|a$ entonces $|a| = |b|$.
- (6) Si $ac|bc$ con $c \neq 0$ entonces $a|b$.
- (7) Si $a_1|b_1, a_2|b_2, \dots, a_n|b_n$, entonces $a_1a_2 \cdots a_n|b_1b_2 \cdots b_n$.

Definición Sean a y b elementos de $\mathbb{Z}$. Suponer que al menos uno de ellos no es cero. Decimos que $k \in \mathbb{N}$ es un *máximo común divisor* de a y b si se cumple que:

$$k|a \text{ y } k|b, \text{ y} \\ \text{si } d|a \text{ y } d|b, \text{ entonces } d|k.$$

En tal caso, escribimos $k = (a, b)$.

2. Demostrar que dados a y b en $\mathbb{Z}$,

- (1) (a, b) existe.
- (2) (a, b) es único.
- (3) Existen enteros m y n tales que $(a, b) = ma + nb$. (Sugerencia: emplear el Principio del Buen Orden).
- (4) $(a, b) = (|a|, |b|) = (a, b + am)$, para cualquier $m \in \mathbb{Z}$.
- (5) $(ma, mb) = |m|(a, b)$ para cualquier $m \in \mathbb{Z} - \{0\}$.

Definición Decimos que los enteros a y b son *primos relativos*, si $(a, b) = 1$.

3. Demostrar que:

- (1) **Teroema.** Si a y b son primos relativos y $a|bc$, entonces $a|c$.
- (2) **Corolario.** Si a y b son primos relativos y Si a y c son primos relativos, entonces a y bc son primos relativos.
- (3) Si $p \in \mathbb{N}$ es un número primo y $a|p$, entonces $a = \pm p$ o $a = \pm 1$.
- (4) Si $p \in \mathbb{N}$ es un número primo y $p|a_1a_2 \cdots a_n$, entonces $p|a_i$ para algún a_i .
- (5) Si $a \in \mathbb{N}$ y $a > 1$, entonces a es primo, o a es un producto de números primos. (Sugerencia: usar el Principio del buen Orden).
- (6) Si $a \in \mathbb{N}$ y $a > 1$, entonces existe una única manera de escribir $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ con $e_i \geq 1$ y $1 < p_1 < p_2 < \cdots < p_r$. (Sugerencia: usar el Principio del buen Orden).

5-6. Considerar el anillo $\mathbb{Z}/(p)$ (con $p > 0$) cuyos elementos son los subconjuntos de $\mathbb{Z}$ de la forma $|k| = \{k + qp \mid q \in \mathbb{Z}\}$. Equipar a $\mathbb{Z}/(p)$ con las operaciones de suma y producto que hacen de la función $\mathbb{Z} \ni k \mapsto |k| \in \mathbb{Z}/(p)$ un morfismo de anillos.

Demostrar que $\mathbb{Z}/(p)$ es un campo si y sólo si p es un primo.

(Pregunta 5: si p es primo, entonces $\mathbb{Z}/(p)$ es campo)

(Pregunta 6: $\mathbb{Z}/(p)$ es campo, entonces p es primo).

Definición Decimos que k es un *mínimo común múltiplo* de a y b si se cumple que:

$$a|k \text{ y } b|k, \text{ y} \\ \text{si } a|c \text{ y } b|c, \text{ entonces } k|c.$$

En tal caso, escribimos $k = |a, b|$

7. Demostrar que:

- (1) $|a, b|$ existe.
- (2) $|a, b|$ es único.
- (3) Si $a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ con $e_i \geq 1$ y $1 < p_1 < p_2 < \cdots < p_r$ y $b = q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$ con $f_i \geq 1$ y $1 < q_1 < q_2 < \cdots < q_r$, son las descomposiciones en números primos de a y b , se puede proporcionar una expresión para $|a, b|$ en términos de estos datos.

8. Sea $\mathbb{F}$ un campo y sean f y g dos elementos del anillo de polinomios $\mathbb{F}[x]$. Demostrar que existen polinomios r y q tales que $f = gq + r$ tales que $r = 0$, o bien el grado de r es estrictamente menor que el grado de g .

9. Sea $I \subset \mathbb{F}[x]$ un ideal. Demostrar que existe un elemento $c \in I$ tal que $f \in I$ si y sólo si existe un $q \in \mathbb{F}[x]$ tal que $f = qc$. (Sugerencia: en el fondo se trata de aplicar el Principio del Buen Orden).

10. Si $f \in \mathbb{F}[x]$ y lo escribimos como $f = a_n x^n + \cdots a_1 x + a_0$, con $a_i \in \mathbb{F}$, definimos, para cada $b \in \mathbb{F}$ una función $\varepsilon_b : \mathbb{F}[x] \rightarrow \mathbb{F}$ mediante,

$$\varepsilon_b(f) = a_n b^n + \cdots a_1 b + a_0$$

(esto es, *evaluar* el polinomio en b). Sea X el polinomio que tiene $a_0 = a_2 = a_3 = \cdots = 0$ y $a_1 = 1$; esto es, $X = x$. Demostrar que

$$\varepsilon_b(f) \iff X - b|f.$$

11. **Bonus problem.** Considerar la siguiente relación S en $\mathbb{R}[x]$:

$$S = \{(p, q) \mid \exists r \in \mathbb{R}[x] \text{ tal que } p - q = (X^2 + 1)r\} \subset \mathbb{R}[x] \times \mathbb{R}[x]$$

Demostrar que:

- (1) S es de equivalencia.
- (2) $\mathbb{F}[x]/S$ es un campo isomorfo a $\mathbb{C}$

¿Qué quiere decir que sea un ‘bonus problem’? Que entender lo que el problema plantea, que saber escribir lo que se tendría que demostrar y justificar cada paso de la demostración, puede significar que se tienen amplias garantías de aprobar el curso de matemáticas elementales con calificación > 8.5 . ¡Inténtenlo!