Demostraciones con números primos (ejercicios)

Objetivos. Acostumbrarse a la definición de número primo, aprender a usarla en demostraciones simples.

Requisitos. Propiedades de divisibilidad, máximo común divisor y sus propiedades, números primos relativos.

Denotamos por $\mathbb{N}$ el conjunto de números enteros positivos.

1. Definición (número primo). Un *número primo* es un número entero mayor que 1 que no tiene divisores enteros positivos excepto 1 y si mismo.

2. Otra forma de definición. Un número p se llama *primo* si $p \in \mathbb{Z}$, $p > 1$, y

$$\mathcal{D}(p) = \{-p, -1, 1, p\}.$$

3. Conjunto de los números primos. Denotamos por $\mathbb{P}$ el conjunto de números primos.

$$\mathbb{P} := \big\{p \in \mathbb{Z}\colon \quad p > 1 \quad \wedge \quad \mathcal{D}(p) = \{-p, -1, 1, p\}\big\}.$$

4. Ejercicio. Para cada uno de los números enteros n de 2 a 10 halle el conjunto de sus divisores enteros y determine si n es primo o no.

$\mathcal{D}(2) = \{\pm 1, \pm 2\}$ $\qquad$ $\mathcal{D}(11) =$

$\mathcal{D}(3) =$ $\qquad$ $\mathcal{D}(12) =$

$\mathcal{D}(4) = \{\pm 1, \pm 2, \pm 4\}$ $\qquad$ $\mathcal{D}(13) =$

$\mathcal{D}(5) =$ $\qquad$ $\mathcal{D}(14) =$

$\mathcal{D}(6) =$ $\qquad$ $\mathcal{D}(15) =$

$\mathcal{D}(7) =$ $\qquad$ $\mathcal{D}(16) =$

$\mathcal{D}(8) =$ $\qquad$ $\mathcal{D}(17) =$

$\mathcal{D}(9) =$ $\qquad$ $\mathcal{D}(18) =$

$\mathcal{D}(10) =$ $\qquad$ $\mathcal{D}(19) =$

Usando la información de arriba escriba todos los números primos menores que 20:

2,

5. Ejercicio. Sea $d \in \mathbb{Z}$ tal que $d \mid 7$ y $d > 1$. Encuentre d.

6. Si sabemos que un número dado es primo, ¿cómo utilizar esta información? Supongamos que $p \in \mathbb{P}$, $d \in \mathbb{Z}$, $d \mid p$ y $d > 1$. Entonces la definición de número primo implica que

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

7. Ejemplo. Sea $a \in \mathbb{Z}$. Demostrar que $\mathrm{mcd}(19, a) = 1$ o $19 \mid a$.

Demostración. Consideremos dos casos que abarcan todas las posibilidades posibles:

$$\text{I. } \mathrm{mcd}(19, a) = 1. \qquad \text{II. } \mathrm{mcd}(19, a) > 1.$$

En el caso I la conclusión ya está demostrada. Consideremos el caso II, cuando

$$\mathrm{mcd}(19, a) \underbrace{\qquad}_{?} 1.$$

En este caso nuestro objetivo es demostrar que $19 \mid a$.

Denotemos $\mathrm{mcd}(19, a)$ por d. Estamos en el caso II, cuando $d > 1$.
De la definición de mcd se sigue que d es un divisor de 19:

$$d \in \mathcal{D}(\underbrace{\qquad}_{?}).$$

Pero $d > 1$ y el número 19 es primo. Por lo tanto,

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

Ahora recordamos que d tambiés es un divisor de $\underbrace{\qquad}_{?}$ y concluimos que $19 \mid a$. □

8. Ejercicio. Sea $b \in \mathbb{Z}$. Demuestre que $\mathrm{mcd}(17, b) = 1$ o $17 \mid b$.

Se recomienda escribir la demostración en una hoja de papel, utilizando el Ejemplo 7.

9. Ejercicio. Sea $c \in \mathbb{Z}$. Demuestre que $\mathrm{mcd}(5, c) = 1$ o $5 \mid c$.

Se recomienda escribir la demostración en una hoja de papel, sin utilizar ejemplos anteriores.

10. Definición (número primo). Un *número primo* es un número entero mayor que $\underbrace{\qquad}_{?}$ que no tiene divisores enteros positivos excepto $\underbrace{\qquad}_{?}$ y $\underbrace{\qquad\qquad\qquad}_{?}$.

11. Otra forma de definición. Un número p se llama *primo* si $p \in \mathbb{Z}$, $p > \underbrace{\qquad}_{?}$, y

$$\mathcal{D}(p) = \underbrace{\qquad\qquad\qquad}_{?}.$$

12. Conjunto de los números primos. Denotamos por $\mathbb{P}$ el conjunto de números primos:

$$\mathbb{P} := \big\{p \in \mathbb{Z}\colon \quad p > \underbrace{\qquad}_{?} \quad \wedge \quad \mathcal{D}(p) = \underbrace{\qquad\qquad\qquad}_{?}\big\}.$$

13. Ejercicio. Sea $d \in \mathbb{Z}$ tal que $d \mid 17$ y $d > 1$. Encuentre d.

14. Si sabemos que un número dado es primo, ¿cómo utilizar esta información?
Supongamos que $p \in \mathbb{P}$, $d \in \mathbb{Z}$, $d \mid p$ y $d > 1$. Entonces la definición de número primo implica que

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

15. ¿Cómo demostrar que un número es primo?
Supongamos que $n \in \mathbb{Z}$. Queremos demostrar que n es primo.
Primero, tenemos que verificar que $n > \underbrace{\qquad}_{?}$.
Segundo, tenemos que mostrar que cualquier divisor entero positivo de n es

$$\underbrace{\qquad}_{?} \quad \text{o} \quad \underbrace{\qquad}_{?}.$$

Reformulamos esta propiedad en una forma más cómoda:
si d es un divisor entero de n y $d > 1$, entonces $d = \underbrace{\qquad}_{?}$.
Si logramos demostrar estas dos propiedades, entonces $n \in \mathbb{P}$.

16. Una forma cómoda de la definición de número primo. Los razonamientos anteriores se pueden escribir de manera breve:

$$p \in \mathbb{P} \qquad p > \underbrace{\qquad}_{?} \quad \wedge \quad \big(\forall d \in \mathbb{Z} \quad (d > 1) \ \wedge \ (d \mid p) \implies d = \underbrace{\qquad}_{?}\big).$$

17. Observación sobre el menor divisor entero mayor que 1 de un número entero mayor que 1. El conjunto de los divisores enteros mayores que 1 del número 45 es

$$\{d \in \mathbb{Z}\colon \quad d > 1 \quad \wedge \quad d \mid 45\} = \{3, \underbrace{\qquad}_{?}, \underbrace{\qquad}_{?}\}.$$

El menor elemento de este conjunto es $\underbrace{\qquad}_{?}$. Notamos que este número es primo.

18. Lema sobre el menor divisor entero mayor que 1 de un número entero mayor que 1. Sea $a \in \mathbb{Z}$, $a > 1$. Denotemos por S al conjunto de los divisores de a que son mayores que 1:

$$S = \{d \in \mathbb{Z}\colon \quad d > 1 \quad \wedge \quad d \mid a\},$$

y denotemos por m al menor elemento del conjunto S. Entonces $m \in \mathbb{P}$.

Demostración. Notamos que el mismo número a pertenece al conjunto $\underbrace{\qquad}_{?}$ porque

$$a > \underbrace{\qquad}_{?}, \qquad\qquad a \mid a.$$

Por eso el conjunto $\underbrace{\qquad}_{?}$ no es vacío, y la definición de m tiene sentido.

Siendo un elemento del conjunto $\underbrace{\qquad}_{?}$, el número m tiene propiedades

$$m > \underbrace{\qquad}_{?}, \qquad\qquad m \mid \underbrace{\qquad}_{?}.$$

Tenemos que demostrar que $m \in \mathbb{P}$, esto es, que los únicos divisores enteros positivos de m son $\underbrace{\qquad}_{?}$ y $\underbrace{\qquad}_{?}$. Equivalentemente, tenemos que demostrar que si b es un divisor entero positivo de m y $b > 1$, entonces $b = \underbrace{\qquad}_{?}$.

Sea b un divisor entero positivo de m tal que $b > 1$. De las propiedades $b \mid m$ y $m \mid a$ concluimos que $b \mid \underbrace{\qquad}_{?}$. Por lo tanto, $b \in \underbrace{\qquad}_{?}$.

Pero m es el elemento mínimo del conjunto $\underbrace{\qquad}_{?}$, así que $m \leqslant b$.

Por otro lado, b es un divisor de m, por eso $b \leqslant m$.

De las dos últimas desigualdades concluimos que $b = \underbrace{\qquad}_{?}$.

Hemos demostrado que m es un número $\underbrace{\qquad\qquad}_{?}$. □

19. Teorema de Eratóstenes. Sea $a \in \mathbb{N}$, $a > 1$. Supongamos que para cada $p \in \mathbb{P}$ tal que $p^2 \leqslant a$ se tiene que $p \nmid a$. Entonces $a \in \mathbb{P}$.

Demostración. Denotemos por m al mínimo entre los divisores enteros de a mayores que 1, esto es, al mínimo elemento del conjunto

$$S = \{d \in \mathbb{Z}\colon \quad d > \underbrace{\qquad}_{?} \quad \wedge \quad d \mid \underbrace{\qquad}_{?}\}.$$

Por el Lema sobre el menor divisor entero mayor que 1 de un número entero mayor que 1, m es un número primo.

Consideremos dos casos: I $m < a$; II $m = a$.

I. Supongamos que $m < a$. Como $m \mid a$, existe un $n \in \mathbb{Z}$ tal que $a = \underbrace{\qquad}_{?}$.

Como $m < a$, concluimos que $n > 1$. Entonces n es un elemento del conjunto $\underbrace{\qquad}_{?}$.

Pero m es el mínimo elemento de este conjunto, así que $m \leqslant \underbrace{\qquad}_{?}$. Por eso

$$m^2 \leqslant m \cdot \underbrace{\qquad}_{?} = \underbrace{\qquad}_{?}.$$

Por la hipótesis del teorema $m \nmid \underbrace{\qquad}_{?}$, lo que contradice a la construcción de m.

La constradicción muestra que el caso $m \underbrace{\qquad}_{?} a$ es imposible.

II. Entonces el único caso posible es $m = \underbrace{\qquad}_{?}$.

Concluimos que a es primo porque $\underbrace{\qquad}_{?}$ lo es. □

Teorema sobre la infinidad de números primos

20. Construcción principal. Dado un conjunto finito de números primos $p_1, \ldots, p_n$ y considerando el número

$$a = p_1 \cdots p_n + 1,$$

entre sus divisores enteros mayores que 1 siempre encontramos un primo diferente de $p_1, \ldots, p_n$.

21. Ejemplo. Sea $a = 2 \cdot 3 \cdot 5 + 1 = \underbrace{\qquad}_{?}$, entonces $\mathcal{D}(a) =$,

y el número a es $\underbrace{\qquad\qquad}_{?}$.

22. Otro ejemplo. Sea $a = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = \underbrace{\qquad\qquad}_{?}$, entonces

$$\mathcal{D}(a) = \{\pm 1, \pm 59, \underbrace{\qquad}_{?}, \underbrace{\qquad\qquad}_{?}\},$$

y el mínimo divisor de a mayor a uno es $m = \underbrace{\qquad}_{?}$.

Notamos que m es un número primo y es diferente de $2, 3, 5, 7, 11, 13$.

23. Teorema sobre la infinidad de números primos. El conjunto $\mathbb{P}$ no es finito.

Demostración. Razonando por contradicción supongamos que $\mathbb{P}$ es finito. Denotemos sus elementos por

$$p_1, \ldots, p_n.$$

Consideremos el número

$$a = p_1 \cdots p_n + 1.$$

Sea m el elemento mínimo del conjunto de los divisores enteros de a mayores a 1:

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

Usando el Lema sobre el menor divisor entero mayor que 1 de un número entero mayor que 1, concluimos que m es un número $\underbrace{\qquad\qquad}_{?}$. Entonces m debe ser uno de los números $\underbrace{\qquad\qquad}_{?}$ y $m \mid p_1 \cdots p_n$. Por otro lado, $m \mid a$. Por consecuencia,

$$m \mid (a - p_1 \cdots p_n).$$

Pero de la definición de a se sigue que $a - p_1 \cdots p_n = \underbrace{\qquad}_{?}$.

Entonces $m \mid \underbrace{\qquad}_{?}$ y por lo tanto $m \leqslant \underbrace{\qquad}_{?}$,

lo que constradice a la construcción de m. □