Álgebra Superior II
Tarea 02: Divisibilidad

Mora Espinosa Miroslava
Rendón Ávila Jesús Mateo
Rubio Pérez Ángel Damián
Valencia Morales Indra Gabriel

April 4, 2025

Facultad de Ciencias
Universidad Nacional Autónoma de México

Profesor: Dr. Gerardo Miguel Tecpa Galván

•**1.** Sean a un número par y b un número impar. Muestra que $mcd(a, b)$ es impar.

Respuesta

Procedemos por contradicción. Supongamos que $mcd(a, b)$ es par.

Por definición de mcd, entonces $mcd(a, b) \mid a$ y $mcd(a, b) \mid b$.

Por ser $mcd(a, b)$ par, entonces $mcd(a, b) \nmid b$ **!**

De lo anterior debe ser $mcd(a, b)$ es impar.$\blacksquare$

• **2.** Un grupo de 23 viajeros llega a un campamento y encuentra 63 montones de sacos, cada montón con el mismo número de sacos, y un montón adicional con 7 sacos (en total hay 64 montones). Si sabemos que los viajeros no podían cargar con más de 50 sacos cada uno y pudieron repartírselos por igual y sin abrirlos, ¿cuántos sacos había en cada uno de los montones?

Respuesta

Como un viajero puede llevar a lo mas 50 sacos y hay x sacos en 63 montones y 7 sacos sueltos, podemos obtener lo siguiente:

$$23 \mid 63x + 7$$

$$i.e\ 63x \equiv -7\ mod\ 23$$

Propongamos $x = 5$ tendriamos entonces:

$$23 \mid 63 \cdot 5 + 7$$

$$23 \mid 315 + 7$$

$$23 \mid 322$$

Por definición de divisibilidad $Existe * \in \mathbb{N}$ tal que $23 \cdot * = 322$.

Si $* = 14$, entonces $23 \cdot 14 = 322$

Así, concluimos que habia 5 sacos por monton $\blacksquare$

• **3.** Demuestra que si a y b son enteros no nulos, entonces $mcd(a, b)|mcm(a, b)$.

Respuesta

Sean a y b enteros no nulos
Sabemos que por definicion de mínimo comun múltiplo
$a \mid mcm(a, b)$ y $b \mid mcm(a, b)$
De igual manera, sabemos que por definición de maximo común divisor
$mcd(a, b) \mid a$ y $mcd(a, b) \mid b$

Por transitividad de la divisibilidad.

Como $mcd(a,b) \mid a$ y $a \mid mcm(a,b)$, entonces $mcd(a,b) \mid mcm(a,b)$
Como $mcd(a,b) \mid b$ y $b \mid mcm(a,b)$, entonces $mcd(a,b) \mid mcm(a,b)$

$\therefore mcd(a,b)|mcm(a,b)$. ∎

• **4.** Muestra que si p y q son dos primos distintos, entonces para todo $a, b \in \mathbb{Z}^+$ se cumple que $mcd(p^a, q^b) = 1$.

Respuesta

Sabemos que p y q son primos y ademas $p \neq q$

Sean entonces $a, b \in \mathbb{Z}^+$ tal que $mcd(p^a, q^b) \neq 1$ y $mcd(p^a, q^b) = r$

Por definición de mcd, entonces:

$$r \mid p^a \ y \ r \mid q^b$$

De $r \mid p^a$ podemos concluir que $r \mid p$

De $r \mid q^b$ podemos concluir que $r \mid q$

Pero sabemos que $p \neq q$, por lo que debe ser $mcd(p^a, q^b) = 1$ **!**

Por lo tanto debe ser $mcd(p^a, q^b) = 1$ ∎

• **5.** Sean $a_1, \ldots, a_n \in \mathbb{Z}$ una colección de enteros Muestra que si para todo $i, j \in \{1, ..., k\}$ con $i \neq j$ se satisface que $mcd(a_i, a_j) = 1$, entonces $mcd(a_k, a_1 \cdot a_2 \cdots a_{k-1}) = 1$.

Respuesta

Procedemos por inducción.

Sea p primo, por ser primo $p \geq 2$ y supongamos que $p \mid mcd(a_k, a_1 \cdot a_2 \cdots a_{k-1})$. y sea a_l con $l \in \{1, \ldots, k-1\}$

Por definición enotnces $mcd(a_k, a_1 \cdot a_2 \cdots a_{k-1}) \mid a_k$ y $mcd(a_k, a_1 \cdot a_2 \cdots a_{k-1}) \mid a_l$.

Así $p \mid a_k$ y $p \mid a_l$. Por definición de mcd, entonces $p \leq mcd(a_k, a_l)$.

Por hipótesis sabemos que $mcd(a_k, a_l) = 1$ **!**

Como no puede ser $p > 1$ y $p \leq 1$, entonces debe ser $mcd(a_k, a_1 \cdot a_2 \cdots a_{k-1}) = 1$ ∎

• **6.** Sean $a_1, \ldots, a_n, b \in \mathbb{Z}$ una colección de enteros tales que para todo $i, j \in \{1, \ldots, k\}$ con $i \neq j$ se satisface que $mcd(a_i, a_j) = 1$. Muestra por inducción que si para todo $i \in \{1, \ldots, k\}$ se cumple que $a_i|b$, entonces $a_1 \cdot a_2 \cdots a_k|b$.

Respuesta

Mostraremos mediante inducción matematica que si para todo $i \in \{1, \ldots, k\}$ se cumple que $a_i \mid b$, entonces $a_1 \cdot a_2 \cdots a_k \mid b$.

Base de inducción: Mostraremos para k=2 que si para todo $i \in \{1, 2\}$ se cumple que $a_i \mid b$, entonces $a_1 \cdot a_2 \mid b$.

Sean $a_1, a_2, b \in \mathbb{Z}$ una colección de enteros tales que para todo $i, j \in \{1, 2\}$ con $i \neq j$ se satisface que $mcd(a_i, a_j) = 1$.

Como $i, j \in \{1, 2\}$, entonces se cumple que $a_i \mid b$ y $a_j \mid b$.

Tomemos $i = 1$ y como $i \neq j$ sea $j = 2$.

Como $a_1 \mid b$, $a_2 \mid b$ y por hipótesis $mcd(a_i, a_j) = mcd(a_1, a_2) = 1$, por lema:

$\therefore a_1 \cdot a_2 \mid b$

$\therefore$ Se cumple el enunciado para la base inductiva. $\blacksquare$

Hipotesis de inducción: Supongamos para k= n que si para todo $i \in \{1, \ldots, n\}$ se cumple que $a_i \mid b$, entonces $a_1 \cdot a_2 \cdots a_n \mid b$

Paso de inducción: Mostraremos para k=n+1 que si para todo $i \in \{1, \ldots, n + 1\}$ se cumple que $a_i \mid b$, entonces $a_1 \cdot a_2 \cdots a_n \cdot a_{n+1} \mid b$

Sean $a_1, \ldots, a_n, a_{n+1}, b \in \mathbb{Z}$ una colección de enteros tales que para todo $i, j \in \{1, ..., n, n + 1\}$ con $i \neq j$ se satisface que $mcd(a_i, a_j) = 1$, por el ejercicio **5** tenemos que $mcd(a_{n+1}, a_1 \cdot a_2 \cdots a_n) = 1$

Veamos que $mcd(a_1 \cdot a_2 \cdots a_n, a_{n+1}) = mcd(a_{n+1}, a_1 \cdot a_2 \cdots a_n)$ por lema, entonces $mcd(a_1 \cdot a_2 \cdots a_n, a_{n+1}) = 1$

Además, como $i, j \in \{1, ..., n, n + 1\}$, entonces $a_i \mid b$ y $a_j \mid b$.

Notemos que $i \in \{1, .., n\}$ y además se cumple que $a_i \mid b$, entonces por hipótesis de inducción $a_1 \cdot a_2 \cdots a_n \mid b$

Como $j \in \{1, ..., n, n + 1\}$, $a_j \mid b$ e $i \neq j$, en particular $a_{n+1} \mid b$.

Como $mcd(a_1 \cdot a_2 \cdots a_n, a_{n+1}) = 1$, $a_1 \cdot a_2 \cdots a_n \mid b$ y $a_{n+1} \mid b$, por lema:

$\therefore a_1 \cdot a_2 \cdot a_n \cdot a_{n+1} \mid b$

$\therefore$ Se cumple el enunciado para el Paso inductivo.

$\therefore$ **Si para todo** $i \in \{1, \ldots, k\}$ **se cumple que** $a_i|b$**, entonces** $a_1 \cdot a_2 \cdots a_k|b$**.** $\blacksquare$

- **7.** Sea p un número primo. Muestra que si $k \in \mathbb{Z}$ es tal que $k < p$, entonces $p \nmid k!$

Respuesta

Supongamos por contradicción que $p \mid k!$, es decir

$$p \mid \prod_{i=1}^{k} i$$

entonces, existe $m \in \{1, ..., k\}$ tal que $p \mid m$
Pero, como $k < p$ y $m < k$, entonces $m < p$, pero eso implica que $p \nmid m$
ya que no existe $w \in \mathbb{Z}$ tal que $wp = m$
$\therefore p \nmid m$ **!**
$\therefore p \nmid k!$ ■

- **8.** Sean $c \neq 0$ y $k \geq 2$. Muestra mediante inducción matemática que si $a_1, \ldots, a_k$ es una colección de enteros no nulos, entonces $mcm(ca_1, ca_2, \ldots, ca_k) = |c| mcm(a_1, a_2, \ldots, a_k)$.

Respuesta

Mostraremos mediante inducción matematica que si $a_1, ..., a_k$ es una colección de enteros no nulos, entonces $mcm(ca_1, ca_2, \ldots, ca_k) = |c| \cdot mcm(a_1, a_2, \ldots, a_k)$.

Caso base: Probaremos para k=2 y $c \neq 0$, que si a_1, a_2 es una colección de enteros no nulos, entonces $mcm(ca_1, ca_2) = |c| \cdot mcm(a_1, a_2)$

Sea a_1, a_2 una colección de enteros no nulos, entonces notemos que

$$\begin{aligned}
mcm(ca_1, ca_2) &= \tfrac{|ca_1 \cdot ca_2|}{mcd(ca_1, ca_2)} && \text{Por teorema} \\
&= \tfrac{|c^2 a_1 \cdot a_2|}{mcd(ca_1, ca_2)} && \text{Por aritmética} \\
&= \tfrac{|c^2||a_1 \cdot a_2|}{|c| \cdot mcd(a_1, a_2)} && \text{Por propiedad de valor absoluto} \\
&= \tfrac{|c| \cdot |c| \cdot |a_1 \cdot a_2|}{|c| \cdot mcd(a_1, a_2)} && \text{Por propiedad de valor absoluto} \\
&= |c| \cdot \tfrac{|a_1 \cdot a_2|}{mcd(a_1, a_2)} && \text{Por hipótesis } c \neq 0 \text{ y por prop de mcd} \\
&= |c| \cdot mcm(a_1, a_2) \blacksquare && \text{Por teorema}
\end{aligned}$$

$\therefore mcm(ca_1, ca_2) = |c| \cdot mcm(a_1, a_2)$, el caso base se cumple.

Hipótesis inductiva: Supondremos para k=n y $c \neq 0$, que si $a_1, ..., a_n$ es una colección de enteros no nulos, entonces $mcm(ca_1, ..., ca_n) = |c| \cdot mcm(a_1, ..., a_n)$

Paso inductivo: Mostraremos para $k = n + 1$ y $c \neq 0$, que si $a_1, ..., a_n, a_{n+1}$ es una colección de enteros no nulos, entonces $mcm(ca_1, ..., ca_n, a_{n+1}) = |c| \cdot mcm(a_1, ..., a_n, a_{n+1})$

Sea $a_1, ..., a_n, a_{n+1}$ una colección de enteros no nulos, en particular,

$a_1, ..., a_n$ es una colección de enteros no nulos, entonces $mcm(ca_1, ..., ca_n) = |c| \cdot mcm(a_1, ..., a_n)$ por hipótesis de inducción.

$$\begin{aligned}
\text{Así } mcm(ca_1, ..., ca_n, ca_{n+1}) &= mcm(mcm(ca_1, ..., ca_n), ca_{n+1}) && \text{Por teorema} \\
&= mcm(|c| \cdot mcm(a_1, ..., a_n), ca_{n+1}) && \text{Por hip. inductiva} \\
&= \frac{|(|c| \cdot mcm(a_1, ..., a_n)) \cdot ca_{n+1}|}{mcd(|c| \cdot mcm(a_1, ..., a_n), ca_{n+1})} && \text{Por teorema} \\
&= \frac{|c \cdot mcm(a_1, ..., a_n) \cdot ca_{n+1}|}{mcd(|c| \cdot mcm(a_1, ..., a_n), ca_{n+1})} && \text{Simplificando}
\end{aligned}$$

Observación
Notemos que para $mcd(|c| \cdot mcm(a_1, ..., a_n), ca_{n+1}$:

- Si $c < 0$ entonces
  $mcd(|c|mcm(a_1, ..., a_n), ca_{n+1}) = mcd((-c) \cdot mcm(a_1, ..., a_n), ca_{n+1})$, pero por propiedad de máximo común divisor, $mcd((-c) \cdot mcm(a_1, ..., a_n), ca_{n+1}) = mcd(c \cdot mcm(a_1, ..., a_n), ca_{n+1})$

  Por hipotesis como $c \neq 0$, entonces
  $mcd(c \cdot mcm(a_1, ..., a_n), ca_{n+1}) = |c| \cdot mcd(mcm(a_1, ..., a_n), a_{n+1})$ por lema.

- Si $c > 0$ entonces
  $mcd(|c|mcm(a_1, ..., a_n), ca_{n+1}) = mcd(c \cdot mcm(a_1, ..., a_n), ca_{n+1})$

  Por hipotesis como $c \neq 0$, entonces
  $mcd(c \cdot mcm(a_1, ..., a_n), ca_{n+1}) = |c| \cdot mcd(mcm(a_1, ..., a_n), a_{n+1})$ por lema.

Con lo anterior, entonces

$$\begin{aligned}
mcm(ca_1, ..., ca_n, ca_{n+1}) &= \frac{|c^2 \cdot mcm(a_1, .., a_n) \cdot a_{n+1}|}{|c| \cdot mcd(mcm(a_1, ..., a_n), a_{n+1})} \\
&= \frac{|c||c| \cdot |mcm(a_1, .., a_n) \cdot a_{n+1}|}{|c| \cdot mcd(mcm(a_1, ..., a_n), a_{n+1})} && \text{Por propiedad de valor absoluto} \\
&= \frac{|(|c| \cdot mcm(a_1, ..., a_n)) \cdot ca_{n+1}|}{mcd(|c| \cdot mcm(a_1, ..., a_n), ca_{n+1})} && \text{Por teorema} \\
&= |c| \cdot \frac{|mcm(a_1, .., a_n) \cdot a_{n+1}|}{|mcd(mcm(a_1, ..., a_n), a_{n+1}),} && \text{Por hipótesis,} c \neq 0 \text{ y por prop de mcd} \\
&= |c| \cdot mcm(mcm(a_1, .., a_n), a_{n+1}) && \text{Por teorema} \\
&= |c| \cdot mcm(a_1, .., a_n, a_{n+1}) \blacksquare && \text{Por propiedad de mínimo común múltiplo}
\end{aligned}$$

$\therefore$ $mcm(ca_1, ..., ca_n, a_{n+1}) = |c| \cdot mcm(a_1, ..., a_n, a_{n+1})$, por lo anterior, se cumple el paso inductivo.

$\therefore$ **Es cierto que si $a_1, \ldots, a_k$ es una colección de enteros no nulos, entonces $mcm(ca_1, ca_2, \ldots, ca_k) = |c|mcm(a_1, a_2, \ldots, a_k)$ para $c \neq 0$ y $k \geq 2$.** $\blacksquare$

- **9.** Sean $a, b \in \mathbb{Z}$ no ambos nulos y $c \neq 0$. Muestra que $mcd(ca, cb) = |c|$ si y sólo si $mcd(a, b) = 1$.

Respuesta

$\Rightarrow\rfloor$ Si $mcd(ca, cb) = |c|, entonces\ mcd(a.b) = 1$

Como $mcd(ca, cb) = |c|$, por propiedad sabemos que
$mcd(ca, cb) = |c| \cdot mcd(a, b)$
Por transitividad,
$|c| = |c| \cdot mcd(a, b)$ y además como $c \neq 0$, entonces
$1 = 1 \cdot mcd(a, b)$
Asi, $mcd(a, b) = 1$
$\therefore$ Si $mcd(ca, cb) = |c|, entonces\ mcd(a.b) = 1$ ■

$\Leftarrow\rfloor$ Si $mcd(a.b) = 1,\ entonces\ mcd(ca, cb) = |c|$

Sabemos que $mcd(a.b) = 1$, como $c \neq 0$, entonces
$|c| = |c| \cdot mcd(a, b)$
Por propiedad,
$|c| \cdot mcd(a, b) = mcd(ca, cb)$
Asi, por transitividad,
$|c| = mcd(ca, cb)$
$\therefore$ Si $mcd(a.b) = 1,\ entonces\ mcd(ca, cb) = |c|$ ■

Por definición de doble contención.
Sean $a, b \in \mathbb{Z}$ no ambos nulos y $c \neq 0$, entonces $mcd(ca, cb) = |c|$ si y sólo si $mcd(a, b) = 1$ ■

- **10.** Muestra que si p es un número primo y $k \in \{1, \ldots, p-1\}$, entonces $p|\binom{p}{k}$.

Respuesta

Sea p un número primo y $k \in \{1, \ldots, p-1\}$, notemos que por propiedad de divisibilidad $p \mid p$. De lo anterior podemos afirmar que:

$$p \mid p \cdot \frac{(p-1)!}{(k-1)!((p-1)-(k-1))!}$$

Ahora hacemos notar que $p > k$ y además son naturales, podemos afirmar que:

$$k\binom{p}{k} = p\binom{p-1}{k-1}$$

Luego, podemos decir de igual forma que:

$$p \mid k \cdot \binom{p}{k}$$

Notemos entonces que $p \mid k$ debido a que, como habíamos establecido por nuestra hipótesis $p > k$, por lo que este término no lo tomaremos en cuenta ya que es imposible que p sea su divisor. Dicho esto concluimos que:

$$p \mid \binom{p}{k} \blacksquare$$

- **11.** Sean $a, b, t \in \mathbb{Z}$ con $t \neq 0$. Muestra que si $mcd(k, t) = 1$ y $at \equiv bt \mod k$, entonces $a \equiv b \mod k$.

Respuesta

Como $at \equiv bt \mod k$, entonces por definición de congruencia
$k \mid at - bt$,
entonces $k \mid t(a - b)$

Como $mcd(k, t) = 1$ y $k \mid t(a - b)$, entonces por propiedad (*Lema 2.2.8*),
$k \mid a - b$, por definición de congruencia, entonces
$a \equiv b \mod k$ ■

- **12.** Muestra que si $a \equiv b \mod k$, entonces $mcd(a, k) = mcd(b, k)$.

Respuesta

Hipotésis. $a \equiv b \mod k$, entonces $k \mid a - b$

Tenemos que $k \mid a$ y $k \mid b$.

$mcd(a, k) \mid a$ y $mcd(a, k) \mid k$

$mcd(b, k) \mid b$ y $mcd(b, k) \mid k$

Como $mcd(a, k) \mid k$ y $k \mid b$, entonces $mcd(a, k) \mid b$

Como $mcd(b, k) \mid k$ y $k \mid a$, entonces $mcd(b, k) \mid a$

De lo anterior sabemos que $mcd(b, k) \mid a$ y $mcd(b, k) \mid b$, tambien $mcd(a, k) \mid a$ y $mcd(a, k) \mid b$

$\therefore mcd(a, k) = mcd(b, k)$ ■

- **13.** Sea $k = mcd(m, n)$. Muestra que si $a \equiv b \mod m$ y $c \equiv d \mod n$, entonces $a + c \equiv b + d \mod k$.

Respuesta

Hipotésis 1: $a \equiv b \mod m$, entonces $m \mid a - b$

Hipotésis 2: $c \equiv d \mod n$, entonces $n \mid c - d$

Como $k = mcd(m, n)$, entonces $k \mid m$ y $k \mid n$

Como $k \mid m$ y $m \mid a - b$, entonces:

$$k \mid a - b$$

Como $k \mid n$ y $n \mid c - d$, entonces:

$$k \mid c - d$$

Así:

$$k \mid (a-b)+(c-d)$$
$$= k \mid (a+c)-b-d$$
$$= k \mid (a+c)-(c+d)$$
$$a+c \equiv b+d \ mod \ k \ \blacksquare$$

- **14.** Sean a, b y k enteros tales que $a \equiv b$ mod k. Muestra que si $0 \leq a < k$ y $0 \leq b < k$, entonces $a = b$.

Respuesta

Sean a, b, k enteros tal que $a \equiv b$ mod k, por definición de congruencia
$k \mid a-b$, por definición de divisibilidad
existe $n \in \mathbb{Z}$ tal que $k \cdot n = a-b$

Como $0 \leq a < k$ y $0 \leq b < k$, entonces restando ambas desigualdades
$0-k < a-b < k$, entonces
$-k < a-b < k$

Dado que $a-b = k \cdot n$ y $k \cdot n \in \mathbb{Z}$, es decir, un múltiplo de k, pero sabemos que
$-k < a-b < k$, por lo que $n = 0$, entonces
$a-b = k \cdot 0 = 0$
$a-b = 0$, despejando
$a = b \ \blacksquare$

- **15.** Considera la ecuación diofantina $56x + 378y = k$. Calcula todos los valores de k entre 100 y 200 para los cuales dicha ecuación tiene solución entera. Calcula la solución para el caso en que $k = 154$.

Respuesta

Para calcular los valores solicitados tenemos que sacar en primer lugar el $mcd(56, 378)$ notemos entonces por algortimo de Euclides:
$378 = 56 \cdot 6 + 42$
$56 = 42 \cdot 1 + 14$
$42 = 14 \cdot 3 + 0$
Así, tomando el ultimo residuo distinto de 0, el $mcd(56, 378) = 14$

Ahora para saber si $14 \mid k$ expresemos la combinación líneal de 14 respeto de 56 y 378
Por lo anterior, supongamos que exiten $s, t \in \mathbb{Z}$ tales que $56t + 378s = 14$

Tambien, debemos calcular un $r \in \mathbb{Z}$ tal que $14 \cdot r = k$
Notemos que por hipotesis, k puede tomar valores entre 100 y 200, si sacamos los multiplos de 14 entre ese rango tenemos el caso particular de $14 \cdot 11 = 154$, asi $r = 11 \ y \ k = 154$

$$\text{mcd}(56, 378) = 14$$

Notemos entonces que para encontrar las soluciones enteras de la ecuación diofantina se debe cumplir que $\text{mcd}(56, 378) \mid K$ que entonces está en un rango $100 < k < 200$, notemos entonces que por definición todos los números enteros que sean múltiplos de 14 tendrán solución entera, obviamente en el rango impuesto:

Ahora notemos que el único múltiplo de 14 que es mayor a 100 es:

$14 \times 8 = 112$ de aquí lo único que resta para conseguir las soluciones es sumar a 112 de 14 en 14.

$$\begin{aligned} 14 \times 9 &= 126 \\ 14 \times 10 &= 140 \\ 14 \times 11 &= 154 \\ 14 \times 12 &= 168 \\ 14 \times 13 &= 182 \\ 14 \times 14 &= 196 \end{aligned}$$

Estos serán los únicos números para los cuales la ecuación diofantina tendrá soluciones enteras. Para el caso específico de $k = 154$, como ya sabemos que es divisor entre el mcd, entonces ahora sacamos la ecuación lineal tal que:

$$56s + 378t = 14$$

esta será:

$$56 \times 7 + 378 \times (-1) = 14$$

Notemos que $14 \times 11 = 154$

por tanto para finalizar nuestra ecuación:

$$(11 \times 7, 11 \times -1) = (77, -11)$$

Comprobando:

$$56 \times 77 + 378 \times (-11) = 154$$

Ejercicios extra

- **Extra 1.**Demuestra que todo número natural $n = p_1^{a_1} \cdots p_k^{a_k}$ no puede tener más de un factor primo p_i mayor a $\sqrt{n}$.

Como tenemos que demostrar una existencia única, procederemos por contradicción. Supongamos que existen dos factores primos $p_i > \sqrt{n}$ y $p_j > \sqrt{n}$ distintos.

Dado que p_i y p_j son dos factores primos distintos, tenemos:

$$p_i \cdot p_j > \sqrt{n} \cdot \sqrt{n} = n$$

De lo anterior, y considerando que por hipótesis tanto p_i como p_j son menores que n (pues son factores primos de n), llegamos a una contradicción. Por definición de divisibilidad:

$$n \mid p_i \cdot p_j$$

lo que implica por propiedades que:

$$n \geq p_i \cdot p_j > n$$

Esto demuestra la contradicción $n > n$. De esto último concluimos que en la factorización:

$$n = p_1^{a_1} \cdots p_k^{a_k}$$

no puede haber más de un factor primo p_i mayor que $\sqrt{n}$.

• **Extra 2.** Sean $a_1, ..., a_n$ una colección de enteros no nulos. Muestra que si $mcd(a_1, ..., a_n) = 1$, entonces se satisface que $mcm(a_1, ..., a_n) =$

$$\prod_{i=1}^{n} a_i$$

Respuesta

Sean $a_1, ..., a_n$ una colección de enteros no nulos tales que $mcd(a_1, ..., a_n) = 1$.

Por teorema, $mcm(a_1, ..., a_n) = \frac{|a_1 \cdots a_n|}{mcd(a_1,...,a_n)}$, pero esto es lo mismo que: $mcm(a_1, ..., a_n) = |a_1 \cdots a_n|$ ya que, $mcd(a_1, ..., a_n) = 1$.

Entonces, como $mcm(a_1, ..., a_n) \geq 1$ por definición de mínimo común múltiplo, y $mcm(a_1, ..., a_n) = |a_1 \cdots a_n|$ entonces, por definición de valor absoluto:

$mcm(a_1, ..., a_n) = a_1 \cdots a_n$

$\therefore$ $mcm(a_1, ..., a_n) =$

$$\prod_{i=1}^{n} a_i$$

$\therefore$ Se cumple que si $mcd(a_1, ..., a_n) = 1$, entonces se satisface que $mcm(a_1, ..., a_n) =$

$$\prod_{i=1}^{n} a_i \blacksquare$$