Matemática Discreta I
Clase 14 - Factorización prima 1

FAMAF / UNC

4 de mayo de 2021

Sabemos que $\lim a_n = l$ y $\lim b_n = m$ $\forall n > 0$

Definición

Se dice que un entero positivo p es *primo* si $p \geq 2$ y los únicos enteros positivos que dividen p son 1 y p mismo.

Definición

Se dice que un entero positivo p es *primo* si $p \geq 2$ y los únicos enteros positivos que dividen p son 1 y p mismo.

Los primeros primos (los menores que 100) son

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97.

Definición

Se dice que un entero positivo p es *primo* si $p \geq 2$ y los únicos enteros positivos que dividen p son 1 y p mismo.

Los primeros primos (los menores que 100) son

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97.

Enfaticemos que de acuerdo a la definición, 1 *no* es primo.

- p es primo si y solo si $P = m_1 m_2 \Rightarrow m_1 = 1, m_2 = p$ o $m_1 = p, m_2 = 1$.

- p es primo si y solo si $P = m_1 m_2 \Rightarrow m_1 = 1, m_2 = p$ o $m_1 = p, m_2 = 1$.
- $m \geq 2$ no es un primo si y sólo si existen $1 < m_1, m_2 < m$, tales que $m = m_1 m_2$.

- p es primo si y solo si $P = m_1 m_2 \Rightarrow m_1 = 1, m_2 = p$ o $m_1 = p, m_2 = 1$.
- $m \geq 2$ no es un primo si y sólo si existen $1 < m_1, m_2 < m$, tales que $m = m_1 m_2$.

No son primos:

$$4 = 2 \cdot 2, \quad 6 = 2 \cdot 3, \quad 8 = 2 \cdot 4, \quad 9 = 3 \cdot 3,$$
$$10 = 2 \cdot 5, \quad 12 = 3 \cdot 4, \quad 14 = 2 \cdot 7, \quad 15 = 3 \cdot 5,$$
$$16 = 2 \cdot 8, \quad 18 = 2 \cdot 9, \quad 20 = 4 \cdot 5, \quad 21 = 3 \cdot 7.$$

$= 63$

Veremos que todo número entero positivo puede expresarse como producto de primos. Por ejemplo

$$825 = 3 \cdot 5 \cdot 5 \cdot 11.$$

Veremos que todo número entero positivo puede expresarse como producto de primos. Por ejemplo

$$825 = 3 \cdot 5 \cdot 5 \cdot 11.$$

Si el entero es negativo, es -1 por un producto de primos

$$-825 = -1 \cdot 3 \cdot 5 \cdot 5 \cdot 11.$$

Veremos que todo número entero positivo puede expresarse como producto de primos. Por ejemplo

$$825 = 3 \cdot 5 \cdot 5 \cdot 11.$$

Si el entero es negativo, es -1 por un producto de primos

$$-825 = -1 \cdot 3 \cdot 5 \cdot 5 \cdot 11.$$

Como consecuencia del axioma del buen orden obtenemos que todo entero positivo es producto de primos (si p es primo, también lo consideramos un producto de primos.)

Teorema

Todo entero mayor que 1 *es producto de números primos.*

Idea $B = \{m : m \text{ no es producto de primos} \wedge m > 1\} \subseteq \mathbb{N}$

Supongamos que $B \neq \emptyset$ (llegaremos a un absurdo)

Si $B \neq \emptyset$, por BO $\Rightarrow \exists$ mo mínimo en B.

Pero mo no es primo $\Rightarrow mo = \overline{m_1 \cdot m_2}$

$1 < m_1, m_2 < mo \Rightarrow m_1, m_2 > 1$ y $\notin B$.

$\Rightarrow m_1 \wedge m_2$ prod. de primos $\Rightarrow mo = m_1 \cdot m_2$ prod. de primos ABS

Teorema

Todo entero mayor que 1 *es producto de números primos.*

Idea de la demostración

Teorema

Todo entero mayor que 1 *es producto de números primos.*

Idea de la demostración

$$B = \{n > 1 : n \text{ no es producto de primos}\}.$$

Teorema

Todo entero mayor que 1 *es producto de números primos.*

Idea de la demostración

$$B = \{n > 1 : n \text{ no es producto de primos}\}.$$

Si $B \neq \emptyset$, por BO existe m mínimo de B.

Teorema

Todo entero mayor que 1 *es producto de números primos.*

Idea de la demostración

$$B = \{n > 0 : n \text{ no es producto de primos}\}.$$

Si $B \neq \emptyset$, por BO existe m mínimo de B.

m no es primo $\Rightarrow m = m_1 m_2$ con $1 < m_1, m_2 < m$.

Teorema

Todo entero mayor que 1 *es producto de números primos.*

Idea de la demostración

$$B = \{n > 1 : n \text{ no es producto de primos}\}.$$

Si $B \neq \emptyset$, por BO existe m mínimo de B.

m no es primo $\Rightarrow m = m_1 m_2$ con $1 < m_1, m_2 < m$.

Como $m_1, m_2 < m$, ambos son producto de primos.

Teorema

Todo entero mayor que 1 *es producto de números primos.*

Idea de la demostración

$$B = \{n > 1 : n \text{ no es producto de primos}\}.$$

Si $B \neq \emptyset$, por BO existe m mínimo de B.

m no es primo $\Rightarrow m = m_1 m_2$ con $1 < m_1, m_2 < m$.

Como $m_1, m_2 < m$, ambos son producto de primos.

Luego $m_1 m_2 = m$ es producto de primos. Absurdo.

Teorema

Todo entero mayor que 1 *es producto de números primos.*

Idea de la demostración

$$B = \{n > 1 : n \text{ no es producto de primos}\}.$$

Si $B \neq \emptyset$, por BO existe m mínimo de B.

m no es primo $\Rightarrow m = m_1 m_2$ con $1 < m_1, m_2 < m$.

Como $m_1, m_2 < m$, ambos son producto de primos.

Luego $m_1 m_2 = m$ es producto de primos. Absurdo.

El absurdo vino de suponer que $B \neq \emptyset$. □

Observación

- Por el teorema, decimos que todo número *admite una factorización con factores primos*.

Observación

- Por el teorema, decimos que todo número *admite una factorización con factores primos*.

Ejemplo

Encontremos la factorización en números primos de 201 000. Esto se hace dividiendo sucesivamente los números hasta llegar a factores primos:

Observación

- Por el teorema, decimos que todo número *admite una factorización con factores primos*.

Ejemplo

Encontremos la factorización en números primos de 201 000. Esto se hace dividiendo sucesivamente los números hasta llegar a factores primos:

$$\begin{aligned} 201\,000 &= 201 \cdot 1000 = 3 \cdot 67 \cdot 10 \cdot 10 \cdot 10 \\ &= 3 \cdot 67 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \\ &= 2^3 \cdot 3 \cdot 5^3 \cdot 67. \end{aligned}$$

Como vimos más arriba $2, 3, 5$ y 67 son números primos y por lo tanto hemos obtenido la descomposición prima de 201 000.

p primo si $a \mid p \Rightarrow a = 1$ o $a = p$ $(a > 0)$

Observación

Sea $a \in \mathbb{Z}$ y p primo. Entonces

a) Si $p \nmid a$, entonces $\text{mcd}(a, p) = 1$.

Dem Sea $d = \text{mcd}(a, p) \Rightarrow$

$d \mid a \wedge d \mid p \Rightarrow d = 1$ o $d = p$

como $p \nmid a \Rightarrow d \neq p \Rightarrow d = 1$.

Observación

Sea $a \in \mathbb{Z}$ y p primo. Entonces

a) Si $p \nmid a$, entonces $\text{mcd}(a, p) = 1$.

b) Si p y p' son primos y $p|p'$ entonces $p = p'$.

Dem $p|p' \Rightarrow p=1$ o $p=p' \overset{p \neq 1}{\Rightarrow} p=p'$

(Vale $a>1$ y $a|p \Rightarrow a=p$)

Observación

Sea $a \in \mathbb{Z}$ y p primo. Entonces

a) Si $p \nmid a$, entonces $\text{mcd}(a, p) = 1$.

b) Si p y p' son primos y $p|p'$ entonces $p = p'$.

Demostración

Observación

Sea $a \in \mathbb{Z}$ y p primo. Entonces

a) Si $p \nmid a$, entonces $\text{mcd}(a, p) = 1$.

b) Si p y p' son primos y $p|p'$ entonces $p = p'$.

Demostración

(a) Como los únicos divisores de p son p y 1, y $p \nmid a$, el único divisor común de p y a es 1.

Observación

Sea $a \in \mathbb{Z}$ y p primo. Entonces

a) Si $p \nmid a$, entonces $\text{mcd}(a, p) = 1$.

b) Si p y p' son primos y $p|p'$ entonces $p = p'$.

Demostración

(a) Como los únicos divisores de p son p y 1, y $p \nmid a$, el único divisor común de p y a es 1.

(b) p' es primo, por lo tanto tiene sólo dos divisores positivos 1 y p'. Como p no es 1, tenemos que $p = p'$. □

Lema

Si $n > 0$ no es primo, entonces existe $m > 0$ tal que $m|n$ y $m \leq \sqrt{n}$.

Lema

Si $n > 0$ no es primo, entonces existe $m > 0$ tal que $m|n$ y $m \leq \sqrt{n}$.

Demostración

Lema

Si $n > 0$ no es primo, entonces existe $m > 0$ tal que $m|n$ y $m \leq \sqrt{n}$.

Demostración

Sea $n > 1$ que no es primo. Entonces existe m_1, m_2 tal que

$$1 < m_1, m_2 < n \quad \text{y} \quad n = m_1 m_2.$$

Lema

Si $n > 0$ no es primo, entonces existe $m > 0$ tal que $m|n$ y $m \leq \sqrt{n}$.

Demostración

Sea $n > 1$ que no es primo. Entonces existe m_1, m_2 tal que

$$1 < m_1, m_2 < n \quad \text{y} \quad n = m_1 m_2.$$

Veamos que $m_1 \leq \sqrt{n}$ o $m_2 \leq \sqrt{n}$

Si $m_1 > \sqrt{n}$ y $m_2 > \sqrt{n}$ entonces

$$n = m_1 m_2 > \sqrt{n}\sqrt{n} = \sqrt{n}^2 = n.$$

Lema

Si $n > 0$ no es primo, entonces existe $m > 0$ tal que $m|n$ y $m \leq \sqrt{n}$.

Demostración

Sea $n > 1$ que no es primo. Entonces existe m_1, m_2 tal que

$$1 < m_1, m_2 < n \quad \text{y} \quad n = m_1 m_2.$$

Si $m_1 > \sqrt{n}$ y $m_2 > \sqrt{n}$ entonces

$$m_1 m_2 > \sqrt{n}\sqrt{n} = \sqrt{n}^2 = n. \qquad (m > m)$$

Absurdo. Vino de suponer que $m_1 > \sqrt{n}$ y $m_2 > \sqrt{n}$.

Luego $m_1 \leq \sqrt{n}$ o $m_2 \leq \sqrt{n}$ □

El contrarrecíproco del lema anterior, es el *criterio de la raíz*:

El contrarrecíproco del lema anterior, es el *criterio de la raíz*:

Proposición

Sea $n \geq 2$. Si para todo m tal que $1 < m \leq \sqrt{n}$ se cumple que $m \nmid n$, entonces n es primo.

El contrarrecíproco del lema anterior, es el *criterio de la raíz*:

Proposición

Sea $n \geq 2$. Si para todo m tal que $1 < m \leq \sqrt{n}$ se cumple que $m \nmid n$, entonces n es primo.

Corolario

Sea $n \geq 2$. Si para todo p primo tal que $1 < p \leq \sqrt{n}$ se cumple que $p \nmid n$, entonces n es primo.

Ejemplo

Verifiquemos si 467 es primo o no.

Ejemplo

Verifiquemos si 467 es primo o no.

Solución

Si no utilizamos el criterio de la raíz deberíamos hacer 465 divisiones: deberíamos comprobar si $m|467$ con $1 < m < 467$.

Ejemplo

Verifiquemos si 467 es primo o no.

Solución

Si no utilizamos el criterio de la raíz deberíamos hacer 465 divisiones: deberíamos comprobar si $m|467$ con $1 < m < 467$.

Como $\sqrt{467} = 21.61...$, sólo debemos comprobar si $m|467$ para $2 \leq m \leq 21$.

Ejemplo

Verifiquemos si 467 es primo o no.

Solución

Si no utilizamos el criterio de la raíz deberíamos hacer 465 divisiones: deberíamos comprobar si $m|467$ con $1 < m < 467$.

Como $\sqrt{467} = 21.61...$, sólo debemos comprobar si $m|467$ para $2 \leq m \leq 21$. (20 comprobaciones)

Un sencilla comprobación (dividiendo) muestra que los números $2, 3, \cdots, 20, 21$ no dividen a 467 y por lo tanto 467 es primo.

Ejemplo

Verifiquemos si 467 es primo o no.

Solución

Si no utilizamos el criterio de la raíz deberíamos hacer 465 divisiones: deberíamos comprobar si $m|467$ con $1 < m < 467$.

Como $\sqrt{467} = 21.61...$, sólo debemos comprobar si $m|467$ para $2 \leq m \leq 21$.

Un sencilla comprobación (dividiendo) muestra que los números $2, 3, \cdots, 20, 21$ no dividen a 467 y por lo tanto 467 es primo.

Observación

En el ejemplo anterior podríamos haber solo comprobado si los primos 2, 3, 5, 7, 11, 13, 17, 19 dividen a 467.

Teorema

Sea p un número primo.

a) Si $p|xy$ entonces $p|x$ o $p|y$.

b) $x_1, x_2, \ldots, x_n$ son enteros tales que

$$p|x_1 x_2 \ldots x_n$$

entonces $p|x_i$ para algún x_i $(1 \leq i \leq n)$.

Observación

La propiedad a) es *muy importante* y podíamos haber definido número primo como aquel número que cumple esta propiedad.

Un error común es asumir que la propiedad a) se mantiene verdadera cuando reemplazamos el primo p por un entero arbitrario . Pero esto claramente falso: por ejemplo

$$6 \mid 3 \cdot 8 \quad \text{pero} \quad 6 \nmid 3 \quad \text{y} \quad 6 \nmid 8.$$

Un error común es asumir que la propiedad a) se mantiene verdadera cuando reemplazamos el primo p por un entero arbitrario . Pero esto claramente falso: por ejemplo

$$6|3 \cdot 8 \quad \text{pero} \quad 6 \not| 3 \quad \text{y} \quad 6 \not| 8.$$

La propiedad a) juega un papel crucial en la demostración del siguiente resultado, que a veces es llamado el *Teorema Fundamental de la Aritmética*.

Teorema

La factorización en primos de un entero positivo $n \geq 2$ es única, salvo el orden de los factores primos.

Luego todo entero positivo n puede escribirse como

$$m = q_1 \cdot q_2 \cdot \cdots \cdot q_{m-1} \cdot q_m$$

donde los q_i son primos no necesariamente distintos.

En la práctica a menudo reunimos los primos iguales en la factorización de n y escribimos

$$n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}, \tag{1}$$

donde $p_1, p_2, \dots, p_r$ son primos distintos y $e_1, e_2, \dots, e_r$ son enteros positivos.

Ejemplo

Encontrar la descomposición prima de 7000.

Solución

$7000 = 1000 \cdot 7 = 10 \cdot 10 \cdot 10 \cdot 7 = 2 \cdot 5 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \cdot 7$, Es decir

$$7000 = 2 \cdot 5 \cdot 2 \cdot 5 \cdot 2 \cdot 5 \cdot 7.$$

Pero suele ser mejor escribirlo como

$$7000 = 2^3 \cdot 5^3 \cdot 7^1.$$