Divisibilidad

Myrian Sadith González
Pedro José Molina Morales

Universidad Nacional Autónoma de Honduras
Facultad de Ciencias
Departamento de Matemática Aplicada

1. Divisibilidad
    - Números primos
    - Algoritmo de división
    - Máximo común divisor
    - Algoritmo de Euclides
    - Mínimo común múltiplo
2. Teorema fundamental de la aritmética
3. Ecuaciones de Diofanto
    - Ejercicios de práctica

Divisibilidad

Definición

Si $a, b \in \mathbb{Z}$ y $b \neq 0$, decimos que b **divide a** a, y lo denotamos $b|a$, si existe un entero k tal que $a = bk$. Cuando esto ocurre, decimos que b es un **divisor** de a, o que a es un **múltiplo** de b.

Divisibilidad

Definición

Si $a, b \in \mathbb{Z}$ y $b \neq 0$, decimos que b **divide a** a, y lo denotamos $b|a$, si existe un entero k tal que $a = bk$. Cuando esto ocurre, decimos que b es un **divisor** de a, o que a es un **múltiplo** de b.

Ejemplos

1. $5|10$

Divisibilidad

Definición

Si $a, b \in \mathbb{Z}$ y $b \neq 0$, decimos que b **divide a** a, y lo denotamos $b|a$, si existe un entero k tal que $a = bk$. Cuando esto ocurre, decimos que b es un **divisor** de a, o que a es un **múltiplo** de b.

Ejemplos

1. $5|10$, dado que $10 = 5(2)$

Divisibilidad

Definición

Si $a, b \in \mathbb{Z}$ y $b \neq 0$, decimos que b **divide a** a, y lo denotamos $b|a$, si existe un entero k tal que $a = bk$. Cuando esto ocurre, decimos que b es un **divisor** de a, o que a es un **múltiplo** de b.

Ejemplos

1. $5|10$, dado que $10 = 5(2)$
2. $n \in \mathbb{Z}$, $2|2n$

Divisibilidad

Definición

Si $a, b \in \mathbb{Z}$ y $b \neq 0$, decimos que b **divide a** a, y lo denotamos $b|a$, si existe un entero k tal que $a = bk$. Cuando esto ocurre, decimos que b es un **divisor** de a, o que a es un **múltiplo** de b.

Ejemplos

1. $5|10$, dado que $10 = 5(2)$
2. $n \in \mathbb{Z}$, $2|2n$, dado que $2n = 2n$.

Divisibilidad

Definición

Si $a, b \in \mathbb{Z}$ y $b \neq 0$, decimos que b **divide a** a, y lo denotamos $b|a$, si existe un entero k tal que $a = bk$. Cuando esto ocurre, decimos que b es un **divisor** de a, o que a es un **múltiplo** de b.

Ejemplos

1. $5|10$, dado que $10 = 5(2)$
2. $n \in \mathbb{Z}$, $2|2n$, dado que $2n = 2n$.
3. $3|369$

Divisibilidad

Definición

Si $a, b \in \mathbb{Z}$ y $b \neq 0$, decimos que b **divide a** a, y lo denotamos $b|a$, si existe un entero k tal que $a = bk$. Cuando esto ocurre, decimos que b es un **divisor** de a, o que a es un **múltiplo** de b.

Ejemplos

1. $5|10$, dado que $10 = 5(2)$
2. $n \in \mathbb{Z}$, $2|2n$, dado que $2n = 2n$.
3. $3|369$, dado que $369 = 3(123)$.

Divisibilidad

Teorema

Para cualesquiera $a, b, c \in \mathbb{Z}$.

a. $1|a$ y $a|0$
b. $[(a|b) \wedge (b|a)] \Rightarrow a = \pm b$
c. $[(a|b) \wedge (b|c)] \Rightarrow a|c$
d. $a|b \Rightarrow a|bx$ para todo $x \in \mathbb{Z}$
e. Si $x = y + z$, para $x, y, z \in \mathbb{Z}$ y a divide a dos de los enteros x, y, z entonces a divide al entero restante.
f. $[(a|b) \wedge (a|c)] \Rightarrow a|(bx + cy)$ para todos $x, y \in \mathbb{Z}$
g. Para $1 \leq i \leq n$ sea $c_i \in \mathbb{Z}$. Si a divide a cada c_i, entonces $a|(c_1x_1 + c_2x_2 + \cdots + c_nx_n)$, donde $x_i \in \mathbb{Z}$ para todo $1 \leq i \leq n$.

Divisibilidad

Demostración:

c. $([(a|b) \wedge (b|c)] \Rightarrow a|c)$

Divisibilidad

Demostración:

c. ($[(a|b) \wedge (b|c)] \Rightarrow a|c$)

Si $a|b$ y $b|c$, entonces $b = am$ y $c = bn$ para algunos $n, m \in \mathbb{Z}$

Divisibilidad

Demostración:

c. $([(a|b) \wedge (b|c)] \Rightarrow a|c)$

Si $a|b$ y $b|c$, entonces $b = am$ y $c = bn$ para algunos $n, m \in \mathbb{Z}$.
Sustituyendo b tenemos que $c = bn = (am)n = a(mn)$

Divisibilidad

Demostración:

c. ($[(a|b) \wedge (b|c)] \Rightarrow a|c$)

Si $a|b$ y $b|c$, entonces $b = am$ y $c = bn$ para algunos $n, m \in \mathbb{Z}$. Sustituyendo b tenemos que $c = bn = (am)n = a(mn)$. Sea $k = mn \in \mathbb{Z}$

Divisibilidad

Demostración:

c. $([(a|b) \wedge (b|c)] \Rightarrow a|c)$

Si $a|b$ y $b|c$, entonces $b = am$ y $c = bn$ para algunos $n, m \in \mathbb{Z}$. Sustituyendo b tenemos que $c = bn = (am)n = a(mn)$. Sea $k = mn \in \mathbb{Z}$, reescribiendo $c = ak$

Divisibilidad

Demostración:

c. ($[(a|b) \wedge (b|c)] \Rightarrow a|c$)

Si $a|b$ y $b|c$, entonces $b = am$ y $c = bn$ para algunos $n, m \in \mathbb{Z}$. Sustituyendo b tenemos que $c = bn = (am)n = a(mn)$. Sea $k = mn \in \mathbb{Z}$, reescribiendo $c = ak \Rightarrow a|c$

Divisibilidad

Demostración:

c. $([(a|b) \wedge (b|c)] \Rightarrow a|c)$

   Si $a|b$ y $b|c$, entonces $b = am$ y $c = bn$ para algunos $n, m \in \mathbb{Z}$. Sustituyendo b tenemos que $c = bn = (am)n = a(mn)$. Sea $k = mn \in \mathbb{Z}$, reescribiendo $c = ak \Rightarrow a|c$

f. $([(a|b) \wedge (a|c)] \Rightarrow a|(bx + cy)$ para todos $x, y \in \mathbb{Z})$

Divisibilidad

Demostración:

c. ($[(a|b) \wedge (b|c)] \Rightarrow a|c$)

Si $a|b$ y $b|c$, entonces $b = am$ y $c = bn$ para algunos $n, m \in \mathbb{Z}$. Sustituyendo b tenemos que $c = bn = (am)n = a(mn)$. Sea $k = mn \in \mathbb{Z}$, reescribiendo $c = ak \Rightarrow a|c$

f. ($[(a|b) \wedge (a|c)] \Rightarrow a|(bx + cy)$ para todos $x, y \in \mathbb{Z}$)

Si $a|b$ y $a|c$, entonces $b = an$ y $c = am$ para algunos $n, m \in \mathbb{Z}$

Divisibilidad

Demostración:

c. ($[(a|b) \wedge (b|c)] \Rightarrow a|c$)

Si $a|b$ y $b|c$, entonces $b = am$ y $c = bn$ para algunos $n, m \in \mathbb{Z}$. Sustituyendo b tenemos que $c = bn = (am)n = a(mn)$. Sea $k = mn \in \mathbb{Z}$, reescribiendo $c = ak \Rightarrow a|c$

f. ($[(a|b) \wedge (a|c)] \Rightarrow a|(bx + cy)$ para todos $x, y \in \mathbb{Z}$)

Si $a|b$ y $a|c$, entonces $b = an$ y $c = am$ para algunos $n, m \in \mathbb{Z}$. Sean $x, y \in \mathbb{Z}$ (tomados arbitrariamente), tenemos que $bx + cy = (an)x + (am)y = a(nx) + a(my) = a(nx + my)$

Divisibilidad

Demostración:

c. $([(a|b) \wedge (b|c)] \Rightarrow a|c)$

Si $a|b$ y $b|c$, entonces $b = am$ y $c = bn$ para algunos $n, m \in \mathbb{Z}$. Sustituyendo b tenemos que $c = bn = (am)n = a(mn)$. Sea $k = mn \in \mathbb{Z}$, reescribiendo $c = ak \Rightarrow a|c$

f. $([(a|b) \wedge (a|c)] \Rightarrow a|(bx + cy)$ para todos $x, y \in \mathbb{Z})$

Si $a|b$ y $a|c$, entonces $b = an$ y $c = am$ para algunos $n, m \in \mathbb{Z}$. Sean $x, y \in \mathbb{Z}$ (tomados arbitrariamente), tenemos que $bx + cy = (an)x + (am)y = a(nx) + a(my) = a(nx + my)$. Sea $k = nx + my \in \mathbb{Z}$ (cerradura de la suma y del producto en $\mathbb{Z}$), reescribiendo $bx + cy = ak$

Divisibilidad

Demostración:

c. $([(a|b) \wedge (b|c)] \Rightarrow a|c)$

Si $a|b$ y $b|c$, entonces $b = am$ y $c = bn$ para algunos $n, m \in \mathbb{Z}$. Sustituyendo b tenemos que $c = bn = (am)n = a(mn)$. Sea $k = mn \in \mathbb{Z}$, reescribiendo $c = ak \Rightarrow a|c$

f. $([(a|b) \wedge (a|c)] \Rightarrow a|(bx + cy)$ para todos $x, y \in \mathbb{Z})$

Si $a|b$ y $a|c$, entonces $b = an$ y $c = am$ para algunos $n, m \in \mathbb{Z}$. Sean $x, y \in \mathbb{Z}$ (tomados arbitrariamente), tenemos que $bx + cy = (an)x + (am)y = a(nx) + a(my) = a(nx + my)$. Sea $k = nx + my \in \mathbb{Z}$ (cerradura de la suma y del producto en $\mathbb{Z}$), reescribiendo $bx + cy = ak \Rightarrow a|(bx + cy)$.

Ejemplos

1. Sean $a, b \in \mathbb{Z}$ tales que $2a + 3b$ sea un múltiplo de 17. Demuestre que 17 divide a $9a + 5b$.

Ejemplos

1. Sean $a, b \in \mathbb{Z}$ tales que $2a + 3b$ sea un múltiplo de 17. Demuestre que 17 divide a $9a + 5b$.

   Demostración:

Ejemplos

1. Sean $a, b \in \mathbb{Z}$ tales que $2a + 3b$ sea un múltiplo de 17. Demuestre que 17 divide a $9a + 5b$.

   Demostración:

   - Por inciso d. del teorema para $x = -4$. Si $17|(2a + 3b)$

Ejemplos

1. Sean $a, b \in \mathbb{Z}$ tales que $2a + 3b$ sea un múltiplo de 17. Demuestre que 17 divide a $9a + 5b$.

   Demostración:

   - Por inciso d. del teorema para $x = -4$. Si $17|(2a+3b) \Rightarrow 17|(-4)(2a+3b)$

Ejemplos

1. Sean $a, b \in \mathbb{Z}$ tales que $2a + 3b$ sea un múltiplo de 17. Demuestre que 17 divide a $9a + 5b$.

   Demostración:

   - Por inciso d. del teorema para $x = -4$. Si $17|(2a + 3b) \Rightarrow 17|(-4)(2a + 3b) \Rightarrow 17|(-8a - 12b)$

Ejemplos

1. Sean $a, b \in \mathbb{Z}$ tales que $2a + 3b$ sea un múltiplo de 17. Demuestre que 17 divide a $9a + 5b$.

   Demostración:

   - Por inciso d. del teorema para $x = -4$. Si $17|(2a + 3b) \Rightarrow 17|(-4)(2a + 3b) \Rightarrow 17|(-8a - 12b)$
   - Tenemos que $17|17(a + b)$

Ejemplos

1. Sean $a, b \in \mathbb{Z}$ tales que $2a + 3b$ sea un múltiplo de 17. Demuestre que 17 divide a $9a + 5b$.

   Demostración:

   - Por inciso d. del teorema para $x = -4$. Si $17|(2a + 3b) \Rightarrow 17|(-4)(2a + 3b) \Rightarrow 17|(-8a - 12b)$
   - Tenemos que $17|17(a + b) \Rightarrow 17|(17a + 17b)$

Ejemplos

1. Sean $a, b \in \mathbb{Z}$ tales que $2a + 3b$ sea un múltiplo de 17. Demuestre que 17 divide a $9a + 5b$.

   Demostración:

   - Por inciso d. del teorema para $x = -4$. Si $17|(2a + 3b) \Rightarrow 17|(-4)(2a + 3b) \Rightarrow 17|(-8a - 12b)$
   - Tenemos que $17|17(a + b) \Rightarrow 17|(17a + 17b)$

   Entonces por inciso f. del teorema para $x = y = 1$

Ejemplos

1. Sean $a, b \in \mathbb{Z}$ tales que $2a + 3b$ sea un múltiplo de 17. Demuestre que 17 divide a $9a + 5b$.

   Demostración:

   - Por inciso d. del teorema para $x = -4$. Si $17|(2a + 3b) \Rightarrow 17|(-4)(2a + 3b) \Rightarrow 17|(-8a - 12b)$
   - Tenemos que $17|17(a + b) \Rightarrow 17|(17a + 17b)$

   Entonces por inciso f. del teorema para $x = y = 1$. Tenemos que $17|[(17a + 17b) + (-8a - 12b)]$

Ejemplos

1. Sean $a, b \in \mathbb{Z}$ tales que $2a + 3b$ sea un múltiplo de 17. Demuestre que 17 divide a $9a + 5b$.

   Demostración:

   - Por inciso d. del teorema para $x = -4$. Si $17|(2a+3b) \Rightarrow 17|(-4)(2a+3b) \Rightarrow 17|(-8a-12b)$
   - Tenemos que $17|17(a+b) \Rightarrow 17|(17a+17b)$

   Entonces por inciso f. del teorema para $x = y = 1$. Tenemos que $17|[(17a+17b)+(-8a-12b)] \Rightarrow 17|[(17-8)a+(17-12)b]$

Ejemplos

1. Sean $a, b \in \mathbb{Z}$ tales que $2a + 3b$ sea un múltiplo de 17. Demuestre que 17 divide a $9a + 5b$.

   Demostración:

   - Por inciso d. del teorema para $x = -4$. Si $17|(2a+3b) \Rightarrow 17|(-4)(2a+3b) \Rightarrow 17|(-8a-12b)$
   - Tenemos que $17|17(a+b) \Rightarrow 17|(17a+17b)$

   Entonces por inciso f. del teorema para $x = y = 1$. Tenemos que $17|[(17a+17b)+(-8a-12b)] \Rightarrow 17|[(17-8)a+(17-12)b] \Rightarrow 17|(9a+5b)$

Ejemplos

2. Sea k cualquier número impar. Demuestre que $k^2 - 1$ es divisible por 8.

Ejemplos

2. Sea k cualquier número impar. Demuestre que $k^2 - 1$ es divisible por 8.

   Demostración:

Ejemplos

2. Sea k cualquier número impar. Demuestre que $k^2 - 1$ es divisible por 8.

   Demostración:

   Como k es un número impar, existe $n \in \mathbb{Z}$ tal que $k = 2n + 1$.

Ejemplos

2. Sea k cualquier número impar. Demuestre que $k^2 - 1$ es divisible por 8.

   Demostración:

   Como k es un número impar, existe $n \in \mathbb{Z}$ tal que $k = 2n + 1$.

$$k^2 - 1 = (2n+1)^2 - 1 = 4n^2 + 4n + 1 - 1 = 4n(n+1)$$

Ejemplos

2. Sea k cualquier número impar. Demuestre que $k^2 - 1$ es divisible por 8.

Demostración:

Como k es un número impar, existe $n \in \mathbb{Z}$ tal que $k = 2n + 1$.

$$k^2 - 1 = (2n+1)^2 - 1 = 4n^2 + 4n + 1 - 1 = 4n(n+1)$$

Entonces, tenemos

$$4|4 \text{ y } 2|n(n+1)$$

Ejemplos

2. Sea k cualquier número impar. Demuestre que $k^2 - 1$ es divisible por 8.

   Demostración:

   Como k es un número impar, existe $n \in \mathbb{Z}$ tal que $k = 2n + 1$.

   $$k^2 - 1 = (2n+1)^2 - 1 = 4n^2 + 4n + 1 - 1 = 4n(n+1)$$

   Entonces, tenemos

   $$\begin{aligned} & 4|4 \text{ y } 2|n(n+1) \\ \Rightarrow\ & 4 \cdot 2|4n(n+1) \end{aligned}$$

Ejemplos

2. Sea k cualquier número impar. Demuestre que $k^2 - 1$ es divisible por 8.

Demostración:

Como k es un número impar, existe $n \in \mathbb{Z}$ tal que $k = 2n + 1$.

$$k^2 - 1 = (2n+1)^2 - 1 = 4n^2 + 4n + 1 - 1 = 4n(n+1)$$

Entonces, tenemos

$$4|4 \text{ y } 2|n(n+1)$$
$$\Rightarrow 4 \cdot 2|4n(n+1) \Rightarrow 8|(k^2 - 1)$$

Por lo tanto, $k^2 - 1$ es divisible por 8.

Propiedades de los números primos

Definición

Un **número primo** es un número natural que tiene únicamente dos divisores positivos distintos: él mismo y el 1.

Propiedades de los números primos

Definición

Un **número primo** es un número natural que tiene únicamente dos divisores positivos distintos: él mismo y el 1.

Definición

Un **número compuesto** es cualquier número natural no primo, es decir, tiene uno o más divisores distintos a 1 y a sí mismo.

Propiedades de los números primos

Definición

Un **número primo** es un número natural que tiene únicamente dos divisores positivos distintos: él mismo y el 1.

Definición

Un **número compuesto** es cualquier número natural no primo, es decir, tiene uno o más divisores distintos a 1 y a sí mismo.

Lema

Si $n \in \mathbb{Z}^+$ y n es compuesto, entonces existe un primo p tal que $p|n$.

Propiedades de los números primos

Definición

Un **número primo** es un número natural que tiene únicamente dos divisores positivos distintos: él mismo y el 1.

Definición

Un **número compuesto** es cualquier número natural no primo, es decir, tiene uno o más divisores distintos a 1 y a sí mismo.

Lema

Si $n \in \mathbb{Z}^+$ y n es compuesto, entonces existe un primo p tal que $p|n$.

Teorema

Euclides. Existe una infinidad de primos.

Propiedades de los números primos

Definición

Un **número primo** es un número natural que tiene únicamente dos divisores positivos distintos: él mismo y el 1.

Definición

Un **número compuesto** es cualquier número natural no primo, es decir, tiene uno o más divisores distintos a 1 y a sí mismo.

Lema

Si $n \in \mathbb{Z}^+$ y n es compuesto, entonces existe un primo p tal que $p|n$.

Teorema

Euclides. Existe una infinidad de primos.

Algoritmo de división

Teorema

Si $a, b \in \mathbb{Z}$, con $b > 0$, entonces existen $q, r \in \mathbb{Z}$ únicos tales que $a = qb + r$, con $0 \leq r < b$.

Algoritmo de división

Teorema

Si $a, b \in \mathbb{Z}$, con $b > 0$, entonces existen $q, r \in \mathbb{Z}$ únicos tales que $a = qb + r$, con $0 \leq r < b$.

Ejemplos

Algoritmo de división

Teorema

Si $a, b \in \mathbb{Z}$, con $b > 0$, entonces existen $q, r \in \mathbb{Z}$ únicos tales que $a = qb + r$, con $0 \leq r < b$.

Ejemplos

1. Cuando $a = 170$ y $b = 11$ en el algoritmo de la división, tenemos que $170 = 15 \cdot 11 + 5$ donde $0 \leq 5 < 11$. Por lo tanto al dividir 170 entre 11, el cociente es 15 y el resto es 5.

Algoritmo de división

Teorema

Si $a, b \in \mathbb{Z}$, con $b > 0$, entonces existen $q, r \in \mathbb{Z}$ únicos tales que $a = qb + r$, con $0 \leq r < b$.

Ejemplos

1. Cuando $a = 170$ y $b = 11$ en el algoritmo de la división, tenemos que $170 = 15 \cdot 11 + 5$ donde $0 \leq 5 < 11$. Por lo tanto al dividir 170 entre 11, el cociente es 15 y el resto es 5.
2. Si el dividendo es 98 y el divisor es 7, del algoritmo de la división tenemos que $98 = 14 \cdot 7$. Así, en este caso, el cociente es 14 y el residuo es 0, y 7 divide exactamente a 98.

Algoritmo de división

Teorema

Si $a, b \in \mathbb{Z}$, con $b > 0$, entonces existen $q, r \in \mathbb{Z}$ únicos tales que $a = qb + r$, con $0 \leq r < b$.

Ejemplos

1. Cuando $a = 170$ y $b = 11$ en el algoritmo de la división, tenemos que $170 = 15 \cdot 11 + 5$ donde $0 \leq 5 < 11$. Por lo tanto al dividir 170 entre 11, el cociente es 15 y el resto es 5.
2. Si el dividendo es 98 y el divisor es 7, del algoritmo de la división tenemos que $98 = 14 \cdot 7$. Así, en este caso, el cociente es 14 y el residuo es 0, y 7 divide exactamente a 98.
3. Sea $a = -45$ y $b = 8$ tenemos $-45 = (-6)8 + 3$, donde $0 \leq 3 < 8$. En consecuencia, el cociente es -6 y el residuo es 3.

Máximo común divisor

Definición

Para $a, b \in \mathbb{Z}$, un entero positivo c es un **divisor común** de a y b si $c|a$ y $c|b$.

Máximo común divisor

Definición

Para $a, b \in \mathbb{Z}$, un entero positivo c es un **divisor común** de a y b si $c|a$ y $c|b$.

Ejemplo:
Los divisores comunes de 30 y 45 son 1, 3, 5 y 15, donde 15 es el mayor de los divisores.

Máximo común divisor

Definición

Para $a, b \in \mathbb{Z}$, un entero positivo c es un **divisor común** de a y b si $c|a$ y $c|b$.

Ejemplo:
Los divisores comunes de 30 y 45 son 1, 3, 5 y 15, donde 15 es el mayor de los divisores.

Definición

Sean $a, b \in \mathbb{Z}$, donde $a \neq 0$ o $b \neq 0$. Entonces $c \in \mathbb{Z}^+$ es el **máximo común divisor** de a, b si

a) $c|a$ y $c|b$

b) para cualquier común divisor d de a y b, tenemos que $d|c$.

Notación: $mcd(a, b)$ es el máximo común divisor de a y b.

Máximo común divisor

Definición

Para $a, b \in \mathbb{Z}$, un entero positivo c es un **divisor común** de a y b si $c|a$ y $c|b$.

Ejemplo:
Los divisores comunes de 30 y 45 son 1, 3, 5 y 15, donde 15 es el mayor de los divisores.

Definición

Sean $a, b \in \mathbb{Z}$, donde $a \neq 0$ o $b \neq 0$. Entonces $c \in \mathbb{Z}^+$ es el **máximo común divisor** de a, b si

a) $c|a$ y $c|b$
b) para cualquier común divisor d de a y b, tenemos que $d|c$.

Notación: $mcd(a, b)$ es el máximo común divisor de a y b.

Ejemplo
El máximo común divisor de 30 y 45 es 15, dado que satisface las condiciones.

Algoritmo de Euclides

Teorema

Si $a, b \in \mathbb{Z}^+$, aplicamos el algoritmo de la división como sigue

$$a = q_1 b + r_1 \qquad\qquad 0 < r_1 < b$$

Algoritmo de Euclides

Teorema

Si $a, b \in \mathbb{Z}^+$, aplicamos el algoritmo de la división como sigue

$$\begin{aligned} a &= q_1 b + r_1 & \qquad 0 < r_1 < b \\ b &= q_2 r_1 + r_2 & \qquad 0 < r_2 < r_1 \end{aligned}$$

Algoritmo de Euclides

Teorema

Si $a, b \in \mathbb{Z}^+$, aplicamos el algoritmo de la división como sigue

$$\begin{aligned} a &= q_1 b + r_1 & \quad 0 < r_1 < b \\ b &= q_2 r_1 + r_2 & \quad 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 & \quad 0 < r_3 < r_2 \end{aligned}$$

Algoritmo de Euclides

Teorema

Si $a, b \in \mathbb{Z}^+$, aplicamos el algoritmo de la división como sigue

$$\begin{array}{cc}
a = q_1 b + r_1 & 0 < r_1 < b \\
b = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\
\vdots & \vdots \\
r_i = q_{i+2} r_{i+1} + r_{i+2} & 0 < r_{i+2} < r_{i+1}
\end{array}$$

Algoritmo de Euclides

Teorema

Si $a, b \in \mathbb{Z}^+$, aplicamos el algoritmo de la división como sigue

$$\begin{array}{rcl} a = q_1 b + r_1 & \qquad & 0 < r_1 < b \\ b = q_2 r_1 + r_2 & & 0 < r_2 < r_1 \\ r_1 = q_3 r_2 + r_3 & & 0 < r_3 < r_2 \\ \vdots & & \vdots \\ r_i = q_{i+2} r_{i+1} + r_{i+2} & & 0 < r_{i+2} < r_{i+1} \\ \vdots & & \vdots \\ r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} & & 0 < r_{k-1} < r_{k-2} \\ r_{k-2} = q_k r_{k-1} + r_k & & 0 < r_k < r_{k-1} \\ r_{k-1} = q_{k+1} r_k + 0 & & \end{array}$$

Entonces, el último resto distinto de cero r_k, es igual a $mcd(a, b)$

Ejemplos

1. Determinar el máximo común divisor de 250 y 111, y exprese el resultado como una combinación lineal de estos enteros

Ejemplo

Ejemplos

1. Determinar el máximo común divisor de 250 y 111, y exprese el resultado como una combinación lineal de estos enteros

Ejemplo

Utilizando el algoritmo de Euclides,

Ejemplos

1. Determinar el máximo común divisor de 250 y 111, y exprese el resultado como una combinación lineal de estos enteros

Ejemplo

Utilizando el algoritmo de Euclides,

$$250 = 2(111) + 28 \qquad 0 < 28 < 111$$

Ejemplos

1. Determinar el máximo común divisor de 250 y 111, y exprese el resultado como una combinación lineal de estos enteros

Ejemplo

Utilizando el algoritmo de Euclides,

$$\begin{aligned} 250 &= 2(111) + 28 & \qquad 0 < 28 < 111 \\ 111 &= 3(28) + 27 & \qquad 0 < 27 < 28 \end{aligned}$$

Ejemplos

1. Determinar el máximo común divisor de 250 y 111, y exprese el resultado como una combinación lineal de estos enteros

Ejemplo

Utilizando el algoritmo de Euclides,

$$\begin{aligned} 250 &= 2(111) + 28 \qquad & 0 < 28 < 111 \\ 111 &= 3(28) + 27 \qquad & 0 < 27 < 28 \\ 28 &= 1(27) + 1 \qquad & 0 < 1 < 27 \end{aligned}$$

Ejemplos

1. Determinar el máximo común divisor de 250 y 111, y exprese el resultado como una combinación lineal de estos enteros

Ejemplo

Utilizando el algoritmo de Euclides,

$$\begin{aligned} 250 &= 2(111) + 28 & \qquad 0 < 28 < 111 \\ 111 &= 3(28) + 27 & \qquad 0 < 27 < 28 \\ 28 &= 1(27) + 1 & \qquad 0 < 1 < 27 \\ 27 &= 27(1) + 0 & \end{aligned}$$

Ejemplos

1. Determinar el máximo común divisor de 250 y 111, y exprese el resultado como una combinación lineal de estos enteros

Ejemplo

Utilizando el algoritmo de Euclides,

$$\begin{array}{rcl} 250 = 2(111) + 28 & \qquad & 0 < 28 < 111 \\ 111 = 3(28) + 27 & & 0 < 27 < 28 \\ 28 = 1(27) + 1 & & 0 < 1 < 27 \\ 27 = 27(1) + 0 & & \end{array}$$

Entonces $mcd(250, 111) = 1$, y así 250 y 111 son primos relativos. Ahora bien, para escribir 1 como combinación lineal de 250 y 111

Ejemplos

1. Determinar el máximo común divisor de 250 y 111, y exprese el resultado como una combinación lineal de estos enteros

Ejemplo

Utilizando el algoritmo de Euclides,

$$\begin{aligned} 250 &= 2(111) + 28 \qquad & 0 < 28 < 111 \\ 111 &= 3(28) + 27 \qquad & 0 < 27 < 28 \\ 28 &= 1(27) + 1 \qquad & 0 < 1 < 27 \\ 27 &= 27(1) + 0 \end{aligned}$$

Entonces $mcd(250, 111) = 1$, y así 250 y 111 son primos relativos. Ahora bien, para escribir 1 como combinación lineal de 250 y 111 , procedemos a trabajar hacia atras desde la tercera ecuación

Ejemplos

1. Determinar el máximo común divisor de 250 y 111, y exprese el resultado como una combinación lineal de estos enteros

Ejemplo

Utilizando el algoritmo de Euclides,

$$\begin{aligned} 250 &= 2(111) + 28 & \quad 0 < 28 < 111 \\ 111 &= 3(28) + 27 & \quad 0 < 27 < 28 \\ 28 &= 1(27) + 1 & \quad 0 < 1 < 27 \\ 27 &= 27(1) + 0 & \end{aligned}$$

Entonces $mcd(250, 111) = 1$, y así 250 y 111 son primos relativos. Ahora bien, para escribir 1 como combinación lineal de 250 y 111 , procedemos a trabajar hacia atras desde la tercera ecuación

$$1 = 28 - 1(27)$$

Ejemplos

1. Determinar el máximo común divisor de 250 y 111, y exprese el resultado como una combinación lineal de estos enteros

Ejemplo

Utilizando el algoritmo de Euclides,

$$\begin{aligned} 250 &= 2(111) + 28 & \qquad 0 < 28 < 111 \\ 111 &= 3(28) + 27 & \qquad 0 < 27 < 28 \\ 28 &= 1(27) + 1 & \qquad 0 < 1 < 27 \\ 27 &= 27(1) + 0 & \end{aligned}$$

Entonces $mcd(250, 111) = 1$, y así 250 y 111 son primos relativos. Ahora bien, para escribir 1 como combinación lineal de 250 y 111 , procedemos a trabajar hacia atras desde la tercera ecuación

$$\begin{aligned} 1 &= 28 - 1(27) \\ &= 28 - 1[111 - 3(28)] \end{aligned}$$

Ejemplos

1. Determinar el máximo común divisor de 250 y 111, y exprese el resultado como una combinación lineal de estos enteros

Ejemplo

Utilizando el algoritmo de Euclides,

$$\begin{aligned} 250 &= 2(111) + 28 \qquad & 0 < 28 < 111 \\ 111 &= 3(28) + 27 \qquad & 0 < 27 < 28 \\ 28 &= 1(27) + 1 \qquad & 0 < 1 < 27 \\ 27 &= 27(1) + 0 \end{aligned}$$

Entonces $mcd(250, 111) = 1$, y así 250 y 111 son primos relativos. Ahora bien, para escribir 1 como combinación lineal de 250 y 111 , procedemos a trabajar hacia atras desde la tercera ecuación

$$\begin{aligned} 1 &= 28 - 1(27) \\ &= 28 - 1[111 - 3(28)] \\ &= (-1)(111) + 4(28) \end{aligned}$$

Ejemplos

1. Determinar el máximo común divisor de 250 y 111, y exprese el resultado como una combinación lineal de estos enteros

Ejemplo

Utilizando el algoritmo de Euclides,

$$\begin{array}{rcl} 250 = 2(111) + 28 & \qquad & 0 < 28 < 111 \\ 111 = 3(28) + 27 & & 0 < 27 < 28 \\ 28 = 1(27) + 1 & & 0 < 1 < 27 \\ 27 = 27(1) + 0 & & \end{array}$$

Entonces $mcd(250, 111) = 1$, y así 250 y 111 son primos relativos. Ahora bien, para escribir 1 como combinación lineal de 250 y 111 , procedemos a trabajar hacia atras desde la tercera ecuación

$$\begin{aligned} 1 &= 28 - 1(27) \\ &= 28 - 1[111 - 3(28)] \\ &= (-1)(111) + 4(28) \\ &= (-1)(111) + 4[250 - 2(111)] \end{aligned}$$

Ejemplos

1. Determinar el máximo común divisor de 250 y 111, y exprese el resultado como una combinación lineal de estos enteros

Ejemplo

Utilizando el algoritmo de Euclides,

$$\begin{aligned} 250 &= 2(111) + 28 & \quad 0 < 28 < 111 \\ 111 &= 3(28) + 27 & \quad 0 < 27 < 28 \\ 28 &= 1(27) + 1 & \quad 0 < 1 < 27 \\ 27 &= 27(1) + 0 & \end{aligned}$$

Entonces $mcd(250, 111) = 1$, y así 250 y 111 son primos relativos. Ahora bien, para escribir 1 como combinación lineal de 250 y 111 , procedemos a trabajar hacia atras desde la tercera ecuación

$$\begin{aligned} 1 &= 28 - 1(27) \\ &= 28 - 1[111 - 3(28)] \\ &= (-1)(111) + 4(28) \\ &= (-1)(111) + 4[250 - 2(111)] \\ &= 4(250) - 9(111) \end{aligned}$$

Ejemplos

2. Para cualquier $n \in \mathbb{Z}^+$, demuestre que los enteros positivos $8n + 3$ y $5n + 2$ son primos relativos.

Ejemplos

2. Para cualquier $n \in \mathbb{Z}^{+}$, demuestre que los enteros positivos $8n + 3$ y $5n + 2$ son primos relativos.

   Solución

Ejemplos

2. Para cualquier $n \in \mathbb{Z}^+$, demuestre que los enteros positivos $8n+3$ y $5n+2$ son primos relativos.

   Solución

   Tenemos que $8n+3 > 5n+2$, y como en el ejemplo anterior, utilizamos el algoritmo de euclides

Ejemplos

2. Para cualquier $n \in \mathbb{Z}^+$, demuestre que los enteros positivos $8n+3$ y $5n+2$ son primos relativos.

Solución

Tenemos que $8n+3 > 5n+2$, y como en el ejemplo anterior, utilizamos el algoritmo de euclides

$$8n+3 = 1(5n+2) + (3n+1) \qquad 0 < 3n+1 < 5n+2$$

Ejemplos

2. Para cualquier $n \in \mathbb{Z}^+$, demuestre que los enteros positivos $8n + 3$ y $5n + 2$ son primos relativos.

   Solución

   Tenemos que $8n + 3 > 5n + 2$, y como en el ejemplo anterior, utilizamos el algoritmo de euclides

$$
\begin{array}{ll}
8n + 3 = 1(5n + 2) + (3n + 1) & \quad 0 < 3n + 1 < 5n + 2 \\
5n + 2 = 1(3n + 1) + (2n + 1) & \quad 0 < 2n + 1 < 3n + 1
\end{array}
$$

Ejemplos

2. Para cualquier $n \in \mathbb{Z}^+$, demuestre que los enteros positivos $8n+3$ y $5n+2$ son primos relativos.

   Solución

   Tenemos que $8n+3 > 5n+2$, y como en el ejemplo anterior, utilizamos el algoritmo de euclides

$$\begin{array}{ll} 8n+3 = 1(5n+2)+(3n+1) & 0 < 3n+1 < 5n+2 \\ 5n+2 = 1(3n+1)+(2n+1) & 0 < 2n+1 < 3n+1 \\ 3n+1 = 1(2n+1)+n & 0 < n < 2n+1 \end{array}$$

Ejemplos

2. Para cualquier $n \in \mathbb{Z}^+$, demuestre que los enteros positivos $8n+3$ y $5n+2$ son primos relativos.

Solución

Tenemos que $8n+3 > 5n+2$, y como en el ejemplo anterior, utilizamos el algoritmo de euclides

$$\begin{aligned}
8n+3 &= 1(5n+2)+(3n+1) & \quad 0 &< 3n+1 < 5n+2 \\
5n+2 &= 1(3n+1)+(2n+1) & \quad 0 &< 2n+1 < 3n+1 \\
3n+1 &= 1(2n+1)+n & \quad 0 &< n < 2n+1 \\
2n+1 &= 2(n)+1 & \quad 0 &< 1 < n
\end{aligned}$$

Ejemplos

2. Para cualquier $n \in \mathbb{Z}^+$, demuestre que los enteros positivos $8n+3$ y $5n+2$ son primos relativos.

Solución

Tenemos que $8n+3 > 5n+2$, y como en el ejemplo anterior, utilizamos el algoritmo de euclides

$$\begin{array}{ll}
8n+3 = 1(5n+2) + (3n+1) & \quad 0 < 3n+1 < 5n+2 \\
5n+2 = 1(3n+1) + (2n+1) & \quad 0 < 2n+1 < 3n+1 \\
3n+1 = 1(2n+1) + n & \quad 0 < n < 2n+1 \\
2n+1 = 2(n) + 1 & \quad 0 < 1 < n \\
n = n(1) + 0 &
\end{array}$$

Ejemplos

2. Para cualquier $n \in \mathbb{Z}^+$, demuestre que los enteros positivos $8n + 3$ y $5n + 2$ son primos relativos.

Solución

Tenemos que $8n + 3 > 5n + 2$, y como en el ejemplo anterior, utilizamos el algoritmo de euclides

$$\begin{array}{ll} 8n+3 = 1(5n+2) + (3n+1) & 0 < 3n+1 < 5n+2 \\ 5n+2 = 1(3n+1) + (2n+1) & 0 < 2n+1 < 3n+1 \\ 3n+1 = 1(2n+1) + n & 0 < n < 2n+1 \\ 2n+1 = 2(n) + 1 & 0 < 1 < n \\ n = n(1) + 0 & \end{array}$$

$$\therefore mcd(8n+3, 5n+2) = 1$$

Mínimo común múltiplo

Definición

Si $a, b, c \in \mathbb{Z}^+$, c es un **múltiplo común** de a, b si c es múltiplo de a y de b. Además, c es el **mínimo común múltiplo** de a, b si es el más pequeño de los enteros positivos que son múltiplos comunes de a, b. Denotamos c como $mcm(a, b)$.

Mínimo común múltiplo

Definición

Si $a, b, c \in \mathbb{Z}^+$, c es un **múltiplo común** de a, b si c es múltiplo de a y de b. Además, c es el **mínimo común múltiplo** de a, b si es el más pequeño de los enteros positivos que son múltiplos comunes de a, b. Denotamos c como $mcm(a, b)$.

Ejemplos

Mínimo común múltiplo

Definición

Si $a, b, c \in \mathbb{Z}^+$, c es un **múltiplo común** de a, b si c es múltiplo de a y de b. Además, c es el **mínimo común múltiplo** de a, b si es el más pequeño de los enteros positivos que son múltiplos comunes de a, b. Denotamos c como $mcm(a, b)$.

Ejemplos

1. Como $15 = 3 \cdot 5$ y ningún otro entero positivo mínimo es un múltiplo de 3 y 5, tenemos que $mcm(5, 3) = 15$.

Mínimo común múltiplo

Definición

Si $a, b, c \in \mathbb{Z}^+$, c es un **múltiplo común** de a, b si c es múltiplo de a y de b. Además, c es el **mínimo común múltiplo** de a, b si es el más pequeño de los enteros positivos que son múltiplos comunes de a, b. Denotamos c como $mcm(a, b)$.

Ejemplos

1. Como $15 = 3 \cdot 5$ y ningún otro entero positivo mínimo es un múltiplo de 3 y 5, tenemos que $mcm(5, 3) = 15$.
2. Para cualquier $n \in \mathbb{Z}^+$, tenemos que $mcm(1, n) = mcm(n, 1) = n$.

Mínimo común múltiplo

Definición

Si $a, b, c \in \mathbb{Z}^+$, c es un **múltiplo común** de a, b si c es múltiplo de a y de b. Además, c es el **mínimo común múltiplo** de a, b si es el más pequeño de los enteros positivos que son múltiplos comunes de a, b. Denotamos c como $mcm(a, b)$.

Ejemplos

1. Como $15 = 3 \cdot 5$ y ningún otro entero positivo mínimo es un múltiplo de 3 y 5, tenemos que $mcm(5, 3) = 15$.
2. Para cualquier $n \in \mathbb{Z}^+$, tenemos que $mcm(1, n) = mcm(n, 1) = n$.
3. Si $a, n \in \mathbb{Z}^+$, tenemos que $mcm(a, na) = na$

Mínimo común múltiplo

Definición

Si $a, b, c \in \mathbb{Z}^+$, c es un **múltiplo común** de a, b si c es múltiplo de a y de b. Además, c es el **mínimo común múltiplo** de a, b si es el más pequeño de los enteros positivos que son múltiplos comunes de a, b. Denotamos c como $mcm(a, b)$.

Ejemplos

1. Como $15 = 3 \cdot 5$ y ningún otro entero positivo mínimo es un múltiplo de 3 y 5, tenemos que $mcm(5, 3) = 15$.
2. Para cualquier $n \in \mathbb{Z}^+$, tenemos que $mcm(1, n) = mcm(n, 1) = n$.
3. Si $a, n \in \mathbb{Z}^+$, tenemos que $mcm(a, na) = na$
4. Si $a, m, n \in \mathbb{Z}^+$ con $m \leq n$, entonces $mcm(a^m, a^n) = a^n$.

Mínimo común múltiplo

Teorema

Para $a, b \in \mathbb{Z}^+$, $ab = mcm(a, b) \cdot mcd(a, b)$

Mínimo común múltiplo

Teorema

Para $a, b \in \mathbb{Z}^+$, $ab = mcm(a, b) \cdot mcd(a, b)$

Ejemplos

Mínimo común múltiplo

Teorema

Para $a, b \in \mathbb{Z}^+$, $ab = mcm(a, b) \cdot mcd(a, b)$

Ejemplos

1. En el ejemplo anterior encontramos que $mcd(250, 111) = 1$. En consecuencia, $mcm(250, 111) = (250)(111) = 27,750$.

Mínimo común múltiplo

Teorema

Para $a, b \in \mathbb{Z}^+$, $ab = mcm(a, b) \cdot mcd(a, b)$

Ejemplos

1. En el ejemplo anterior encontramos que $mcd(250, 111) = 1$. En consecuencia, $mcm(250, 111) = (250)(111) = 27, 750$.
2. Sean $a, m, n \in \mathbb{Z}^+$ con $m \leq n$, entonces

$$mcd(a^m, a^n) = \frac{(a^m)(a^n)}{a^n} = a^m$$

Teorema fundamental de la aritmética

Lema

Si $a, b \in \mathbb{Z}^+$ y p es primo, entonces $p|ab \Rightarrow p|a$ o $p|b$.

Teorema fundamental de la aritmética

Lema

Si $a, b \in \mathbb{Z}^+$ y p es primo, entonces $p|ab \Rightarrow p|a$ o $p|b$.

Lema

Sea $a_i \in \mathbb{Z}^+$ para todo $1 \leq i \leq n$. Si p es primo y $p|a_1 a_2 \cdots a_n$, entonces $p|a_i$ para algún $1 \leq i \leq n$

Teorema fundamental de la aritmética

Lema

Si $a, b \in \mathbb{Z}^+$ y p es primo, entonces $p|ab \Rightarrow p|a$ o $p|b$.

Lema

Sea $a_i \in \mathbb{Z}^+$ para todo $1 \leq i \leq n$. Si p es primo y $p|a_1 a_2 \cdots a_n$, entonces $p|a_i$ para algún $1 \leq i \leq n$

Teorema fundamental de la aritmética

Cada entero $n > 1$ puede escribirse como un producto de primos de forma única, excepto por el orden de estos.

Ejemplos

1. Escriba el número 546756 como un producto de números primos

Ejemplos

1. Escriba el número 546756 como un producto de números primos
   Solución:

Ejemplos

1. Escriba el número 546756 como un producto de números primos
   Solución:

$$546756 = 2(273378)$$

Ejemplos

1. Escriba el número 546756 como un producto de números primos
   Solución:

$$\begin{aligned} 546756 &= 2(273378) \\ &= 2^2(136689) \end{aligned}$$

Ejemplos

1. Escriba el número 546756 como un producto de números primos
   Solución:

$$\begin{aligned} 546756 &= 2(273378) \\ &= 2^2(136689) \\ &= 2^2 \cdot 3(45563) \end{aligned}$$

Ejemplos

1. Escriba el número 546756 como un producto de números primos
   Solución:

$$
\begin{aligned}
546756 &= 2(273378)\\
&= 2^2(136689)\\
&= 2^2 \cdot 3(45563)\\
&= 2^2 \cdot 3 \cdot 7(6509)
\end{aligned}
$$

Ejemplos

1. Escriba el número 546756 como un producto de números primos
   Solución:

$$
\begin{aligned}
546756 &= 2(273378)\\
&= 2^2(136689)\\
&= 2^2 \cdot 3(45563)\\
&= 2^2 \cdot 3 \cdot 7(6509)\\
&= 2^2 \cdot 3 \cdot 7 \cdot 23 \cdot 283
\end{aligned}
$$

Ejemplos

1. Escriba el número 546756 como un producto de números primos
   Solución:

$$
\begin{aligned}
546756 &= 2(273378)\\
&= 2^2(136689)\\
&= 2^2\cdot 3(45563)\\
&= 2^2\cdot 3\cdot 7(6509)\\
&= 2^2\cdot 3\cdot 7\cdot 23\cdot 283
\end{aligned}
$$

Nota: Para verificar si un número n es primo, vamos a dividir por todos los números primos menores a $\sqrt{n}$, y si ninguno de estos lo divide, entonces n es primo.

Ejemplos

2. Sea $n \in \mathbb{Z}^+$. Determine la cantidad de divisores positivos de n.

Ejemplos

2. Sea $n \in \mathbb{Z}^+$. Determine la cantidad de divisores positivos de n.

Solución

Ejemplos

2. Sea $n \in \mathbb{Z}^+$. Determine la cantidad de divisores positivos de n.

   Solución

   Por el teorema fundamental de la aritmética, tenemos que

   $$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

   donde para cada $1 \leq i \leq k$, p_i es primo, y $e_i > 0$.

Ejemplos

2. Sea $n \in \mathbb{Z}^+$. Determine la cantidad de divisores positivos de n.

   Solución

   Por el teorema fundamental de la aritmética, tenemos que

   $$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

   donde para cada $1 \leq i \leq k$, p_i es primo, y $e_i > 0$.

   Si $m|n$

Ejemplos

2. Sea $n \in \mathbb{Z}^+$. Determine la cantidad de divisores positivos de n.

Solución

Por el teorema fundamental de la aritmética, tenemos que

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

donde para cada $1 \leq i \leq k$, p_i es primo, y $e_i > 0$.

Si $m|n$, entonces

$$m = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

donde $0 \leq f_i \leq e_i$, para todo $1 \leq i \leq k$.

Ejemplos

2. Sea $n \in \mathbb{Z}^+$. Determine la cantidad de divisores positivos de n.

   Solución

   Por el teorema fundamental de la aritmética, tenemos que

   $$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

   donde para cada $1 \leq i \leq k$, p_i es primo, y $e_i > 0$.

   Si $m|n$, entonces

   $$m = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

   donde $0 \leq f_i \leq e_i$, para todo $1 \leq i \leq k$.

   Así por la regla del producto, el número de divisores positivos de n es

   $$(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$$

Ejemplos

2. Sea $n \in \mathbb{Z}^+$. Determine la cantidad de divisores positivos de n.

Solución

Por el teorema fundamental de la aritmética, tenemos que

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

donde para cada $1 \leq i \leq k$, p_i es primo, y $e_i > 0$.

Si $m|n$, entonces

$$m = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

donde $0 \leq f_i \leq e_i$, para todo $1 \leq i \leq k$.

Así por la regla del producto, el número de divisores positivos de n es

$$(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$$

Por ejemplo, del ejemplo anterior tenemos que $546756 = 2^2 \cdot 3 \cdot 7 \cdot 23 \cdot 283$, tiene $(2 + 1)(1 + 1)(1 + 1)(1 + 1)(1 + 1) = 48$ divisores.

Ecuaciones de Diofanto

Definición

Una **ecuación de diofanto o ecuación diofántica** tiene la forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

donde $a_1, a_2, ..., a_n, b$ son enteros y se exige soluciones también enteras.
La ecuación diofántica más simple es la ecuación de dos incógnitas, $ax + by = c$, donde a, b, c son enteros.

Teorema

Una ecuación diofántica de la forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

tiene solución si, y solo si $mcd(a_1, a_2, ..., a_n)$ divide b.

Ecuaciones de Diofanto

Teorema

La ecuación diofántica $ax + by = c$ tiene solución si, y solo si $mcd(a, b)|c$

En este caso la ecuación tiene una infinidad de soluciones.

Ecuaciones de Diofanto

Teorema

La ecuación diofántica $ax + by = c$ tiene solución si, y solo si $mcd(a, b)|c$

En este caso la ecuación tiene una infinidad de soluciones.

La solución general de una ecuación de diofanto de la forma

$$ax + by = c$$

es

$$\begin{cases} x = x_1 + k\dfrac{b}{mcd(a,b)} \\ \\ y = y_1 - k\dfrac{a}{mcd(a,b)} \quad \forall k \in \mathbb{Z} \end{cases}$$

donde x_1 y y_1 son una solución particular de la ecuación.

Ejemplos

1. Calcular las soluciones enteras de la ecuación diofántica

$$66x + 550y = 88$$

Ejemplos

1. Calcular las soluciones enteras de la ecuación diofántica

$$66x + 550y = 88$$

Solución

Ejemplos

1. Calcular las soluciones enteras de la ecuación diofántica

$$66x + 550y = 88$$

Solución

Primeramente veamos que si admite solución entera, calculando el máximo común divisor por el algoritmo de euclides

Ejemplos

1. Calcular las soluciones enteras de la ecuación diofántica

$$66x + 550y = 88$$

Solución

Primeramente veamos que si admite solución entera, calculando el máximo común divisor por el algoritmo de euclides

$$\begin{aligned} 550 &= 8(66) + 22 \\ 66 &= 3(22) + 0 \end{aligned}$$

Ejemplos

1. Calcular las soluciones enteras de la ecuación diofántica

$$66x + 550y = 88$$

Solución

Primeramente veamos que si admite solución entera, calculando el máximo común divisor por el algoritmo de euclides

$$\begin{aligned} 550 &= 8(66) + 22 \\ 66 &= 3(22) + 0 \end{aligned}$$

$mcd(66, 550) = 22$ y $22|88$, entonces la ecuación si admite soluciones enteras.

Ejemplos

1. Calcular las soluciones enteras de la ecuación diofántica

$$66x + 550y = 88$$

Solución

Primeramente veamos que si admite solución entera, calculando el máximo común divisor por el algoritmo de euclides

$$\begin{aligned} 550 &= 8(66) + 22 \\ 66 &= 3(22) + 0 \end{aligned}$$

$mcd(66, 550) = 22$ y $22|88$, entonces la ecuación si admite soluciones enteras.

Ahora bien, calculamos las soluciones particulares, para ello necesitamos escribir el máximo común divisor como combinación lineal de 550 y 66, obteniendo que

$$22 = 550 - 8(66)$$

Ejemplos

Ahora multiplicamos por un número tal que obtengamos una ecuación similar a la ecuación diofántica, en este caso es 4.

Ejemplos

Ahora multiplicamos por un número tal que obtengamos una ecuación similar a la ecuación diofántica, en este caso es 4.

$$\begin{array}{lll} & 4(22) & = 4(550 - 8(66)) \\ \Rightarrow & 88 & = 4(550) - 32(66) \end{array}$$

Ejemplos

Ahora multiplicamos por un número tal que obtengamos una ecuación similar a la ecuación diofántica, en este caso es 4.

$$\begin{aligned} & 4(22) && = 4(550 - 8(66)) \\ \Rightarrow \quad & 88 && = 4(550) - 32(66) \end{aligned}$$

Podemos ver que ya tenemos la solucion particular con $x_1 = -32$ y $y_1 = 4$

Ejemplos

Ahora multiplicamos por un número tal que obtengamos una ecuación similar a la ecuación diofántica, en este caso es 4.

$$\begin{array}{lll} & 4(22) & = 4(550 - 8(66)) \\ \Rightarrow & 88 & = 4(550) - 32(66) \end{array}$$

Podemos ver que ya tenemos la solucion particular con $x_1 = -32$ y $y_1 = 4$, entonces la solución general es

Ejemplos

Ahora multiplicamos por un número tal que obtengamos una ecuación similar a la ecuación diofántica, en este caso es 4.

$$\begin{array}{lll} & 4(22) & = 4(550 - 8(66)) \\ \Rightarrow & 88 & = 4(550) - 32(66) \end{array}$$

Podemos ver que ya tenemos la solucion particular con $x_1 = -32$ y $y_1 = 4$, entonces la solución general es

$$\begin{cases} x = -32 + k\frac{550}{22} \\ y = 4 - k\frac{66}{22} \end{cases}$$

Ejemplos

Ahora multiplicamos por un número tal que obtengamos una ecuación similar a la ecuación diofántica, en este caso es 4.

$$\begin{aligned} & 4(22) && = 4(550 - 8(66)) \\ \Rightarrow \quad & 88 && = 4(550) - 32(66) \end{aligned}$$

Podemos ver que ya tenemos la solucion particular con $x_1 = -32$ y $y_1 = 4$, entonces la solución general es

$$\begin{cases} x = -32 + k\frac{550}{22} \\ y = 4 - k\frac{66}{22} \end{cases} \Rightarrow \begin{cases} x = -32 + 25k \\ y = 4 - 3k \end{cases}$$

Ejemplos

Ahora multiplicamos por un número tal que obtengamos una ecuación similar a la ecuación diofántica, en este caso es 4.

$$\begin{array}{lll} & 4(22) & = 4(550 - 8(66)) \\ \Rightarrow & 88 & = 4(550) - 32(66) \end{array}$$

Podemos ver que ya tenemos la solucion particular con $x_1 = -32$ y $y_1 = 4$, entonces la solución general es

$$\left\{ \begin{array}{l} x = -32 + k\frac{550}{22} \\ y = 4 - k\frac{66}{22} \end{array} \right. \Rightarrow \left\{ \begin{array}{l} x = -32 + 25k \\ y = 4 - 3k \end{array} \right.$$

para todo $k \in \mathbb{Z}$.

Ejemplos

Ahora bien, si el problema nos impone condiciones, como por ejemplo $x \geq 18$ y $y \geq -8$, para la ecuación diofántica

$$66x + 550y = 88$$

Ejemplos

Ahora bien, si el problema nos impone condiciones, como por ejemplo $x \geq 18$ y $y \geq -8$, para la ecuación diofántica

$$66x + 550y = 88$$

ya no podemos concluir la solución general para todo k, lo cuál debemos de encontrar los valores de k para que se cumplan las condiciones, procedemos de la siguiente forma.

Ejemplos

Ahora bien, si el problema nos impone condiciones, como por ejemplo $x \geq 18$ y $y \geq -8$, para la ecuación diofántica

$$66x + 550y = 88$$

ya no podemos concluir la solución general para todo k, lo cuál debemos de encontrar los valores de k para que se cumplan las condiciones, procedemos de la siguiente forma.

- $x \geq 18 \Rightarrow -32 + 25k \geq 18 \Rightarrow k \geq 2$

Ejemplos

Ahora bien, si el problema nos impone condiciones, como por ejemplo $x \geq 18$ y $y \geq -8$, para la ecuación diofántica

$$66x + 550y = 88$$

ya no podemos concluir la solución general para todo k, lo cuál debemos de encontrar los valores de k para que se cumplan las condiciones, procedemos de la siguiente forma.

- $x \geq 18 \Rightarrow -32 + 25k \geq 18 \Rightarrow k \geq 2$
- $y \geq -8 \Rightarrow 4 - 3k \geq -8 \Rightarrow k \leq 4$

Ejemplos

Ahora bien, si el problema nos impone condiciones, como por ejemplo $x \geq 18$ y $y \geq -8$, para la ecuación diofántica

$$66x + 550y = 88$$

ya no podemos concluir la solución general para todo k, lo cuál debemos de encontrar los valores de k para que se cumplan las condiciones, procedemos de la siguiente forma.

- $x \geq 18 \Rightarrow -32 + 25k \geq 18 \Rightarrow k \geq 2$
- $y \geq -8 \Rightarrow 4 - 3k \geq -8 \Rightarrow k \leq 4$

Ahora tomamos la intersección de los dos conjuntos para k teniendo que $2 \leq k \leq 4$

$$\therefore \begin{cases} x = -32 + 25k \\ y = 4 - 3k \end{cases} \quad 2 \leq k \leq 4$$

Ejemplos

2. Una bufanda cuesta 19 rublos, pero el comprador no tiene más que billetes de tres rublos, y la cajera sólo de cinco. ¿Puede en estas condiciones abonarse el importe de la compra, y cómo hacerlo?

Ejemplos

2. Una bufanda cuesta 19 rublos, pero el comprador no tiene más que billetes de tres rublos, y la cajera sólo de cinco. ¿Puede en estas condiciones abonarse el importe de la compra, y cómo hacerlo?

   Solución:

Ejemplos

2. Una bufanda cuesta 19 rublos, pero el comprador no tiene más que billetes de tres rublos, y la cajera sólo de cinco. ¿Puede en estas condiciones abonarse el importe de la compra, y cómo hacerlo?

   Solución:

   El objetivo de este problema se reduce a saber cuántos billetes de tres rublos deben entregarse a la cajera para que ella dé de vuelta con billetes de cinco, cobrando los 19 rublos.

Ejemplos

2. Una bufanda cuesta 19 rublos, pero el comprador no tiene más que billetes de tres rublos, y la cajera sólo de cinco. ¿Puede en estas condiciones abonarse el importe de la compra, y cómo hacerlo?

Solución:

El objetivo de este problema se reduce a saber cuántos billetes de tres rublos deben entregarse a la cajera para que ella dé de vuelta con billetes de cinco, cobrando los 19 rublos.
Entonces las incógnitas son: el número de billetes de tres rublos (x) y el número de billetes de cinco rublos (y). Entonces la ecuación diofántica es

$$3x - 5y = 19$$

Ejemplos

2. Una bufanda cuesta 19 rublos, pero el comprador no tiene más que billetes de tres rublos, y la cajera sólo de cinco. ¿Puede en estas condiciones abonarse el importe de la compra, y cómo hacerlo?

   Solución:

   El objetivo de este problema se reduce a saber cuántos billetes de tres rublos deben entregarse a la cajera para que ella dé de vuelta con billetes de cinco, cobrando los 19 rublos.
   Entonces las incógnitas son: el número de billetes de tres rublos (x) y el número de billetes de cinco rublos (y). Entonces la ecuación diofántica es

   $$3x - 5y = 19$$

   También debemos de considerar que $x > 0$ y $y > 0$ dado que son billetes.

Ejemplos

2. Una bufanda cuesta 19 rublos, pero el comprador no tiene más que billetes de tres rublos, y la cajera sólo de cinco. ¿Puede en estas condiciones abonarse el importe de la compra, y cómo hacerlo?

Solución:

El objetivo de este problema se reduce a saber cuántos billetes de tres rublos deben entregarse a la cajera para que ella dé de vuelta con billetes de cinco, cobrando los 19 rublos.
Entonces las incógnitas son: el número de billetes de tres rublos (x) y el número de billetes de cinco rublos (y). Entonces la ecuación diofántica es

$$3x - 5y = 19$$

También debemos de considerar que $x > 0$ y $y > 0$ dado que son billetes.

Ahora bien, obsevemos que $mcd(3, -5) = mcd(3, 5) = 1$ y $1|19$, entonces la ecuación tiene solución.

Ejemplos

Primeramente calcularemos la solución particular escribiendo $mcd(3, -5)$ como combinación lineal de estos, utilizando el algoritmo de Euclides, de la siguiente forma

$$-5 = -2(3) + 1$$

Ejemplos

Primeramente calcularemos la solución particular escribiendo $mcd(3,-5)$ como combinación lineal de estos, utilizando el algoritmo de Euclides, de la siguiente forma

$$-5 = -2(3) + 1 \Rightarrow 1 = 1(-5) + 2(3)$$

Ejemplos

Primeramente calcularemos la solución particular escribiendo $mcd(3, -5)$ como combinación lineal de estos, utilizando el algoritmo de Euclides, de la siguiente forma

$$-5 = -2(3) + 1 \Rightarrow 1 = 1(-5) + 2(3)$$

Multiplicamos por 19 para tener una ecuación similar a la ecuación anterior

$$19 = 19(1(-5) + 2(3)) = 19(-5) + 38(3)$$

Ejemplos

Primeramente calcularemos la solución particular escribiendo $mcd(3, -5)$ como combinación lineal de estos, utilizando el algoritmo de Euclides, de la siguiente forma

$$-5 = -2(3) + 1 \Rightarrow 1 = 1(-5) + 2(3)$$

Multiplicamos por 19 para tener una ecuación similar a la ecuación anterior

$$19 = 19(1(-5) + 2(3)) = 19(-5) + 38(3)$$

entonces $x_1 = 38$ y $y_1 = 19$

Ejemplos

La solución general está dada por

$$\begin{cases} x = 38 - 5k \\ y = 19 - 3k \end{cases}$$

Ejemplos

La solución general está dada por

$$\begin{cases} x = 38 - 5k \\ y = 19 - 3k \end{cases}$$

pero no podemos decir que para todo $k \in \mathbb{Z}$

Ejemplos

La solución general está dada por

$$\begin{cases} x = 38 - 5k \\ y = 19 - 3k \end{cases}$$

pero no podemos decir que para todo $k \in \mathbb{Z}$. Recordemos las condiciones que $x > 0$ y $y > 0$, entonces procedemos a encontrar los valores de k que cumplan las condiciones.

Ejemplos

La solución general está dada por

$$\begin{cases} x = 38 - 5k \\ y = 19 - 3k \end{cases}$$

pero no podemos decir que para todo $k \in \mathbb{Z}$. Recordemos las condiciones que $x > 0$ y $y > 0$, entonces procedemos a encontrar los valores de k que cumplan las condiciones.

- $x > 0 \Rightarrow 38 - 5k > 0 \Rightarrow k < \frac{38}{5} \Rightarrow k \leq 7$

Ejemplos

La solución general está dada por

$$\begin{cases} x = 38 - 5k \\ y = 19 - 3k \end{cases}$$

pero no podemos decir que para todo $k \in \mathbb{Z}$. Recordemos las condiciones que $x > 0$ y $y > 0$, entonces procedemos a encontrar los valores de k que cumplan las condiciones.

- $x > 0 \Rightarrow 38 - 5k > 0 \Rightarrow k < \frac{38}{5} \Rightarrow k \leq 7$
- $y > 0 \Rightarrow 19 - 3k > 0 \Rightarrow k < \frac{19}{3} \Rightarrow k \leq 6$

Ejemplos

La solución general está dada por

$$\begin{cases} x = 38 - 5k \\ y = 19 - 3k \end{cases}$$

pero no podemos decir que para todo $k \in \mathbb{Z}$. Recordemos las condiciones que $x > 0$ y $y > 0$, entonces procedemos a encontrar los valores de k que cumplan las condiciones.

- $x > 0 \Rightarrow 38 - 5k > 0 \Rightarrow k < \frac{38}{5} \Rightarrow k \leq 7$
- $y > 0 \Rightarrow 19 - 3k > 0 \Rightarrow k < \frac{19}{3} \Rightarrow k \leq 6$

Tomamos la intersección de los dos conjuntos para k, teniendo que $k \leq 6$.

$$\therefore \begin{cases} x = 38 - 5k \\ y = 19 - 3k \end{cases} \quad k \leq 6$$

Ejercicios de práctica

1. Demuestre los incisos restantes del primer teorema.
2. Encuentre la solución general de la ecuación de diofanto

$$4x + 6y = 20$$