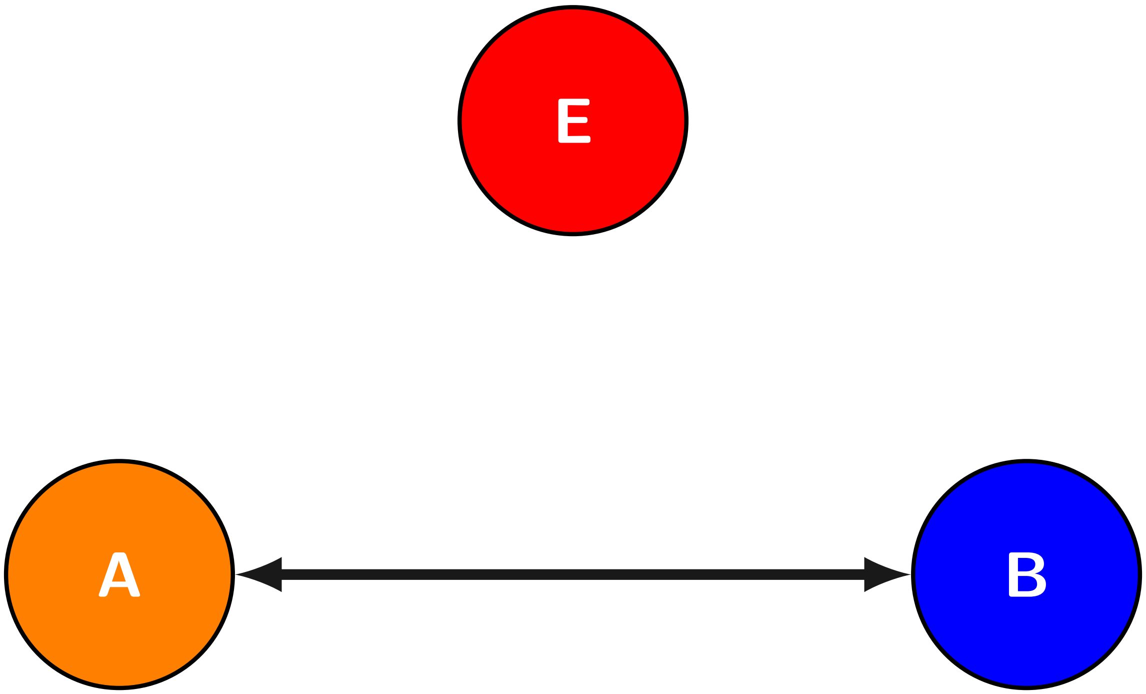
Teoría de números - IIC1253

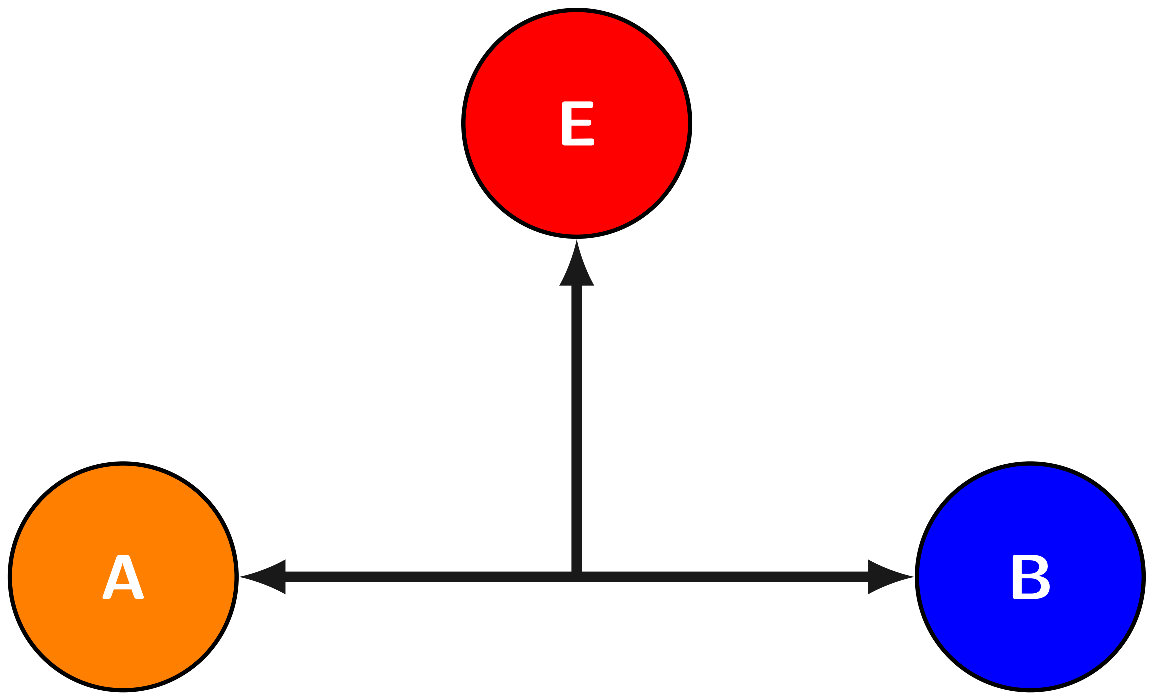
Marcelo Arenas

Motivación: comunicación segura

Motivación: comunicación segura



Motivación: comunicación segura



División Euclidiana

División Euclidiana

Dados números $a, b \in \mathbb{Z}$, utilizamos la notación $a|b$ para indicar que a divide a b.

División Euclidiana

Dados números $a, b \in \mathbb{Z}$, utilizamos la notación $a|b$ para indicar que a divide a b.

- Vale decir, existe $k \in \mathbb{Z}$ tal que $a \cdot k = b$.

División Euclidiana

Dados números $a, b \in \mathbb{Z}$, utilizamos la notación $a|b$ para indicar que a divide a b.

- Vale decir, existe $k \in \mathbb{Z}$ tal que $a \cdot k = b$.

Proposición

1. *Si $n|a$, entonces $n|(a \cdot b)$.*
2. *Si $n|a$ y $n|b$, entonces $n|(a+b)$ y $n|(a-b)$.*

División Euclidiana

Dados números $a, b \in \mathbb{Z}$, utilizamos la notación $a|b$ para indicar que a divide a b.

- Vale decir, existe $k \in \mathbb{Z}$ tal que $a \cdot k = b$.

Proposición

1. *Si $n|a$, entonces $n|(a \cdot b)$.*
2. *Si $n|a$ y $n|b$, entonces $n|(a + b)$ y $n|(a - b)$.*

Ejercicio

Demuestre la proposición.

División Euclidiana

Teorema

Para cada $a, b \in \mathbb{Z}$ *tal que* $b \neq 0$, *existen números únicos* $p, q \in \mathbb{Z}$ *tales que:*

$$a = p \cdot b + q \quad y \quad 0 \leq q < |b|.$$

La demostración del teorema

Sea $S = \{a - k \cdot b \mid k \in \mathbb{Z} \text{ y } a - k \cdot b \geq 0\}$.

La demostración del teorema

Sea $S = \{a - k \cdot b \mid k \in \mathbb{Z} \text{ y } a - k \cdot b \geq 0\}$.

- Note que $S \subseteq \mathbb{N}$.

La demostración del teorema

Sea $S = \{a - k \cdot b \mid k \in \mathbb{Z} \text{ y } a - k \cdot b \geq 0\}$.

- Note que $S \subseteq \mathbb{N}$.

Vamos a demostrar que $S \neq \emptyset$.

La demostración del teorema

Sea $S = \{a - k \cdot b \mid k \in \mathbb{Z} \text{ y } a - k \cdot b \geq 0\}$.

- Note que $S \subseteq \mathbb{N}$.

Vamos a demostrar que $S \neq \emptyset$.

- Suponga que $a \geq 0$. Entonces para $k = 0$ se tiene que $a - k \cdot b = a \geq 0$. Concluimos que $a \in S$.

La demostración del teorema

Sea $S = \{a - k \cdot b \mid k \in \mathbb{Z} \text{ y } a - k \cdot b \geq 0\}$.

- Note que $S \subseteq \mathbb{N}$.

Vamos a demostrar que $S \neq \emptyset$.

- Suponga que $a \geq 0$. Entonces para $k = 0$ se tiene que $a - k \cdot b = a \geq 0$. Concluimos que $a \in S$.

- Suponga que $a < 0$ y $b \geq 1$.

La demostración del teorema

Sea $S = \{a - k \cdot b \mid k \in \mathbb{Z} \text{ y } a - k \cdot b \geq 0\}$.

- Note que $S \subseteq \mathbb{N}$.

Vamos a demostrar que $S \neq \emptyset$.

- Suponga que $a \geq 0$. Entonces para $k = 0$ se tiene que $a - k \cdot b = a \geq 0$. Concluimos que $a \in S$.

- Suponga que $a < 0$ y $b \geq 1$.

  Entonces para $k = a$ se tiene que $a - k \cdot b = a - a \cdot b = a \cdot (1 - b)$.

La demostración del teorema

Sea $S = \{a - k \cdot b \mid k \in \mathbb{Z} \text{ y } a - k \cdot b \geq 0\}$.

- Note que $S \subseteq \mathbb{N}$.

Vamos a demostrar que $S \neq \emptyset$.

- Suponga que $a \geq 0$. Entonces para $k = 0$ se tiene que $a - k \cdot b = a \geq 0$. Concluimos que $a \in S$.

- Suponga que $a < 0$ y $b \geq 1$.

  Entonces para $k = a$ se tiene que $a - k \cdot b = a - a \cdot b = a \cdot (1 - b)$.

  Dado que $b \geq 1$, se tiene que $1 - b \leq 0$. Así, dado que $a < 0$, concluimos que $a \cdot (1 - b) \geq 0$, y tenemos que $a - a \cdot b \in S$.

La demostración del teorema

- Suponga que $a < 0$ y $b \leq -1$.

La demostración del teorema

- Suponga que $a < 0$ y $b \leq -1$.

  Entonces para $k = -a$ se tiene que $a - k \cdot b = a + a \cdot b = a \cdot (1 + b)$.

La demostración del teorema

- Suponga que $a < 0$ y $b \leq -1$.

  Entonces para $k = -a$ se tiene que $a - k \cdot b = a + a \cdot b = a \cdot (1 + b)$.

  Dado que $b \leq -1$, se tiene que $1 + b \leq 0$. Así, dado que $a < 0$, concluimos que $a \cdot (1 + b) \geq 0$, y tenemos que $a + a \cdot b \in S$.

La demostración del teorema

- Suponga que $a < 0$ y $b \leq -1$.

  Entonces para $k = -a$ se tiene que $a - k \cdot b = a + a \cdot b = a \cdot (1 + b)$.

  Dado que $b \leq -1$, se tiene que $1 + b \leq 0$. Así, dado que $a < 0$, concluimos que $a \cdot (1 + b) \geq 0$, y tenemos que $a + a \cdot b \in S$.

Dado que $S \neq \emptyset$ y $S \subseteq \mathbb{N}$, sabemos por el principio del mínimo que S tiene un menor elemento q.

La demostración del teorema

- Suponga que $a < 0$ y $b \leq -1$.

  Entonces para $k = -a$ se tiene que $a - k \cdot b = a + a \cdot b = a \cdot (1 + b)$.

  Dado que $b \leq -1$, se tiene que $1 + b \leq 0$. Así, dado que $a < 0$, concluimos que $a \cdot (1 + b) \geq 0$, y tenemos que $a + a \cdot b \in S$.

Dado que $S \neq \emptyset$ y $S \subseteq \mathbb{N}$, sabemos por el principio del mínimo que S tiene un menor elemento q.

- Note que $q = a - p \cdot b$ para $p \in \mathbb{Z}$.

La demostración del teorema

Vamos a demostrar que $0 \leq q < |b|$.

La demostración del teorema

Vamos a demostrar que $0 \leq q < |b|$.

- Sabemos que $q \geq 0$.

La demostración del teorema

Vamos a demostrar que $0 \leq q < |b|$.

- Sabemos que $q \geq 0$.

Por contradicción, suponga que $q \geq |b|$.

La demostración del teorema

Vamos a demostrar que $0 \leq q < |b|$.

- Sabemos que $q \geq 0$.

Por contradicción, suponga que $q \geq |b|$.

A partir del supuesto de que $q \geq |b|$ vamos a demostrar que q no es el menor elemento de S, lo cual nos lleva a una contradicción.

La demostración del teorema

Vamos a demostrar que $0 \leq q < |b|$.

- Sabemos que $q \geq 0$.

Por contradicción, suponga que $q \geq |b|$.

A partir del supuesto de que $q \geq |b|$ vamos a demostrar que q no es el menor elemento de S, lo cual nos lleva a una contradicción.

- Suponga que $b > 0$. Tenemos entonces que $q \geq b$.

La demostración del teorema

Vamos a demostrar que $0 \leq q < |b|$.

- Sabemos que $q \geq 0$.

Por contradicción, suponga que $q \geq |b|$.

A partir del supuesto de que $q \geq |b|$ vamos a demostrar que q no es el menor elemento de S, lo cual nos lleva a una contradicción.

- Suponga que $b > 0$. Tenemos entonces que $q \geq b$.

  Tenemos que $q - b \geq 0$ y $q - b = a - p \cdot b - b = a - (p+1) \cdot b$.

La demostración del teorema

Vamos a demostrar que $0 \leq q < |b|$.

- Sabemos que $q \geq 0$.

Por contradicción, suponga que $q \geq |b|$.

A partir del supuesto de que $q \geq |b|$ vamos a demostrar que q no es el menor elemento de S, lo cual nos lleva a una contradicción.

- Suponga que $b > 0$. Tenemos entonces que $q \geq b$.

  Tenemos que $q - b \geq 0$ y $q - b = a - p \cdot b - b = a - (p + 1) \cdot b$.

  Por lo tanto q no es el menor elemento de S puesto que $q - b \in S$ y $q - b < q$.

La demostración del teorema

- Suponga que $b < 0$. Tenemos entonces que $q \geq -b$.

La demostración del teorema

- Suponga que $b < 0$. Tenemos entonces que $q \geq -b$.

  Tenemos que $q + b \geq 0$ y $q + b = a - p \cdot b + b = a - (p - 1) \cdot b$.

La demostración del teorema

- Suponga que $b < 0$. Tenemos entonces que $q \geq -b$.

  Tenemos que $q + b \geq 0$ y $q + b = a - p \cdot b + b = a - (p - 1) \cdot b$.

  Por lo tanto q no es el menor elemento de S puesto que $q + b \in S$ y $q + b < q$.

La demostración del teorema

- Suponga que $b < 0$. Tenemos entonces que $q \geq -b$.

  Tenemos que $q + b \geq 0$ y $q + b = a - p \cdot b + b = a - (p-1) \cdot b$.

  Por lo tanto q no es el menor elemento de S puesto que $q + b \in S$ y $q + b < q$.

Demostramos entonces que existen $p, q \in \mathbb{Z}$ tales que:

$$a = p \cdot b + q \quad \text{y} \quad 0 \leq q < |b|$$

La demostración del teorema

- Suponga que $b < 0$. Tenemos entonces que $q \geq -b$.

  Tenemos que $q + b \geq 0$ y $q + b = a - p \cdot b + b = a - (p - 1) \cdot b$.

  Por lo tanto q no es el menor elemento de S puesto que $q + b \in S$ y $q + b < q$.

Demostramos entonces que existen $p, q \in \mathbb{Z}$ tales que:

$$a = p \cdot b + q \quad \text{y} \quad 0 \leq q < |b|$$

Nos queda demostrar que los números p, q que satisfacen la condición anterior son únicos.

La demostración del teorema

- Suponga que $b < 0$. Tenemos entonces que $q \geq -b$.

  Tenemos que $q + b \geq 0$ y $q + b = a - p \cdot b + b = a - (p-1) \cdot b$.

  Por lo tanto q no es el menor elemento de S puesto que $q + b \in S$ y $q + b < q$.

Demostramos entonces que existen $p, q \in \mathbb{Z}$ tales que:

$$a = p \cdot b + q \quad \text{y} \quad 0 \leq q < |b|$$

Nos queda demostrar que los números p, q que satisfacen la condición anterior son únicos.

- Suponga que existen $r, s \in \mathbb{Z}$ tales que $a = r \cdot b + s$ y $0 \leq s < |b|$.

La demostración del teorema

Tenemos que $p \cdot b + q = r \cdot b + s$.

La demostración del teorema

Tenemos que $p \cdot b + q = r \cdot b + s$.

- Por lo tanto $(p - r) \cdot b = s - q$.

La demostración del teorema

Tenemos que $p \cdot b + q = r \cdot b + s$.

- Por lo tanto $(p - r) \cdot b = s - q$.

Tenemos entonces que $b | (s - q)$.

La demostración del teorema

Tenemos que $p \cdot b + q = r \cdot b + s$.

- Por lo tanto $(p - r) \cdot b = s - q$.

Tenemos entonces que $b | (s - q)$.

Dado que $0 \leq q < |b|$, tenemos que $-|b| < -q \leq 0$.

La demostración del teorema

Tenemos que $p \cdot b + q = r \cdot b + s$.

- Por lo tanto $(p - r) \cdot b = s - q$.

Tenemos entonces que $b | (s - q)$.

Dado que $0 \leq q < |b|$, tenemos que $-|b| < -q \leq 0$.

- Por lo tanto $-|b| < s - q < |b|$, puesto que $0 \leq s < |b|$.

La demostración del teorema

Dado que $b|(s-q)$ y $-|b| < s-q < |b|$, concluimos que $s-q=0$.

La demostración del teorema

Dado que $b|(s-q)$ y $-|b| < s-q < |b|$, concluimos que $s-q=0$.

Así, dado que $(p-r)\cdot b = s-q$ y $b \neq 0$, concluimos que $p-r=0$.

La demostración del teorema

Dado que $b|(s-q)$ y $-|b| < s-q < |b|$, concluimos que $s-q=0$.

Así, dado que $(p-r)\cdot b = s-q$ y $b \neq 0$, concluimos que $p-r=0$.

Concluimos que $r=p$ y $s=q$.

La demostración del teorema

Dado que $b|(s-q)$ y $-|b| < s-q < |b|$, concluimos que $s-q=0$.

Así, dado que $(p-r)\cdot b = s-q$ y $b \neq 0$, concluimos que $p-r=0$.

Concluimos que $r=p$ y $s=q$.

- Por lo tanto, existen números únicos p, q tales que $a = p\cdot b + q$ y $0 \leq q < |b|$. $\square$

El resto de la división

La definición del resto

Sean $a, b \in \mathbb{Z}$ tales que $b \neq 0$.

La definición del resto

Sean $a, b \in \mathbb{Z}$ tales que $b \neq 0$.

Definición

El resto de la división de a en b se define como el único número $q \in \mathbb{Z}$ tal que $a = p \cdot b + q$, para $p \in \mathbb{Z}$, y $0 \leq q < |b|$.

La definición del resto

Sean $a, b \in \mathbb{Z}$ tales que $b \neq 0$.

Definición

El resto de la división de a en b se define como el único número $q \in \mathbb{Z}$ *tal que* $a = p \cdot b + q$, *para* $p \in \mathbb{Z}$, *y* $0 \leq q < |b|$.

Usamos la notación $a \bmod b$ para el resto de la división entre a y b.

- El resto también se denota como módulo.

La definición del resto: ejercicios

Calcule los siguientes restos:

$$
\begin{aligned}
10 \bmod 2 &= \\
15 \bmod 2 &= \\
20 \bmod 3 &= \\
15 \bmod 3 &= \\
-15 \bmod 3 &= \\
-20 \bmod 3 &= \\
10 \bmod -3 &= \\
33 \bmod -7 &=
\end{aligned}
$$

La definición del resto: ejercicios

Calcule los siguientes restos:

$$\begin{aligned}
10 \bmod 2 &= 0 \\
15 \bmod 2 &= \\
20 \bmod 3 &= \\
15 \bmod 3 &= \\
-15 \bmod 3 &= \\
-20 \bmod 3 &= \\
10 \bmod -3 &= \\
33 \bmod -7 &=
\end{aligned}$$

La definición del resto: ejercicios

Calcule los siguientes restos:

$$
\begin{aligned}
10 \bmod 2 &= 0 \\
15 \bmod 2 &= 1 \\
20 \bmod 3 &= \\
15 \bmod 3 &= \\
-15 \bmod 3 &= \\
-20 \bmod 3 &= \\
10 \bmod -3 &= \\
33 \bmod -7 &=
\end{aligned}
$$

La definición del resto: ejercicios

Calcule los siguientes restos:

$$
\begin{aligned}
10 \bmod 2 &= 0 \\
15 \bmod 2 &= 1 \\
20 \bmod 3 &= 2 \\
15 \bmod 3 &= \\
-15 \bmod 3 &= \\
-20 \bmod 3 &= \\
10 \bmod -3 &= \\
33 \bmod -7 &=
\end{aligned}
$$

La definición del resto: ejercicios

Calcule los siguientes restos:

$$\begin{aligned}
10 \bmod 2 &= 0 \\
15 \bmod 2 &= 1 \\
20 \bmod 3 &= 2 \\
15 \bmod 3 &= 0 \\
-15 \bmod 3 &= \\
-20 \bmod 3 &= \\
10 \bmod -3 &= \\
33 \bmod -7 &=
\end{aligned}$$

La definición del resto: ejercicios

Calcule los siguientes restos:

$$
\begin{aligned}
10 \bmod 2 &= 0 \\
15 \bmod 2 &= 1 \\
20 \bmod 3 &= 2 \\
15 \bmod 3 &= 0 \\
-15 \bmod 3 &= 0 \\
-20 \bmod 3 &= \\
10 \bmod -3 &= \\
33 \bmod -7 &=
\end{aligned}
$$

La definición del resto: ejercicios

Calcule los siguientes restos:

$$
\begin{aligned}
10 \bmod 2 &= 0 \\
15 \bmod 2 &= 1 \\
20 \bmod 3 &= 2 \\
15 \bmod 3 &= 0 \\
-15 \bmod 3 &= 0 \\
-20 \bmod 3 &= 1 \\
10 \bmod -3 &= \\
33 \bmod -7 &=
\end{aligned}
$$

La definición del resto: ejercicios

Calcule los siguientes restos:

$$\begin{aligned}
10 \bmod 2 &= 0\\
15 \bmod 2 &= 1\\
20 \bmod 3 &= 2\\
15 \bmod 3 &= 0\\
-15 \bmod 3 &= 0\\
-20 \bmod 3 &= 1\\
10 \bmod -3 &= 1\\
33 \bmod -7 &=
\end{aligned}$$

La definición del resto: ejercicios

Calcule los siguientes restos:

$$\begin{aligned}
10 \bmod 2 &= 0 \\
15 \bmod 2 &= 1 \\
20 \bmod 3 &= 2 \\
15 \bmod 3 &= 0 \\
-15 \bmod 3 &= 0 \\
-20 \bmod 3 &= 1 \\
10 \bmod -3 &= 1 \\
33 \bmod -7 &= 5
\end{aligned}$$

Aritmética modular

Aritmética modular

Definición

Sea $n \in \mathbb{Z}$. *Para cada* $a, b \in \mathbb{Z}$:

$$a \equiv_n b \quad \text{si y sólo si} \quad n | (b - a).$$

Aritmética modular

Definición

Sea $n \in \mathbb{Z}$. *Para cada* $a, b \in \mathbb{Z}$*:*

$$a \equiv_n b \quad \text{si y sólo si} \quad n \mid (b - a).$$

Ya vimos que $\equiv_n$ es una relación de equivalencia.

Aritmética modular

Definición

Sea $n \in \mathbb{Z}$. Para cada $a, b \in \mathbb{Z}$:

$$a \equiv_n b \quad \textit{si y sólo si} \quad n | (b - a).$$

Ya vimos que $\equiv_n$ es una relación de equivalencia.

- En particular, tenemos que $n|(b-a)$ si y sólo si $n|(a-b)$.

Aritmética modular

Definición

Sea $n \in \mathbb{Z}$. Para cada $a, b \in \mathbb{Z}$:

$$a \equiv_n b \quad \textit{si y sólo si} \quad n | (b - a).$$

Ya vimos que $\equiv_n$ es una relación de equivalencia.

- En particular, tenemos que $n|(b-a)$ si y sólo si $n|(a-b)$.

Vamos a estudiar otras propiedades fundamentales de $\equiv_n$.

Aritmética modular: propiedades básicas

Proposición

$a \equiv_n b$ *si y sólo si* $a \bmod n = b \bmod n$.

Aritmética modular: propiedades básicas

Proposición

$a \equiv_n b$ si y sólo si $a \bmod n = b \bmod n$.

Demostración: ($\Leftarrow$) Sabemos que:

$$\begin{array}{rcl} a & = & \alpha \cdot n + \beta \qquad 0 \leq \beta < |n| \\ b & = & \gamma \cdot n + \delta \qquad 0 \leq \delta < |n| \end{array}$$

Aritmética modular: propiedades básicas

Proposición

$a \equiv_n b$ si y sólo si $a \bmod n = b \bmod n$.

Demostración: ($\Leftarrow$) Sabemos que:

$$\begin{array}{rclcl} a & = & \alpha \cdot n + \beta & & 0 \leq \beta < |n| \\ b & = & \gamma \cdot n + \delta & & 0 \leq \delta < |n| \end{array}$$

Por hipótesis: $\beta = \delta$.

Aritmética modular: propiedades básicas

Proposición

$a \equiv_n b$ si y sólo si $a \bmod n = b \bmod n$.

Demostración: ($\Leftarrow$) Sabemos que:

$$\begin{array}{rclcl} a & = & \alpha \cdot n + \beta & & 0 \leq \beta < |n| \\ b & = & \gamma \cdot n + \delta & & 0 \leq \delta < |n| \end{array}$$

Por hipótesis: $\beta = \delta$.

- Puesto que $a \bmod n = \beta$ y $b \bmod n = \delta$.

Aritmética modular: propiedades básicas

Proposición

$a \equiv_n b$ si y sólo si $a \bmod n = b \bmod n$.

Demostración: ($\Leftarrow$) Sabemos que:

$$\begin{array}{lcll} a & = & \alpha \cdot n + \beta & \quad 0 \leq \beta < |n| \\ b & = & \gamma \cdot n + \delta & \quad 0 \leq \delta < |n| \end{array}$$

Por hipótesis: $\beta = \delta$.

- Puesto que $a \bmod n = \beta$ y $b \bmod n = \delta$.

Tenemos que: $(b - a) = (\gamma - \alpha) \cdot n$.

Aritmética modular: propiedades básicas

Proposición

$a \equiv_n b$ si y sólo si $a \bmod n = b \bmod n$.

Demostración: ($\Leftarrow$) Sabemos que:

$$\begin{array}{rcl} a & = & \alpha \cdot n + \beta \qquad 0 \leq \beta < |n| \\ b & = & \gamma \cdot n + \delta \qquad 0 \leq \delta < |n| \end{array}$$

Por hipótesis: $\beta = \delta$.

- Puesto que $a \bmod n = \beta$ y $b \bmod n = \delta$.

Tenemos que: $(b - a) = (\gamma - \alpha) \cdot n$.

- Por lo tanto: $n|(b - a)$, de lo cual se concluye que $a \equiv_n b$.

Aritmética modular: propiedades básicas

($\Rightarrow$) Suponga que $a \bmod n \neq b \bmod n$.

Aritmética modular: propiedades básicas

($\Rightarrow$) Suponga que $a \bmod n \neq b \bmod n$.

- Tenemos que $\beta \neq \delta$ en las ecuaciones de la parte ($\Leftarrow$).

Aritmética modular: propiedades básicas

($\Rightarrow$) Suponga que $a \bmod n \neq b \bmod n$.

- Tenemos que $\beta \neq \delta$ en las ecuaciones de la parte ($\Leftarrow$).

Sin perdida de generalidad suponemos que $\beta < \delta$.

Aritmética modular: propiedades básicas

($\Rightarrow$) Suponga que $a \bmod n \neq b \bmod n$.

- Tenemos que $\beta \neq \delta$ en las ecuaciones de la parte ($\Leftarrow$).

Sin perdida de generalidad suponemos que $\beta < \delta$.

Se tiene que:

$$b - a \quad = \quad (\gamma - \alpha) \cdot n + (\delta - \beta)$$

Aritmética modular: propiedades básicas

($\Rightarrow$) Suponga que $a \bmod n \neq b \bmod n$.

- Tenemos que $\beta \neq \delta$ en las ecuaciones de la parte ($\Leftarrow$).

Sin perdida de generalidad suponemos que $\beta < \delta$.

Se tiene que:

$$b - a \quad = \quad (\gamma - \alpha) \cdot n + (\delta - \beta)$$

Pero $1 \leq (\delta - \beta) \leq \delta < |n|$.

Aritmética modular: propiedades básicas

($\Rightarrow$) Suponga que $a \bmod n \neq b \bmod n$.

- Tenemos que $\beta \neq \delta$ en las ecuaciones de la parte ($\Leftarrow$).

Sin perdida de generalidad suponemos que $\beta < \delta$.

Se tiene que:

$$b - a \quad = \quad (\gamma - \alpha) \cdot n + (\delta - \beta)$$

Pero $1 \leq (\delta - \beta) \leq \delta < |n|$.

- Por lo tanto $n \not| (b - a)$, de lo cual se concluye que $a \not\equiv_n b$.

$\square$

Aritmética modular: propiedades básicas

Corolario

$a \equiv_n (a \, mod \, n)$.

Aritmética modular: propiedades básicas

Corolario

$a \equiv_n (a \, mod \, n)$.

Ejercicio

Demuestre el corolario

Aritmética modular: propiedades básicas

Proposición

Si $a \equiv_n b$ y $c \equiv_n d$, entonces:

$$\begin{aligned} (a+c) &\equiv_n (b+d) \\ (a \cdot c) &\equiv_n (b \cdot d) \end{aligned}$$

Aritmética modular: propiedades básicas

Proposición

Si $a \equiv_n b$ *y* $c \equiv_n d$*, entonces:*

$$\begin{aligned} (a + c) &\equiv_n (b + d) \\ (a \cdot c) &\equiv_n (b \cdot d) \end{aligned}$$

Demostración: Tenemos que $n|(b - a)$ y $n|(d - c)$.

Aritmética modular: propiedades básicas

Proposición

Si $a \equiv_n b$ *y* $c \equiv_n d$*, entonces:*

$$\begin{aligned}(a+c) &\equiv_n (b+d)\\ (a\cdot c) &\equiv_n (b\cdot d)\end{aligned}$$

Demostración: Tenemos que $n|(b-a)$ y $n|(d-c)$.

- Por lo tanto $n\cdot k = b-a$ y $n\cdot \ell = d-c$, para $k,\ell \in \mathbb{Z}$.

Aritmética modular: propiedades básicas

Proposición

Si $a \equiv_n b$ *y* $c \equiv_n d$, *entonces:*

$$\begin{aligned} (a+c) &\equiv_n (b+d) \\ (a \cdot c) &\equiv_n (b \cdot d) \end{aligned}$$

Demostración: Tenemos que $n|(b-a)$ y $n|(d-c)$.

- Por lo tanto $n \cdot k = b - a$ y $n \cdot \ell = d - c$, para $k, \ell \in \mathbb{Z}$.

Concluimos que $n \cdot (k + \ell) = b + d - (a + c)$.

Aritmética modular: propiedades básicas

Proposición

Si $a \equiv_n b$ y $c \equiv_n d$, entonces:

$$\begin{aligned} (a+c) &\equiv_n (b+d) \\ (a \cdot c) &\equiv_n (b \cdot d) \end{aligned}$$

Demostración: Tenemos que $n|(b-a)$ y $n|(d-c)$.

- Por lo tanto $n \cdot k = b - a$ y $n \cdot \ell = d - c$, para $k, \ell \in \mathbb{Z}$.

Concluimos que $n \cdot (k + \ell) = b + d - (a + c)$.

- Por lo tanto $a + c \equiv_n b + d$.

Aritmética modular: propiedades básicas

Reordenando las identidades anteriores obtenemos que $n \cdot k + a = b$ y $n \cdot \ell + c = d$.

Aritmética modular: propiedades básicas

Reordenando las identidades anteriores obtenemos que $n \cdot k + a = b$ y $n \cdot \ell + c = d$.

Por lo tanto $(n \cdot k + a) \cdot (n \cdot \ell + c) = b \cdot d$.

Aritmética modular: propiedades básicas

Reordenando las identidades anteriores obtenemos que $n \cdot k + a = b$ y $n \cdot \ell + c = d$.

Por lo tanto $(n \cdot k + a) \cdot (n \cdot \ell + c) = b \cdot d$.

- De esto concluimos que $n^2 \cdot k \cdot \ell + n \cdot k \cdot c + n \cdot \ell \cdot a + a \cdot c = b \cdot d$.

Aritmética modular: propiedades básicas

Reordenando las identidades anteriores obtenemos que $n \cdot k + a = b$ y $n \cdot \ell + c = d$.

Por lo tanto $(n \cdot k + a) \cdot (n \cdot \ell + c) = b \cdot d$.

- De esto concluimos que $n^2 \cdot k \cdot \ell + n \cdot k \cdot c + n \cdot \ell \cdot a + a \cdot c = b \cdot d$.

Se deduce que $n \cdot (n \cdot k \cdot \ell + k \cdot c + \ell \cdot a) = b \cdot d - a \cdot c$.

Aritmética modular: propiedades básicas

Reordenando las identidades anteriores obtenemos que $n \cdot k + a = b$ y $n \cdot \ell + c = d$.

Por lo tanto $(n \cdot k + a) \cdot (n \cdot \ell + c) = b \cdot d$.

- De esto concluimos que $n^2 \cdot k \cdot \ell + n \cdot k \cdot c + n \cdot \ell \cdot a + a \cdot c = b \cdot d$.

Se deduce que $n \cdot (n \cdot k \cdot \ell + k \cdot c + \ell \cdot a) = b \cdot d - a \cdot c$.

- Por lo tanto $a \cdot c \equiv_n b \cdot d$.

Aritmética modular: propiedades básicas

Corolario

$$
\begin{aligned}
(a + b) \, mod \, n &= (a \, mod \, n + b) \, mod \, n \\
(a \cdot b) \, mod \, n &= (a \, mod \, n \cdot b) \, mod \, n
\end{aligned}
$$

Aritmética modular: propiedades básicas

Corolario

$$
\begin{aligned}
(a + b) \, mod \, n &= (a \, mod \, n + b) \, mod \, n \\
(a \cdot b) \, mod \, n &= (a \, mod \, n \cdot b) \, mod \, n
\end{aligned}
$$

Ejercicio

Demuestre el corolario.

Ejercicios

1. Demuestre que un número $n \in \mathbb{N}$ es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

Ejercicios

1. Demuestre que un número $n \in \mathbb{N}$ es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

2. De reglas de división para los números 4 y 8.

Ejercicios

1. Demuestre que un número $n \in \mathbb{N}$ es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

2. De reglas de división para los números 4 y 8.

3. Calcule $1000^{1000^{1000}} \bmod 17$.
   - Note que el número $1000^{1000^{1000}}$ tiene más dígitos que el número estimado de electrones en el universo observable.

Máximo común divisor y el algoritmo extendido de Euclides

Máximo común divisor

Sea $\mathrm{MCD}(a, b)$ el máximo común divisor de los números a y b.

Máximo común divisor

Sea $\mathrm{MCD}(a, b)$ el máximo común divisor de los números a y b.

- Vale decir, el máximo número $k \in \mathbb{Z}$ tal que $k|a$ y $k|b$.

Máximo común divisor

Sea $\mathrm{MCD}(a, b)$ el máximo común divisor de los números a y b.

- Vale decir, el máximo número $k \in \mathbb{Z}$ tal que $k|a$ y $k|b$.

Ejemplo

Tenemos que:

$$\begin{aligned}
\mathrm{MCD}(10, 18) &= \\
\mathrm{MCD}(18, 24) &= \\
\mathrm{MCD}(15, 17) &= \\
\mathrm{MCD}(0, 17) &= \\
\mathrm{MCD}(-10, 18) &= \\
\mathrm{MCD}(-10, -18) &=
\end{aligned}$$

Máximo común divisor

Sea $\mathrm{MCD}(a, b)$ el máximo común divisor de los números a y b.

- Vale decir, el máximo número $k \in \mathbb{Z}$ tal que $k|a$ y $k|b$.

Ejemplo

Tenemos que:

$$\begin{aligned}
\mathrm{MCD}(10, 18) &= 2 \\
\mathrm{MCD}(18, 24) &= \\
\mathrm{MCD}(15, 17) &= \\
\mathrm{MCD}(0, 17) &= \\
\mathrm{MCD}(-10, 18) &= \\
\mathrm{MCD}(-10, -18) &=
\end{aligned}$$

Máximo común divisor

Sea $\text{MCD}(a, b)$ el máximo común divisor de los números a y b.

- Vale decir, el máximo número $k \in \mathbb{Z}$ tal que $k|a$ y $k|b$.

Ejemplo

Tenemos que:

$$\begin{aligned}
\text{MCD}(10, 18) &= 2 \\
\text{MCD}(18, 24) &= 6 \\
\text{MCD}(15, 17) &= \\
\text{MCD}(0, 17) &= \\
\text{MCD}(-10, 18) &= \\
\text{MCD}(-10, -18) &=
\end{aligned}$$

Máximo común divisor

Sea $\mathrm{MCD}(a, b)$ el máximo común divisor de los números a y b.

- Vale decir, el máximo número $k \in \mathbb{Z}$ tal que $k|a$ y $k|b$.

Ejemplo

Tenemos que:

$$\begin{aligned}
\mathrm{MCD}(10, 18) &= 2 \\
\mathrm{MCD}(18, 24) &= 6 \\
\mathrm{MCD}(15, 17) &= 1 \\
\mathrm{MCD}(0, 17) &= \\
\mathrm{MCD}(-10, 18) &= \\
\mathrm{MCD}(-10, -18) &=
\end{aligned}$$

Máximo común divisor

Sea $\mathrm{MCD}(a, b)$ el máximo común divisor de los números a y b.

- Vale decir, el máximo número $k \in \mathbb{Z}$ tal que $k|a$ y $k|b$.

Ejemplo

Tenemos que:

$$\begin{aligned} \mathrm{MCD}(10, 18) &= 2 \\ \mathrm{MCD}(18, 24) &= 6 \\ \mathrm{MCD}(15, 17) &= 1 \\ \mathrm{MCD}(0, 17) &= 17 \\ \mathrm{MCD}(-10, 18) &= \\ \mathrm{MCD}(-10, -18) &= \end{aligned}$$

Máximo común divisor

Sea $\mathrm{MCD}(a, b)$ el máximo común divisor de los números a y b.

- Vale decir, el máximo número $k \in \mathbb{Z}$ tal que $k|a$ y $k|b$.

Ejemplo

Tenemos que:

$$
\begin{aligned}
\mathrm{MCD}(10, 18) &= 2 \\
\mathrm{MCD}(18, 24) &= 6 \\
\mathrm{MCD}(15, 17) &= 1 \\
\mathrm{MCD}(0, 17) &= 17 \\
\mathrm{MCD}(-10, 18) &= 2 \\
\mathrm{MCD}(-10, -18) &=
\end{aligned}
$$

Máximo común divisor

Sea $\mathrm{MCD}(a, b)$ el máximo común divisor de los números a y b.

- Vale decir, el máximo número $k \in \mathbb{Z}$ tal que $k|a$ y $k|b$.

Ejemplo

Tenemos que:

$$
\begin{array}{rcl}
\mathrm{MCD}(10, 18) & = & 2 \\
\mathrm{MCD}(18, 24) & = & 6 \\
\mathrm{MCD}(15, 17) & = & 1 \\
\mathrm{MCD}(0, 17) & = & 17 \\
\mathrm{MCD}(-10, 18) & = & 2 \\
\mathrm{MCD}(-10, -18) & = & 2
\end{array}
$$

Máximo común divisor

¿Cómo podemos calcular MCD(a, b)?

Máximo común divisor

¿Cómo podemos calcular $\mathrm{MCD}(a, b)$?

Proposición

Si $b \neq 0$, entonces $MCD(a, b) = MCD(b, a \bmod b)$

Máximo común divisor

¿Cómo podemos calcular $\text{MCD}(a, b)$?

Proposición

Si $b \neq 0$, entonces $MCD(a, b) = MCD(b, a \bmod b)$

Demostración: Vamos a demostrar que un número c divide a a y b si y sólo si c divide a b y $a \bmod b$.

- De esto se concluye que $\text{MCD}(a, b) = \text{MCD}(b, a \bmod b)$.

Máximo común divisor

Sabemos que $a = \alpha \cdot b + (a \bmod b)$.

Máximo común divisor

Sabemos que $a = \alpha \cdot b + (a \bmod b)$.

$(\Rightarrow)$ Suponga que $c|a$ y $c|b$.

Máximo común divisor

Sabemos que $a = \alpha \cdot b + (a \bmod b)$.

$(\Rightarrow)$ Suponga que $c|a$ y $c|b$.

Dado que $(a \bmod b) = a - \alpha \cdot b$, concluimos que $c|(a \bmod b)$.

Máximo común divisor

Sabemos que $a = \alpha \cdot b + (a \bmod b)$.

($\Rightarrow$) Suponga que $c|a$ y $c|b$.

Dado que $(a \bmod b) = a - \alpha \cdot b$, concluimos que $c|(a \bmod b)$.

($\Leftarrow$) Suponga que $c|b$ y $c|(a \bmod b)$.

Máximo común divisor

Sabemos que $a = \alpha \cdot b + (a \bmod b)$.

($\Rightarrow$) Suponga que $c | a$ y $c | b$.

Dado que $(a \bmod b) = a - \alpha \cdot b$, concluimos que $c | (a \bmod b)$.

($\Leftarrow$) Suponga que $c | b$ y $c | (a \bmod b)$.

Dado que $a = \alpha \cdot b + (a \bmod b)$, tenemos que $c | a$. $\square$

Cálculo de máximo común divisor

De lo anterior, concluimos la siguiente identidad:

$$\mathrm{MCD}(a, b) = \begin{cases} a & b = 0 \\ \mathrm{MCD}(b, a \bmod b) & b \neq 0 \end{cases}$$

Cálculo de máximo común divisor

De lo anterior, concluimos la siguiente identidad:

$$\mathrm{MCD}(a, b) = \begin{cases} a & b = 0 \\ \mathrm{MCD}(b, a \bmod b) & b \neq 0 \end{cases}$$

Podemos usar esta identidad para generar un algoritmo recursivo para calcular el máximo común divisor.

Cálculo de máximo común divisor

De lo anterior, concluimos la siguiente identidad:

$$\mathrm{MCD}(a, b) = \begin{cases} a & b = 0 \\ \mathrm{MCD}(b, a \bmod b) & b \neq 0 \end{cases}$$

Podemos usar esta identidad para generar un algoritmo recursivo para calcular el máximo común divisor.

- ¿Cómo se ve este algoritmo?

Algoritmo extendido de Euclides

El algoritmo discutido en la lámina anterior puede ser extendido para calcular números $s, t \in \mathbb{Z}$ tales que:

$$\mathrm{MCD}(a, b) = s \cdot a + t \cdot b$$

Algoritmo extendido de Euclides

El algoritmo discutido en la lámina anterior puede ser extendido para calcular números $s, t \in \mathbb{Z}$ tales que:

$$\mathrm{MCD}(a, b) = s \cdot a + t \cdot b$$

Vamos a mostrar cómo funciona el algoritmo suponiendo que a y b son números naturales tales que $b \neq 0$.

Algoritmo extendido de Euclides

El algoritmo discutido en la lámina anterior puede ser extendido para calcular números $s, t \in \mathbb{Z}$ tales que:

$$\mathrm{MCD}(a, b) = s \cdot a + t \cdot b$$

Vamos a mostrar cómo funciona el algoritmo suponiendo que a y b son números naturales tales que $b \neq 0$.

- Bajo este supuesto tenemos que $a = \lfloor \frac{a}{b} \rfloor \cdot b + a \bmod b$.

Algoritmo extendido de Euclides

El algoritmo discutido en la lámina anterior puede ser extendido para calcular números $s, t \in \mathbb{Z}$ tales que:

$$\mathrm{MCD}(a, b) = s \cdot a + t \cdot b$$

Vamos a mostrar cómo funciona el algoritmo suponiendo que a y b son números naturales tales que $b \neq 0$.

- Bajo este supuesto tenemos que $a = \lfloor \frac{a}{b} \rfloor \cdot b + a \bmod b$.

Ejercicio

Suponiendo que tiene el algoritmo para el caso anterior, indique cómo se ve el algoritmo en el caso general en que $a, b \in \mathbb{Z}$ y $b \neq 0$.

Algoritmo extendido de Euclides

Suponga que $a \geq b > 0$, y defina la siguiente sucesión:

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_{i+1} &= r_{i-1} \bmod r_i \qquad (i \geq 2) \end{aligned}$$

Algoritmo extendido de Euclides

Suponga que $a \geq b > 0$, y defina la siguiente sucesión:

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_{i+1} &= r_{i-1} \bmod r_i \qquad (i \geq 2) \end{aligned}$$

Calculamos esta sucesión hasta un número k tal que $r_k = 0$.

Algoritmo extendido de Euclides

Suponga que $a \geq b > 0$, y defina la siguiente sucesión:

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_{i+1} &= r_{i-1} \bmod r_i \qquad (i \geq 2) \end{aligned}$$

Calculamos esta sucesión hasta un número k tal que $r_k = 0$.

- Tenemos que $\text{MCD}(a, b) = r_{k-1}$.

Algoritmo extendido de Euclides

Al mismo tiempo calculamos sucesiones s_i, t_i tales que:

$$r_i = s_i \cdot a + t_i \cdot b$$

Algoritmo extendido de Euclides

Al mismo tiempo calculamos sucesiones s_i, t_i tales que:

$$r_i \quad = \quad s_i \cdot a + t_i \cdot b$$

Tenemos que: $\mathrm{MCD}(a, b) = r_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot b$

Algoritmo extendido de Euclides

Al mismo tiempo calculamos sucesiones s_i, t_i tales que:

$$r_i \quad = \quad s_i \cdot a + t_i \cdot b$$

Tenemos que: $\mathrm{MCD}(a, b) = r_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot b$

Sean:

$$\begin{array}{ll} s_0 = 1 & \qquad t_0 = 0 \\ s_1 = 0 & \qquad t_1 = 1 \end{array}$$

Algoritmo extendido de Euclides

Al mismo tiempo calculamos sucesiones s_i, t_i tales que:

$$r_i \quad = \quad s_i \cdot a + t_i \cdot b$$

Tenemos que: $\mathrm{MCD}(a, b) = r_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot b$

Sean:

$$\begin{array}{ll} s_0 = 1 & \qquad t_0 = 0 \\ s_1 = 0 & \qquad t_1 = 1 \end{array}$$

Se tiene que:

$$\begin{aligned} r_0 &= s_0 \cdot a + t_0 \cdot b \\ r_1 &= s_1 \cdot a + t_1 \cdot b \end{aligned}$$

Algoritmo extendido de Euclides

Dado que $r_{i-1} = \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot r_i + r_{i-1} \bmod r_i$, tenemos que:

$$r_{i-1} \quad = \quad \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot r_i + r_{i+1}$$

Algoritmo extendido de Euclides

Dado que $r_{i-1} = \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot r_i + r_{i-1} \bmod r_i$, tenemos que:

$$r_{i-1} \quad = \quad \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot r_i + r_{i+1}$$

Por lo tanto:

$$s_{i-1} \cdot a + t_{i-1} \cdot b \quad = \quad \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot (s_i \cdot a + t_i \cdot b) + r_{i+1}$$

Algoritmo extendido de Euclides

Dado que $r_{i-1} = \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot r_i + r_{i-1} \bmod r_i$, tenemos que:

$$r_{i-1} \quad = \quad \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot r_i + r_{i+1}$$

Por lo tanto:

$$s_{i-1} \cdot a + t_{i-1} \cdot b \quad = \quad \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot (s_i \cdot a + t_i \cdot b) + r_{i+1}$$

Concluimos que:

$$r_{i+1} \quad = \quad (s_{i-1} - \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot s_i) \cdot a + (t_{i-1} - \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot t_i) \cdot b$$

Algoritmo extendido de Euclides

Dado que $r_{i-1} = \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot r_i + r_{i-1} \bmod r_i$, tenemos que:

$$r_{i-1} \quad = \quad \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot r_i + r_{i+1}$$

Por lo tanto:

$$s_{i-1} \cdot a + t_{i-1} \cdot b \quad = \quad \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot (s_i \cdot a + t_i \cdot b) + r_{i+1}$$

Concluimos que:

$$r_{i+1} \quad = \quad (s_{i-1} - \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot s_i) \cdot a + (t_{i-1} - \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot t_i) \cdot b$$

Definimos entonces:

$$\begin{aligned} s_{i+1} &= s_{i-1} - \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot s_i \\ t_{i+1} &= t_{i-1} - \lfloor \frac{r_{i-1}}{r_i} \rfloor \cdot t_i \end{aligned}$$

Algoritmo extendido de Euclides

Ejemplo

Vamos a usar el algoritmo para $a = 60$ y $b = 13$.

Algoritmo extendido de Euclides

Ejemplo

Vamos a usar el algoritmo para $a = 60$ y $b = 13$.

Inicialmente:

$$\begin{array}{lll} r_0 = 60 & s_0 = 1 & t_0 = 0 \\ r_1 = 13 & s_1 = 0 & t_1 = 1 \end{array}$$

Algoritmo extendido de Euclides

Ejemplo

Vamos a usar el algoritmo para $a = 60$ y $b = 13$.

Inicialmente:

$$\begin{array}{lll} r_0 = 60 & s_0 = 1 & t_0 = 0 \\ r_1 = 13 & s_1 = 0 & t_1 = 1 \end{array}$$

Entonces tenemos que:

$$\begin{array}{rcl} r_2 & = & r_0 \bmod r_1 \\ s_2 & = & s_0 - \lfloor \frac{r_0}{r_1} \rfloor \cdot s_1 \\ t_2 & = & t_0 - \lfloor \frac{r_0}{r_1} \rfloor \cdot t_1 \end{array}$$

Algoritmo extendido para calcular el máximo común divisor

Ejemplo

Por lo tanto:

$$r_2 = 8 \qquad s_2 = 1 \qquad t_2 = -4$$

Algoritmo extendido para calcular el máximo común divisor

Ejemplo

Por lo tanto:

$$r_2 = 8 \qquad s_2 = 1 \qquad t_2 = -4$$

Y el proceso continua:

$$\begin{array}{lll} r_3 = 5 & s_3 = -1 & t_3 = 5 \\ r_4 = 3 & s_4 = 2 & t_4 = -9 \\ r_5 = 2 & s_5 = -3 & t_5 = 14 \\ r_6 = 1 & s_6 = 5 & t_6 = -23 \\ r_7 = 0 & s_7 = -13 & t_7 = 60 \end{array}$$

Algoritmo extendido para calcular el máximo común divisor

Ejemplo

Por lo tanto:

$$r_2 = 8 \qquad s_2 = 1 \qquad t_2 = -4$$

Y el proceso continua:

$$\begin{array}{lll} r_3 = 5 & s_3 = -1 & t_3 = 5 \\ r_4 = 3 & s_4 = 2 & t_4 = -9 \\ r_5 = 2 & s_5 = -3 & t_5 = 14 \\ r_6 = 1 & s_6 = 5 & t_6 = -23 \\ r_7 = 0 & s_7 = -13 & t_7 = 60 \end{array}$$

Tenemos que: $\mathrm{MCD}(60, 13) = 1 = 5 \cdot 60 + (-23) \cdot 13$

La identidad de Bézout

De la existencia del algoritmo extendido de Euclides obtenemos la siguiente identidad.

La identidad de Bézout

De la existencia del algoritmo extendido de Euclides obtenemos la siguiente identidad.

Teorema (Identidad de Bézout)

Para cada $a, b \in \mathbb{Z}$ tal que $a \neq 0$ o $b \neq 0$, existen $s, t \in \mathbb{Z}$ tales que $\text{MCD}(a, b) = s \cdot a + t \cdot b$.

El teorema fundamental de la aritmética

La descomposición de un número

Teorema

Cada número natural $n > 1$ *se puede expresar de una única manera como producto de potencias de números primos.*

La descomposición de un número

Teorema

Cada número natural $n > 1$ se puede expresar de una única manera como producto de potencias de números primos.

Ya demostramos que cada número natural se puede expresar como producto de potencias de números primos.

La descomposición de un número

Teorema

Cada número natural $n > 1$ se puede expresar de una única manera como producto de potencias de números primos.

Ya demostramos que cada número natural se puede expresar como producto de potencias de números primos.

- ¿Qué técnica usamos para demostrar esto?

La descomposición de un número

Teorema

Cada número natural $n > 1$ se puede expresar de una única manera como producto de potencias de números primos.

Ya demostramos que cada número natural se puede expresar como producto de potencias de números primos.

- ¿Qué técnica usamos para demostrar esto?

Nos falta demostrar la unicidad.

Un lema fundamental

Lema

Sea p un número primo. Si $p|(a \cdot b)$, entonces $p|a$ o $p|b$.

Un lema fundamental

Lema

Sea p un número primo. Si $p|(a \cdot b)$, entonces $p|a$ o $p|b$.

Note que el lema anterior no es cierto si p no es un primo: $6|(2 \cdot 3)$, pero $6 \not| 2$ y $6 \not| 3$.

Un lema fundamental

Lema

Sea p un número primo. Si $p|(a \cdot b)$, entonces $p|a$ o $p|b$.

Note que el lema anterior no es cierto si p no es un primo: $6|(2 \cdot 3)$, pero $6 \not| 2$ y $6 \not| 3$.

En ayudantía van a demostrar este lema usando la identidad de Bézout.

Un lema fundamental

Lema

Sea p un número primo. Si $p|(a \cdot b)$, entonces $p|a$ o $p|b$.

Note que el lema anterior no es cierto si p no es un primo: $6|(2 \cdot 3)$, pero $6 \not| 2$ y $6 \not| 3$.

En ayudantía van a demostrar este lema usando la identidad de Bézout.

- Y van a demostrar el teorema fundamental de la aritmética usando este lema.