Matemáticas Discretas I

Enteros

Juan Francisco Díaz Frias

Profesor Titular (1993-hoy)
juanfco.diaz@correounivalle.edu.co
Edif. B13 - 4009
Universidad del Valle

Febrero 2022

Plan

Plan

Plan

Plan

Plan

Motivación

- El computador es discreto desde su arquitectura. La abstracción más sencilla implementada sobre el hardware es la de los números enteros. Un número finito de bits representa un número entero. Y a partir de allí se construyen abstracciones más complejas.
- Computar, consiste en transformar esos enteros manipulándolos con operaciones bien definidas.
- Comprender la teoría de los enteros es esencial para comprender cómo funciona el computador. Adicionalmente, es esencial para construir aplicaciones usadas comúnmente en computación, como dígitos de chequeo o sistemas de encriptación de mensajes basados en aritmética modular.
- Estudiaremos entonces las nociones de divisibilidad, primalidad, congruencias y aritmética modular.
- Adicionalmente, los enteros se pueden estudiar de forma estructural, lo cual permitirá razonar sobre ellos de manera particular con una técnica de demostración muy poderosa denominada inducción.

Motivación

- El computador es discreto desde su arquitectura. La abstracción más sencilla implementada sobre el hardware es la de los números enteros. Un número finito de bits representa un número entero. Y a partir de allí se construyen abstracciones más complejas.
- Computar, consiste en transformar esos enteros manipulándolos con operaciones bien definidas.
- Comprender la teoría de los enteros es esencial para comprender cómo funciona el computador. Adicionalmente, es esencial para construir aplicaciones usadas comúnmente en computación, como dígitos de chequeo o sistemas de encriptación de mensajes basados en aritmética modular.
- Estudiaremos entonces las nociones de divisibilidad, primalidad, congruencias y aritmética modular.
- Adicionalmente, los enteros se pueden estudiar de forma estructural, lo cual permitirá razonar sobre ellos de manera particular con una técnica de demostración muy poderosa denominada inducción.

Motivación

- El computador es discreto desde su arquitectura. La abstracción más sencilla implementada sobre el hardware es la de los números enteros. Un número finito de bits representa un número entero. Y a partir de allí se construyen abstracciones más complejas.
- Computar, consiste en transformar esos enteros manipulándolos con operaciones bien definidas.
- Comprender la teoría de los enteros es esencial para comprender cómo funciona el computador. Adicionalmente, es esencial para construir aplicaciones usadas comúnmente en computación, como dígitos de chequeo o sistemas de encriptación de mensajes basados en aritmética modular.
- Estudiaremos entonces las nociones de divisibilidad, primalidad, congruencias y aritmética modular.
- Adicionalmente, los enteros se pueden estudiar de forma estructural, lo cual permitirá razonar sobre ellos de manera particular con una técnica de demostración muy poderosa denominada inducción.

Motivación

- El computador es discreto desde su arquitectura. La abstracción más sencilla implementada sobre el hardware es la de los números enteros. Un número finito de bits representa un número entero. Y a partir de allí se construyen abstracciones más complejas.
- Computar, consiste en transformar esos enteros manipulándolos con operaciones bien definidas.
- Comprender la teoría de los enteros es esencial para comprender cómo funciona el computador. Adicionalmente, es esencial para construir aplicaciones usadas comúnmente en computación, como dígitos de chequeo o sistemas de encriptación de mensajes basados en aritmética modular.
- Estudiaremos entonces las nociones de divisibilidad, primalidad, congruencias y aritmética modular.
- Adicionalmente, los enteros se pueden estudiar de forma estructural, lo cual permitirá razonar sobre ellos de manera particular con una técnica de demostración muy poderosa denominada inducción.

Motivación

- El computador es discreto desde su arquitectura. La abstracción más sencilla implementada sobre el hardware es la de los números enteros. Un número finito de bits representa un número entero. Y a partir de allí se construyen abstracciones más complejas.
- Computar, consiste en transformar esos enteros manipulándolos con operaciones bien definidas.
- Comprender la teoría de los enteros es esencial para comprender cómo funciona el computador. Adicionalmente, es esencial para construir aplicaciones usadas comúnmente en computación, como dígitos de chequeo o sistemas de encriptación de mensajes basados en aritmética modular.
- Estudiaremos entonces las nociones de divisibilidad, primalidad, congruencias y aritmética modular.
- Adicionalmente, los enteros se pueden estudiar de forma estructural, lo cual permitirá razonar sobre ellos de manera particular con una técnica de demostración muy poderosa denominada inducción.

La naturaleza de $\mathbb{N}$ (1)

- Antes de empezar a ver algunas de las propiedades y aplicaciones de los números naturales y enteros, es importante establecer su naturaleza.
- Los axiomas de Peano definen de manera exacta al conjunto de los números naturales. Fueron establecidos por Giuseppe Peano, matemático italiano en el siglo XIX. El conjunto de los números naturales, $\mathbb{N}$, es el conjunto de elementos que se pueden construir a partir de una constante, 0, y una función sucesor, $S : \mathbb{N} \rightarrow \mathbb{N}$ y los siguientes 5 axiomas fundamentales:
  1. $0 \in \mathbb{N}$ 0 es un número natural
  2. $\forall n | n \in \mathbb{N} : S(n) \in \mathbb{N}$ si n es natural, su sucesor también lo es
  3. $\forall n | n \in \mathbb{N} : S(n) \neq 0$ el 0 no es sucesor de ningún natural
  4. $\forall n, m | n, m \in \mathbb{N} : S(n) = S(m) \Longrightarrow n = m$
  5. $\forall A | A \subseteq \mathbb{N} : (0 \in A \wedge (\forall n | n \in A : S(n) \in A)) \Longrightarrow A = \mathbb{N}$

La naturaleza de $\mathbb{N}$ (1)

- Antes de empezar a ver algunas de las propiedades y aplicaciones de los números naturales y enteros, es importante establecer su naturaleza.
- Los axiomas de Peano definen de manera exacta al conjunto de los números naturales. Fueron establecidos por Giuseppe Peano, matemático italiano en el siglo XIX. El conjunto de los números naturales, $\mathbb{N}$, es el conjunto de elementos que se pueden construir a partir de una constante, 0, y una función sucesor, $S : \mathbb{N} \to \mathbb{N}$ y los siguientes 5 axiomas fundamentales:
  1. $0 \in \mathbb{N}$ — 0 es un número natural
  2. $\forall n | n \in \mathbb{N} : S(n) \in \mathbb{N}$ — si n es natural, su sucesor también lo es
  3. $\forall n | n \in \mathbb{N} : S(n) \neq 0$ — el 0 no es sucesor de ningún natural
  4. $\forall n, m | n, m \in \mathbb{N} : S(n) = S(m) \implies n = m$ — S es $1-1$
  5. $\forall A | A \subseteq \mathbb{N} : (0 \in A \wedge (\forall n | n \in A : S(n) \in A)) \implies A = \mathbb{N}$ — Inducción

La naturaleza de $\mathbb{N}$ (1)

- Antes de empezar a ver algunas de las propiedades y aplicaciones de los números naturales y enteros, es importante establecer su naturaleza.
- Los axiomas de Peano definen de manera exacta al conjunto de los números naturales. Fueron establecidos por Giuseppe Peano, matemático italiano en el siglo XIX. El conjunto de los números naturales, $\mathbb{N}$, es el conjunto de elementos que se pueden construir a partir de una constante, 0, y una función sucesor, $S : \mathbb{N} \to \mathbb{N}$ y los siguientes 5 axiomas fundamentales:
  1. $0 \in \mathbb{N}$ — 0 es un número natural
  2. $\forall n | n \in \mathbb{N} : S(n) \in \mathbb{N}$ — si n es natural, su sucesor también lo es
  3. $\forall n | n \in \mathbb{N} : S(n) \neq 0$ — el 0 no es sucesor de ningún natural
  4. $\forall n, m | n, m \in \mathbb{N} : S(n) = S(m) \implies n = m$ — S es $1-1$
  5. $\forall A | A \subseteq \mathbb{N} : (0 \in A \wedge (\forall n | n \in A : S(n) \in A)) \implies A = \mathbb{N}$ — Inducción

La naturaleza de $\mathbb{N}$ (1)

- Antes de empezar a ver algunas de las propiedades y aplicaciones de los números naturales y enteros, es importante establecer su naturaleza.
- Los axiomas de Peano definen de manera exacta al conjunto de los números naturales. Fueron establecidos por Giuseppe Peano, matemático italiano en el siglo XIX. El conjunto de los números naturales, $\mathbb{N}$, es el conjunto de elementos que se pueden construir a partir de una constante, 0, y una función sucesor, $S : \mathbb{N} \to \mathbb{N}$ y los siguientes 5 axiomas fundamentales:
  1. $0 \in \mathbb{N}$ — 0 es un número natural
  2. $\forall n | n \in \mathbb{N} : S(n) \in \mathbb{N}$ — si n es natural, su sucesor también lo es
  3. $\forall n | n \in \mathbb{N} : S(n) \neq 0$ — el 0 no es sucesor de ningún natural
  4. $\forall n, m | n, m \in \mathbb{N} : S(n) = S(m) \implies n = m$ — S es $1-1$
  5. $\forall A | A \subseteq \mathbb{N} : (0 \in A \wedge (\forall n | n \in A : S(n) \in A)) \implies A = \mathbb{N}$ — Inducción

La naturaleza de $\mathbb{N}$ (1)

- Antes de empezar a ver algunas de las propiedades y aplicaciones de los números naturales y enteros, es importante establecer su naturaleza.
- Los axiomas de Peano definen de manera exacta al conjunto de los números naturales. Fueron establecidos por Giuseppe Peano, matemático italiano en el siglo XIX. El conjunto de los números naturales, $\mathbb{N}$, es el conjunto de elementos que se pueden construir a partir de una constante, 0, y una función sucesor, $S : \mathbb{N} \to \mathbb{N}$ y los siguientes 5 axiomas fundamentales:
  1. $0 \in \mathbb{N}$ — 0 es un número natural
  2. $\forall n | n \in \mathbb{N} : S(n) \in \mathbb{N}$ — si n es natural, su sucesor también lo es
  3. $\forall n | n \in \mathbb{N} : S(n) \neq 0$ — el 0 no es sucesor de ningún natural
  4. $\forall n, m | n, m \in \mathbb{N} : S(n) = S(m) \implies n = m$ — S es $1-1$
  5. $\forall A | A \subseteq \mathbb{N} : (0 \in A \wedge (\forall n | n \in A : S(n) \in A)) \implies A = \mathbb{N}$ — Inducción

La naturaleza de $\mathbb{N}$ (1)

- Antes de empezar a ver algunas de las propiedades y aplicaciones de los números naturales y enteros, es importante establecer su naturaleza.
- Los axiomas de Peano definen de manera exacta al conjunto de los números naturales. Fueron establecidos por Giuseppe Peano, matemático italiano en el siglo XIX. El conjunto de los números naturales, $\mathbb{N}$, es el conjunto de elementos que se pueden construir a partir de una constante, 0, y una función sucesor, $S : \mathbb{N} \rightarrow \mathbb{N}$ y los siguientes 5 axiomas fundamentales:
    1. $0 \in \mathbb{N}$ — 0 es un número natural
    2. $\forall n | n \in \mathbb{N} : S(n) \in \mathbb{N}$ — si n es natural, su sucesor también lo es
    3. $\forall n | n \in \mathbb{N} : S(n) \neq 0$ — el 0 no es sucesor de ningún natural
    4. $\forall n, m | n, m \in \mathbb{N} : S(n) = S(m) \implies n = m$ — S es $1-1$
    5. $\forall A | A \subseteq \mathbb{N} : (0 \in A \wedge (\forall n | n \in A : S(n) \in A)) \implies A = \mathbb{N}$ — Inducción

La naturaleza de $\mathbb{N}$ (1)

- Antes de empezar a ver algunas de las propiedades y aplicaciones de los números naturales y enteros, es importante establecer su naturaleza.
- Los axiomas de Peano definen de manera exacta al conjunto de los números naturales. Fueron establecidos por Giuseppe Peano, matemático italiano en el siglo XIX. El conjunto de los números naturales, $\mathbb{N}$, es el conjunto de elementos que se pueden construir a partir de una constante, 0, y una función sucesor, $S : \mathbb{N} \rightarrow \mathbb{N}$ y los siguientes 5 axiomas fundamentales:
  1. $0 \in \mathbb{N}$ — 0 es un número natural
  2. $\forall n | n \in \mathbb{N} : S(n) \in \mathbb{N}$ — si n es natural, su sucesor también lo es
  3. $\forall n | n \in \mathbb{N} : S(n) \neq 0$ — el 0 no es sucesor de ningún natural
  4. $\forall n, m | n, m \in \mathbb{N} : S(n) = S(m) \implies n = m$ — S es $1-1$
  5. $\forall A | A \subseteq \mathbb{N} : (0 \in A \wedge (\forall n | n \in A : S(n) \in A)) \implies A = \mathbb{N}$ — Inducción

La naturaleza de $\mathbb{N}$ (2)

- Tratemos de ver gráficamente los números naturales a partir de los axiomas de Peano:
  1. $0 \in \mathbb{N}$ — 0 es un número natural
  2. $\forall n | n \in \mathbb{N} : S(n) \in \mathbb{N}$ — si n es natural, su sucesor también lo es
  3. $\forall n | n \in \mathbb{N} : S(n) \neq 0$ — el 0 no es sucesor de ningún natural
  4. $\forall n, m | n, m \in \mathbb{N} : S(n) = S(m) \implies n = m$ — S es $1-1$
  5. $\forall A | A \subseteq \mathbb{N} : (0 \in A \wedge (\forall n | n \in A : S(n) \in A)) \implies A = \mathbb{N}$ — Inducción

- Los enteros, $\mathbb{Z}$, pueden concebirse como dos copias de $\mathbb{N}$, a una de las cuales se le añade un signo '-'y se identifica -0 con 0. Su representación gráfica es una recta que crece en las dos direcciones.

La naturaleza de $\mathbb{N}$ (2)

- Tratemos de ver gráficamente los números naturales a partir de los axiomas de Peano:
  1. $0 \in \mathbb{N}$ — 0 es un número natural
  2. $\forall n | n \in \mathbb{N} : S(n) \in \mathbb{N}$ — si n es natural, su sucesor también lo es
  3. $\forall n | n \in \mathbb{N} : S(n) \neq 0$ — el 0 no es sucesor de ningún natural
  4. $\forall n, m | n, m \in \mathbb{N} : S(n) = S(m) \implies n = m$ — S es $1-1$
  5. $\forall A | A \subseteq \mathbb{N} : (0 \in A \wedge (\forall n | n \in A : S(n) \in A)) \implies A = \mathbb{N}$ — Inducción

- Los enteros, $\mathbb{Z}$, pueden concebirse como dos copias de $\mathbb{N}$, a una de las cuales se le añade un signo '-'y se identifica -0 con 0. Su representación gráfica es una recta que crece en las dos direcciones.

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
- Definamos la relación de orden $n < m$ entre dos números naturales:

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
- Definamos la relación de orden $n < m$ entre dos números naturales:

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
- Definamos la relación de orden $n < m$ entre dos números naturales:

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
- Definamos la relación de orden $n < m$ entre dos números naturales:

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
  Ax. ×1:$\forall n | n \in \mathbb{N} : n \times 0 = 0$
  Ax. ×2: $\forall n | n \in \mathbb{N} : n \times S(m) = (n \times m) + n$
  Por ejemplo:
  $S(S(0)) \times S(0) = (S(S(0)) \times 0) + S(S(0)) = 0 + S(S(0)) = S(S(0))$
- Definamos la relación de orden $n < m$ entre dos números naturales:

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
  Ax. ×1: $\forall n | n \in \mathbb{N} : n \times 0 = 0$
  Ax. ×2: $\forall n | n \in \mathbb{N} : n \times S(m) = (n \times m) + n$
  Por ejemplo:
  $S(S(0)) \times S(0) = (S(S(0)) \times 0) + S(S(0)) = 0 + S(S(0)) = \ldots = S(S(0))$
- Definamos la relación de orden $n < m$ entre dos números naturales:

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
  Ax. ×1:$\forall n | n \in \mathbb{N} : n \times 0 = 0$
  Ax. ×2: $\forall n | n \in \mathbb{N} : n \times S(m) = (n \times m) + n$
  Por ejemplo:
  $S(S(0)) \times S(0) = (S(S(0)) \times 0) + S(S(0)) = 0 + S(S(0)) = \ldots = S(S(0))$
- Definamos la relación de orden $n < m$ entre dos números naturales:

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
  Ax. ×1: $\forall n | n \in \mathbb{N} : n \times 0 = 0$
  Ax. ×2: $\forall n | n \in \mathbb{N} : n \times S(m) = (n \times m) + n$
  Por ejemplo:
  $S(S(0)) \times S(0) = (S(S(0)) \times 0) + S(S(0)) = 0 + S(S(0)) = \ldots = S(S(0))$
- Definamos la relación de orden $n < m$ entre dos números naturales:
  Ax. <1: $\forall n | n \in \mathbb{N} : (0 < n) = (0 \neq n)$
  Ax. <2: $\forall n | n \in \mathbb{N} : S(n) < 0 = false$
  Ax. <2: $\forall n | n \in \mathbb{N} : (S(n) < S(m)) = (n < m)$
  Por ejemplo: $S(S(0)) < S(0) = S(0) < 0 = false$

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
  Ax. $\times$1:$\forall n | n \in \mathbb{N} : n \times 0 = 0$
  Ax. $\times$2: $\forall n | n \in \mathbb{N} : n \times S(m) = (n \times m) + n$
  Por ejemplo:
  $S(S(0)) \times S(0) = (S(S(0)) \times 0) + S(S(0)) = 0 + S(S(0)) = \ldots = S(S(0))$
- Definamos la relación de orden $n < m$ entre dos números naturales:
  Ax. <1:$\forall n | n \in \mathbb{N} : (0 < n) \equiv (0 \neq n)$
  Ax. <2:$\forall n | n \in \mathbb{N} : S(n) < 0 \equiv false$
  Ax. <2:$\forall n | n \in \mathbb{N} : (S(n) < S(m)) \equiv (n < m)$
  Por ejemplo: $S(S(0)) < S(0) = S(0) < 0 = false$

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
  Ax. ×1:$\forall n | n \in \mathbb{N} : n \times 0 = 0$
  Ax. ×2: $\forall n | n \in \mathbb{N} : n \times S(m) = (n \times m) + n$
  Por ejemplo:
  $S(S(0)) \times S(0) = (S(S(0)) \times 0) + S(S(0)) = 0 + S(S(0)) = \ldots = S(S(0))$
- Definamos la relación de orden $n < m$ entre dos números naturales:
  Ax. <1:$\forall n | n \in \mathbb{N} : (0 < n) \equiv (0 \neq n)$
  Ax. <2:$\forall n | n \in \mathbb{N} : S(n) < 0 \equiv false$
  Ax. <2:$\forall n | n \in \mathbb{N} : (S(n) < S(m)) \equiv (n < m)$
  Por ejemplo: $S(S(0)) < S(0) \equiv S(0) < 0 \equiv false$

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
  Ax. ×1: $\forall n | n \in \mathbb{N} : n \times 0 = 0$
  Ax. ×2: $\forall n | n \in \mathbb{N} : n \times S(m) = (n \times m) + n$
  Por ejemplo:
  $S(S(0)) \times S(0) = (S(S(0)) \times 0) + S(S(0)) = 0 + S(S(0)) = \ldots = S(S(0))$
- Definamos la relación de orden $n < m$ entre dos números naturales:
  Ax. <1: $\forall n | n \in \mathbb{N} : (0 < n) \equiv (0 \neq n)$
  Ax. <2: $\forall n | n \in \mathbb{N} : S(n) < 0 \equiv false$
  Ax. <2: $\forall n | n \in \mathbb{N} : (S(n) < S(m)) \equiv (n < m)$
  Por ejemplo: $S(S(0)) < S(0) = S(0) < 0 \equiv false$

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
  Ax. ×1:$\forall n | n \in \mathbb{N} : n \times 0 = 0$
  Ax. ×2: $\forall n | n \in \mathbb{N} : n \times S(m) = (n \times m) + n$
  Por ejemplo:
  $S(S(0)) \times S(0) = (S(S(0)) \times 0) + S(S(0)) = 0 + S(S(0)) = \ldots = S(S(0))$
- Definamos la relación de orden $n < m$ entre dos números naturales:
  Ax. <1:$\forall n | n \in \mathbb{N} : (0 < n) \equiv (0 \neq n)$
  Ax. <2:$\forall n | n \in \mathbb{N} : S(n) < 0 \equiv \mathit{false}$
  Ax. <2:$\forall n | n \in \mathbb{N} : (S(n) < S(m)) \equiv (n < m)$
  Por ejemplo: $S(S(0)) < S(0) = S(0) < 0 \equiv \mathit{false}$

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
  Ax. ×1: $\forall n | n \in \mathbb{N} : n \times 0 = 0$
  Ax. ×2: $\forall n | n \in \mathbb{N} : n \times S(m) = (n \times m) + n$
  Por ejemplo:
  $S(S(0)) \times S(0) = (S(S(0)) \times 0) + S(S(0)) = 0 + S(S(0)) = \ldots = S(S(0))$
- Definamos la relación de orden $n < m$ entre dos números naturales:
  Ax. <1: $\forall n | n \in \mathbb{N} : (0 < n) \equiv (0 \neq n)$
  Ax. <2: $\forall n | n \in \mathbb{N} : S(n) < 0 \equiv \mathit{false}$
  Ax. <2: $\forall n | n \in \mathbb{N} : (S(n) < S(m)) \equiv (n < m)$
  Por ejemplo: $S(S(0)) < S(0) = S(0) < 0 \equiv \mathit{false}$

Suma, multiplicación y orden en $\mathbb{N}$

- Una vez entendida la naturaleza de $\mathbb{N}$ podemos definir operaciones básicas sobre ellos, como la suma, la multiplicación, o relaciones básicas, como la relación de orden.
- Definamos la suma $n + m$ de dos números naturales:
  Ax. +1: $\forall n | n \in \mathbb{N} : n + 0 = n$
  Ax. +2: $\forall n | n \in \mathbb{N} : n + S(m) = S(n + m)$
  Por ejemplo: $S(S(0)) + S(0) = S(S(S(0)) + 0) = S(S(S(0)))$
- Definamos la multiplicación $n \times m$ de dos números naturales:
  Ax. ×1:$\forall n | n \in \mathbb{N} : n \times 0 = 0$
  Ax. ×2: $\forall n | n \in \mathbb{N} : n \times S(m) = (n \times m) + n$
  Por ejemplo:
  $S(S(0)) \times S(0) = (S(S(0)) \times 0) + S(S(0)) = 0 + S(S(0)) = \ldots = S(S(0))$
- Definamos la relación de orden $n < m$ entre dos números naturales:
  Ax. <1:$\forall n | n \in \mathbb{N} : (0 < n) \equiv (0 \neq n)$
  Ax. <2:$\forall n | n \in \mathbb{N} : S(n) < 0 \equiv \mathit{false}$
  Ax. <2:$\forall n | n \in \mathbb{N} : (S(n) < S(m)) \equiv (n < m)$
  Por ejemplo: $S(S(0)) < S(0) = S(0) < 0 \equiv \mathit{false}$

Representaciones de $\mathbb{N}$

- Evidentemente, trabajar con la representación de números naturales asociada a los axiomas de Peano sería impráctico: ¿Cuánto tiempo y espacio se gastaría uno para escribir el número entero que hoy escribimos como 12537?
- Entonces, ¿cómo representar los números naturales?
  - ¿Con cuántos símbolos? 1? 2? 8? 10? 16?
  - El sistema de numeración decimal que hoy usamos utiliza 10 símbolos: $\{0,1,2,3,4,5,6,7,8,9\}$.

$$12537 = 1 * 10^4 + 2 * 10^3 + 5 * 10^2 + 3 * 10^1 + 7 * 10^0$$

  - Al número 10 se le denomina la base del sistema de numeración.

Representaciones de $\mathbb{N}$

- Evidentemente, trabajar con la representación de números naturales asociada a los axiomas de Peano sería impráctico: ¿Cuánto tiempo y espacio se gastaría uno para escribir el número entero que hoy escribimos como 12537?
- Entonces, ¿cómo representar los números naturales?
  - ¿Con cuántos símbolos? 1? 2? 8? 10? 16?
  - El sistema de numeración decimal que hoy usamos utiliza 10 símbolos: {0,1,2,3,4,5,6,7,8,9}.

$$12537 = 1 * 10^4 + 2 * 10^3 + 5 * 10^2 + 3 * 10^1 + 7 * 10^0$$

  - Al número 10 se le denomina la base del sistema de numeración.

Representaciones de $\mathbb{N}$

- Evidentemente, trabajar con la representación de números naturales asociada a los axiomas de Peano sería impráctico: ¿Cuánto tiempo y espacio se gastaría uno para escribir el número entero que hoy escribimos como 12537?
- Entonces, ¿cómo representar los números naturales?
  - ¿Con cuántos símbolos? 1? 2? 8? 10? 16?
  - El sistema de numeración decimal que hoy usamos utiliza 10 símbolos: {0,1,2,3,4,5,6,7,8,9}.

$$12537 = 1 * 10^4 + 2 * 10^3 + 5 * 10^2 + 3 * 10^1 + 7 * 10^0$$

  - Al número 10 se le denomina la base del sistema de numeración.

Representaciones de $\mathbb{N}$

- Evidentemente, trabajar con la representación de números naturales asociada a los axiomas de Peano sería impráctico: ¿Cuánto tiempo y espacio se gastaría uno para escribir el número entero que hoy escribimos como 12537?
- Entonces, ¿cómo representar los números naturales?
  - ¿Con cuántos símbolos? 1? 2? 8? 10? 16?
  - El sistema de numeración decimal que hoy usamos utiliza 10 símbolos: $\{0,1,2,3,4,5,6,7,8,9\}$.

$$12537 = 1 * 10^4 + 2 * 10^3 + 5 * 10^2 + 3 * 10^1 + 7 * 10^0$$

  - Al número 10 se le denomina la base del sistema de numeración.

Representaciones de $\mathbb{N}$

- Evidentemente, trabajar con la representación de números naturales asociada a los axiomas de Peano sería impráctico: ¿Cuánto tiempo y espacio se gastaría uno para escribir el número entero que hoy escribimos como 12537?
- Entonces, ¿cómo representar los números naturales?
  - ¿Con cuántos símbolos? 1? 2? 8? 10? 16?
  - El sistema de numeración decimal que hoy usamos utiliza 10 símbolos: $\{0,1,2,3,4,5,6,7,8,9\}$.

$$12537 = 1 * 10^4 + 2 * 10^3 + 5 * 10^2 + 3 * 10^1 + 7 * 10^0$$

  - Al número 10 se le denomina la base del sistema de numeración.

Representación de $\mathbb{N}$ en base b

Sea b un número entero mayor que 1. Si n es un entero positivo, n se puede expresar de manera única como

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

donde k es un entero no negativo, $a_0, a_1, \ldots, a_k$ son enteros no negativos menores que b y $a_k \neq 0$.
A $(a_k a_{k-1} \ldots a_1 a_0)_b$ se le denomina la expansión de n en base b.
Puesto que la base 10 es la que conocemos y usamos, en lugar de escribir $(12357)_{10}$ escribimos 12357.

Representación de $\mathbb{N}$ en base b

Sea b un número entero mayor que 1. Si n es un entero positivo, n se puede expresar de manera única como

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

donde k es un entero no negativo, $a_0, a_1, \ldots, a_k$ son enteros no negativos menores que b y $a_k \neq 0$.
A $(a_k a_{k-1} \ldots a_1 a_0)_b$ se le denomina la expansión de n en base b.
Puesto que la base 10 es la que conocemos y usamos, en lugar de escribir $(12357)_{10}$ escribimos 12357.

Representación de $\mathbb{N}$ en base b

Sea b un número entero mayor que 1. Si n es un entero positivo, n se puede expresar de manera única como

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

donde k es un entero no negativo, $a_0, a_1, \ldots, a_k$ son enteros no negativos menores que b y $a_k \neq 0$.
A $(a_k a_{k-1} \ldots a_1 a_0)_b$ se le denomina la expansión de n en base b.
Puesto que la base 10 es la que conocemos y usamos, en lugar de escribir $(12357)_{10}$ escribimos 12357.

Representación de $\mathbb{N}$ en base b (cont.)

Las bases más usadas en informática, además de la base 10, son:

- Base 2: Da lugar al sistema de numeración binario. Los símbolos usados son {0,1}.

$$(10101)_2 = 1 * 2^4 + 0 * 2^3 + 1 * 2^2 + 0 * 2^1 + 1 * 2^0 = 21$$

- Base 8: Da lugar al sistema de numeración octal. Los símbolos usados son {0,1, 2, 3, 4, 5, 6, 7}.

$$(17016)_8 = 1 * 8^4 + 7 * 8^3 + 0 * 8^2 + 1 * 8^1 + 6 * 8^0 = 7694$$

- Base 16: Da lugar al sistema de numeración hexadecimal. Los símbolos usados son {0,1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}.

$$(2AE0B)_{16} = 2 * 16^4 + 10 * 16^3 + 14 * 16^2 + 0 * 16^1 + 11 * 16^0 = 175627$$

- Queda claro cómo calcular la representación decimal de un número natural dada su expansión en base b.

Representación de $\mathbb{N}$ en base b (cont.)

Las bases más usadas en informática, además de la base 10, son:

- Base 2: Da lugar al sistema de numeración binario. Los símbolos usados son {0,1}.

$$(10101)_2 = 1 * 2^4 + 0 * 2^3 + 1 * 2^2 + 0 * 2^1 + 1 * 2^0 = 21$$

- Base 8: Da lugar al sistema de numeración octal. Los símbolos usados son {0,1, 2, 3, 4, 5, 6, 7}.

$$(17016)_8 = 1 * 8^4 + 7 * 8^3 + 0 * 8^2 + 1 * 8^1 + 6 * 8^0 = 7694$$

- Base 16: Da lugar al sistema de numeración hexadecimal. Los símbolos usados son {0,1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}.

$$(2AE0B)_{16} = 2 * 16^4 + 10 * 16^3 + 14 * 16^2 + 0 * 16^1 + 11 * 16^0 = 175627$$

- Queda claro cómo calcular la representación decimal de un número natural dada su expansión en base b. ¿Y dada la representación decimal de un número natural, cómo calcular su expansión en base b?

Representación de $\mathbb{N}$ en base b (cont.)

Las bases más usadas en informática, además de la base 10, son:

- Base 2: Da lugar al sistema de numeración binario. Los símbolos usados son {0,1}.

$$(10101)_2 = 1 * 2^4 + 0 * 2^3 + 1 * 2^2 + 0 * 2^1 + 1 * 2^0 = 21$$

- Base 8: Da lugar al sistema de numeración octal. Los símbolos usados son {0,1, 2, 3, 4, 5, 6, 7}.

$$(17016)_8 = 1 * 8^4 + 7 * 8^3 + 0 * 8^2 + 1 * 8^1 + 6 * 8^0 = 7694$$

- Base 16: Da lugar al sistema de numeración hexadecimal. Los símbolos usados son {0,1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}.

$$(2AE0B)_{16} = 2 * 16^4 + 10 * 16^3 + 14 * 16^2 + 0 * 16^1 + 11 * 16^0 = 175627$$

- Queda claro cómo calcular la representación decimal de un número natural dada su expansión en base b. ¿Y dada la representación decimal de un número natural, cómo calcular su expansión en base b?

Representación de $\mathbb{N}$ en base b (cont.)

Las bases más usadas en informática, además de la base 10, son:

- Base 2: Da lugar al sistema de numeración binario. Los símbolos usados son $\{0,1\}$.

$$(10101)_2 = 1 * 2^4 + 0 * 2^3 + 1 * 2^2 + 0 * 2^1 + 1 * 2^0 = 21$$

- Base 8: Da lugar al sistema de numeración octal. Los símbolos usados son $\{0,1, 2, 3, 4, 5, 6, 7\}$.

$$(17016)_8 = 1 * 8^4 + 7 * 8^3 + 0 * 8^2 + 1 * 8^1 + 6 * 8^0 = 7694$$

- Base 16: Da lugar al sistema de numeración hexadecimal. Los símbolos usados son $\{0,1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$.

$$(2AE0B)_{16} = 2 * 16^4 + 10 * 16^3 + 14 * 16^2 + 0 * 16^1 + 11 * 16^0 = 175627$$

- Queda claro cómo calcular la representación decimal de un número natural dada su expansión en base b. ¿Y dada la representación decimal de un número natural, cómo calcular su expansión en base b?

Representación de $\mathbb{N}$ en base b (cont.)

Las bases más usadas en informática, además de la base 10, son:

- Base 2: Da lugar al sistema de numeración binario. Los símbolos usados son {0,1}.

$$(10101)_2 = 1 * 2^4 + 0 * 2^3 + 1 * 2^2 + 0 * 2^1 + 1 * 2^0 = 21$$

- Base 8: Da lugar al sistema de numeración octal. Los símbolos usados son {0,1, 2, 3, 4, 5, 6, 7}.

$$(17016)_8 = 1 * 8^4 + 7 * 8^3 + 0 * 8^2 + 1 * 8^1 + 6 * 8^0 = 7694$$

- Base 16: Da lugar al sistema de numeración hexadecimal. Los símbolos usados son {0,1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}.

$$(2AE0B)_{16} = 2 * 16^4 + 10 * 16^3 + 14 * 16^2 + 0 * 16^1 + 11 * 16^0 = 175627$$

- Queda claro cómo calcular la representación decimal de un número natural dada su expansión en base b. ¿Y dada la representación decimal de un número natural, cómo calcular su expansión en base b?

Plan

Divisibilidad: definiciones

- En adelante, supondremos conocidos los siguientes conjuntos numéricos:
  $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ Los enteros
  $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ Los naturales
  $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ Los enteros positivos
- Dados $n, m \in \mathbb{Z}$, se dice que n divide a m, y se denota $n|m$, si:

$$n|m \equiv \exists q \in \mathbb{Z}| : m = nq$$

  Se dice también que:
- Ejemplos:

Divisibilidad: definiciones

- En adelante, supondremos conocidos los siguientes conjuntos numéricos:
  $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ Los enteros
  $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ Los naturales
  $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ Los enteros positivos
- Dados $n, m \in \mathbb{Z}$, se dice que n divide a m, y se denota $n|m$, si:

$$n|m \equiv \exists q \in \mathbb{Z}| : m = nq$$

  Se dice también que:

- Ejemplos:

Divisibilidad: definiciones

- En adelante, supondremos conocidos los siguientes conjuntos numéricos:
  $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ Los enteros
  $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ Los naturales
  $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ Los enteros positivos
- Dados $n, m \in \mathbb{Z}$, se dice que n divide a m, y se denota $n|m$, si:

$$n|m \equiv \exists q \in \mathbb{Z}| : m = nq$$

  Se dice también que:
  n es un divisor de m
  m es un múltiplo de n
- Ejemplos:

Divisibilidad: definiciones

- En adelante, supondremos conocidos los siguientes conjuntos numéricos:
  $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ Los enteros
  $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ Los naturales
  $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ Los enteros positivos
- Dados $n, m \in \mathbb{Z}$, se dice que *n divide a m*, y se denota $n|m$, si:

$$n|m \equiv \exists q \in \mathbb{Z}| : m = nq$$

  Se dice también que:
  n es un divisor de m
  m es un múltiplo de n
- Ejemplos:

Divisibilidad: definiciones

- En adelante, supondremos conocidos los siguientes conjuntos numéricos:
  $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ Los enteros
  $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ Los naturales
  $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ Los enteros positivos
- Dados $n, m \in \mathbb{Z}$, se dice que n divide a m, y se denota $n|m$, si:

$$n|m \equiv \exists q \in \mathbb{Z}| : m = nq$$

  Se dice también que:
  n es un divisor de m
  m es un múltiplo de n
- Ejemplos:

Divisibilidad: definiciones

- En adelante, supondremos conocidos los siguientes conjuntos numéricos:
  $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ Los enteros
  $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ Los naturales
  $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ Los enteros positivos
- Dados $n, m \in \mathbb{Z}$, se dice que n divide a m, y se denota $n|m$, si:

$$n|m \equiv \exists q \in \mathbb{Z}| : m = nq$$

  Se dice también que:
  n es un divisor de m
  m es un múltiplo de n
- Ejemplos:
  Teo:$3|12$: $true \equiv 12 = 3 \times 4 \implies \exists q \in \mathbb{Z}| : 12 = 3q \equiv 3|12$
  Teo:$3|-12$: $true \equiv -12 = 3 \times -4 \implies \exists q \in \mathbb{Z}| : -12 = 3q \equiv 3|-12$
  Teo:$4|24$: $true \equiv 24 = 4 \times 6 \implies \exists q \in \mathbb{Z}| : 24 = 4q \equiv 4|24$

Divisibilidad: definiciones

- En adelante, supondremos conocidos los siguientes conjuntos numéricos:
  $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ Los enteros
  $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ Los naturales
  $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ Los enteros positivos
- Dados $n, m \in \mathbb{Z}$, se dice que n divide a m, y se denota $n|m$, si:

$$n|m \equiv \exists q \in \mathbb{Z}| : m = nq$$

  Se dice también que:
  n es un divisor de m
  m es un múltiplo de n
- Ejemplos:
  Teo:$3|12$: $true \equiv 12 = 3 \times 4 \implies \exists q \in \mathbb{Z}| : 12 = 3q \equiv 3|12$
  Teo:$3|-12$: $true \equiv -12 = 3 \times -4 \implies \exists q \in \mathbb{Z}| : -12 = 3q \equiv 3|-12$
  Teo:$4|24$: $true \equiv 24 = 4 \times 6 \implies \exists q \in \mathbb{Z}| : 24$

Divisibilidad: definiciones

- En adelante, supondremos conocidos los siguientes conjuntos numéricos:
  $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ Los enteros
  $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ Los naturales
  $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ Los enteros positivos
- Dados $n, m \in \mathbb{Z}$, se dice que n divide a m, y se denota $n|m$, si:

$$n|m \equiv \exists q \in \mathbb{Z}| : m = nq$$

  Se dice también que:
  n es un divisor de m
  m es un múltiplo de n
- Ejemplos:
  Teo: $3|12$: $true \equiv 12 = 3 \times 4 \implies \exists q \in \mathbb{Z}| : 12 = 3q \equiv 3|12$
  Teo: $3|-12$: $true \equiv -12 = 3 \times -4 \implies \exists q \in \mathbb{Z}| : -12 = 3q \equiv 3|-12$
  Teo: $4|24$: $true \equiv 24 = 4 \times 6 \implies \exists q \in \mathbb{Z}| : 24 = 4q \equiv 4|24$

Divisibilidad: definiciones

- En adelante, supondremos conocidos los siguientes conjuntos numéricos:
  $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ Los enteros
  $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ Los naturales
  $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ Los enteros positivos
- Dados $n, m \in \mathbb{Z}$, se dice que n divide a m, y se denota $n|m$, si:

$$n|m \equiv \exists q \in \mathbb{Z}| : m = nq$$

  Se dice también que:
  n es un divisor de m
  m es un múltiplo de n
- Ejemplos:
  Teo:$3|12$: $true \equiv 12 = 3 \times 4 \implies \exists q \in \mathbb{Z}| : 12 = 3q \equiv 3|12$
  Teo:$3|-12$: $true \equiv -12 = 3 \times -4 \implies \exists q \in \mathbb{Z}| : -12 = 3q \equiv 3|-12$
  Teo:$4|24$: $true \equiv 24 = 4 \times 6 \implies \exists q \in \mathbb{Z}| : 24 = 4q \equiv 4|24$

Divisibilidad: definiciones

- En adelante, supondremos conocidos los siguientes conjuntos numéricos:
  $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ Los enteros
  $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ Los naturales
  $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ Los enteros positivos
- Dados $n, m \in \mathbb{Z}$, se dice que n divide a m, y se denota $n|m$, si:

  $$n|m \equiv \exists q \in \mathbb{Z}| : m = nq$$

  Se dice también que:
  n es un divisor de m
  m es un múltiplo de n
- Ejemplos:
  Teo:$3|12$: $true \equiv 12 = 3 \times 4 \implies \exists q \in \mathbb{Z}| : 12 = 3q \equiv 3|12$
  Teo:$3|-12$: $true \equiv -12 = 3 \times -4 \implies \exists q \in \mathbb{Z}| : -12 = 3q \equiv 3|-12$
  Teo:$4|24$: $true \equiv 24 = 4 \times 6 \implies \exists q \in \mathbb{Z}| : 24 = 4q \equiv 4|24$

Divisibilidad: definiciones

- En adelante, supondremos conocidos los siguientes conjuntos numéricos:
  $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ Los enteros
  $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ Los naturales
  $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ Los enteros positivos
- Dados $n, m \in \mathbb{Z}$, se dice que n divide a m, y se denota $n|m$, si:

  $$n|m \equiv \exists q \in \mathbb{Z}| : m = nq$$

  Se dice también que:
  n es un divisor de m
  m es un múltiplo de n
- Ejemplos:
  Teo:$3|12$: $true \equiv 12 = 3 \times 4 \implies \exists q \in \mathbb{Z}| : 12 = 3q \equiv 3|12$
  Teo:$3|-12$: $true \equiv -12 = 3 \times -4 \implies \exists q \in \mathbb{Z}| : -12 = 3q \equiv 3|-12$
  Teo:$4|24$: $true \equiv 24 = 4 \times 6 \implies \exists q \in \mathbb{Z}| : 24 = 4q \equiv 4|24$

Plan

Divisibilidad: teoremas (1)

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

$$a|b \wedge a|c \implies a|(b+c)$$

Teo-1:	$a\|b \wedge a\|c \implies a\|(b+c)$	
Hip.:	$H_1 : a\|b,\ H_2 : a\|c$	
	Exp.	Just.
1	$a\|b$	Hipótesis H_1
2	$\exists q \in \mathbb{Z}\| : b = aq$	Definición de $\|$ en (1)
3	$b = aq_1$	Instanciación existencial de (2)
4	$a\|c$	Hipótesis H_2
5	$\exists q \in \mathbb{Z}\| : c = aq$	Definición de $\|$ en (4)
6	$c = aq_2$	Instanciación existencial de (5)
7	$b + c = (aq_1 + aq_2)$	Aritmética (3),(6)
8	$b + c = a(q_1 + q_2)$	Factorización (7)
9	$a\|(b+c)$	Definición $\|$ sobre (8)
		$\diamond$

Divisibilidad: teoremas (1)

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

$$a|b \wedge a|c \implies a|(b+c)$$

Teo-1:	$a\|b \wedge a\|c \implies a\|(b+c)$	
Hip.:	$H_1 : a\|b,\ H_2 : a\|c$	
	Exp.	Just.
1	$a\|b$	Hipótesis H_1
2	$\exists q \in \mathbb{Z}\| : b = aq$	Definición de | en (1)
3	$b = aq_1$	Instanciación existencial de (2)
4	$a\|c$	Hipótesis H_2
5	$\exists q \in \mathbb{Z}\| : c = aq$	Definición de | en (4)
6	$c = aq_2$	Instanciación existencial de (5)
7	$b + c = (aq_1 + aq_2)$	Aritmética (3),(6)
8	$b + c = a(q_1 + q_2)$	Factorización (7)
9	$a\|(b+c)$	Definición | sobre (8)
		$\diamond$

Divisibilidad: teoremas (2)

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

$$a|b \implies \forall c| : a|bc$$

Teo-2:	$a\|b \implies \forall c\| : a\|bc$	
Hip.:	$H_1 : a\|b$	
	Exp.	Just.
1	$a\|b$	Hipótesis H_1
2	$\exists q \in \mathbb{Z}\| : b = aq$	Definición de $\|$ en (1)
3	$b = aq_1$	Instanciación existencial de (2)
4	$bc = a(q_1 c)$	Multiplicar por c arbitrario a ambos lados de (3)
5	$a\|(bc)$	Definición de $\|$, $q_1 c \in \mathbb{Z}$
6	$\forall c\| : a\|bc$	Generalización universal, c arbitrario
		$\diamond$

Divisibilidad: teoremas (2)

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

$$a|b \implies \forall c| : a|bc$$

Teo-2:	$a\|b \implies \forall c\| : a\|bc$	
Hip.:	$H_1 : a\|b$	
	Exp.	Just.
1	$a\|b$	Hipótesis H_1
2	$\exists q \in \mathbb{Z}\| : b = aq$	Definición de $\|$ en (1)
3	$b = aq_1$	Instanciación existencial de (2)
4	$bc = a(q_1c)$	Multiplicar por c arbitrario a ambos lados de (3)
5	$a\|(bc)$	Definición de $\|$, $q_1c \in \mathbb{Z}$
6	$\forall c\| : a\|bc$	Generalización universal, c arbitrario
		$\diamond$

Divisibilidad: teoremas (3)

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

$$a|b \wedge b|c \implies a|c$$

Teo-3:	$a\|b \wedge b\|c \implies a\|c$	
Hip.:	$H_1 : a\|b,\ H_2 : b\|c$	
	Exp.	Just.
1	$a\|b$	Hipótesis H_1
2	$\exists q \in \mathbb{Z}\| : b = aq$	Definición de $\|$ en (1)
3	$b = aq_1$	Instanciación existencial de (2)
4	$b\|c$	Hipótesis H_2
5	$\exists q \in \mathbb{Z}\| : c = bq$	Definición de $\|$ en (4)
6	$c = bq_2$	Instanciación existencial de (5)
7	$c = a(q_1 q_2)$	Aritmética (3),(6)
8	$a\|c$	Definición $\|$ sobre (7)
		$\diamond$

Divisibilidad: teoremas (3)

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

$$a|b \wedge b|c \implies a|c$$

Teo-3:	$a\|b \wedge b\|c \implies a\|c$	
Hip.:	$H_1 : a\|b,\ H_2 : b\|c$	
	Exp.	Just.
1	$a\|b$	Hipótesis H_1
2	$\exists q \in \mathbb{Z}\| : b = aq$	Definición de $\|$ en (1)
3	$b = aq_1$	Instanciación existencial de (2)
4	$b\|c$	Hipótesis H_2
5	$\exists q \in \mathbb{Z}\| : c = bq$	Definición de $\|$ en (4)
6	$c = bq_2$	Instanciación existencial de (5)
7	$c = a(q_1 q_2)$	Aritmética (3),(6)
8	$a\|c$	Definición $\|$ sobre (7)
		$\diamond$

Divisibilidad: teoremas (4)

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

$$a|b \wedge a|c \implies \forall m, n \in \mathbb{Z}| : a|(mb + nc)$$

Teo-4:	$a\|b \wedge a\|c \implies \forall m, n \in \mathbb{Z}\| : a\|(mb + nc)$	
Hip.:	$H_1 : a\|b,\ H_2 : a\|c$	
	Exp.	Just.
1	$a\|b$	Hipótesis H_1
2	$a\|bm$	Teo-2, m arbitrario
3	$a\|c$	Hipótesis H_2
4	$a\|cn$	Teo-2, n arbitrario
5	$a\|(bm + cn)$	Teo-1, (2) y (4)
6	$\forall m, n \in \mathbb{Z}\| : a\|(bm + cn)$	Generalización Universal (5)
		$\diamond$

Divisibilidad: teoremas (4)

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

$$a|b \wedge a|c \implies \forall m, n \in \mathbb{Z}| : a|(mb + nc)$$

Teo-4:	$a\|b \wedge a\|c \implies \forall m, n \in \mathbb{Z}\| : a\|(mb + nc)$	
Hip.:	$H_1 : a\|b,\ H_2 : a\|c$	
	Exp.	Just.
1	$a\|b$	Hipótesis H_1
2	$a\|bm$	Teo-2, m arbitrario
3	$a\|c$	Hipótesis H_2
4	$a\|cn$	Teo-2, n arbitrario
5	$a\|(bm + cn)$	Teo-1, (2) y (4)
6	$\forall m, n \in \mathbb{Z}\| : a\|(bm + cn)$	Generalización Universal (5)
		$\diamond$

Plan

Divisibilidad: Algoritmo de la división (1)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- El teorema anterior es conocido como el algoritmo de la división. No es en realidad un algoritmo, sino un teorema de existencia.
- n es el dividendo, d es el divisor, q es el cociente y r es el residuo de la división.
- Al cociente de la división de n en d se le denota:

$$q = n \div d$$

- Al residuo de la división de n en d se le denota:

$$r = n \mod d$$

- Por tanto

$$n = (n \div d)d + (n \mod d)$$

Divisibilidad: Algoritmo de la división (1)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- El teorema anterior es conocido como el algoritmo de la división. No es en realidad un algoritmo, sino un teorema de existencia.
- n es el dividendo, d es el divisor, q es el cociente y r es el residuo de la división.
- Al cociente de la división de n en d se le denota:

$$q = n \div d$$

- Al residuo de la división de n en d se le denota:

$$r = n \mod d$$

- Por tanto

$$n = (n \div d)d + (n \mod d)$$

Divisibilidad: Algoritmo de la división (1)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- El teorema anterior es conocido como el algoritmo de la división. No es en realidad un algoritmo, sino un teorema de existencia.
- n es el dividendo, d es el divisor, q es el cociente y r es el residuo de la división.
- Al cociente de la división de n en d se le denota:

$$q = n \div d$$

- Al residuo de la división de n en d se le denota:

$$r = n \mod d$$

- Por tanto

$$n = (n \div d)d + (n \mod d)$$

Divisibilidad: Algoritmo de la división (1)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- El teorema anterior es conocido como el algoritmo de la división. No es en realidad un algoritmo, sino un teorema de existencia.
- n es el dividendo, d es el divisor, q es el cociente y r es el residuo de la división.
- Al cociente de la división de n en d se le denota:

$$q = n \div d$$

- Al residuo de la división de n en d se le denota:

$$r = n \mod d$$

- Por tanto

$$n = (n \div d)d + (n \mod d)$$

Divisibilidad: Algoritmo de la división (1)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- El teorema anterior es conocido como el algoritmo de la división. No es en realidad un algoritmo, sino un teorema de existencia.
- n es el dividendo, d es el divisor, q es el cociente y r es el residuo de la división.
- Al cociente de la división de n en d se le denota:

$$q = n \div d$$

- Al residuo de la división de n en d se le denota:

$$r = n \mod d$$

- Por tanto

$$n = (n \div d)d + (n \mod d)$$

Divisibilidad: Algoritmo de la división (1)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- El teorema anterior es conocido como el algoritmo de la división. No es en realidad un algoritmo, sino un teorema de existencia.
- n es el dividendo, d es el divisor, q es el cociente y r es el residuo de la división.
- Al cociente de la división de n en d se le denota:

$$q = n \div d$$

- Al residuo de la división de n en d se le denota:

$$r = n \mod d$$

- Por tanto

$$n = (n \div d)d + (n \mod d)$$

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$
  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$
- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$

- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$

  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$

- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$

- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$
  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$
- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$
- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$
  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$
- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$
- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$
  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$
- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$

- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$
  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$
- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$
  $-11 = 4 \times 0 + (-11)$
  $-11 = 4 \times -1 + (-7)$
  $-11 = 4 \times -2 + (-3)$
  $-11 = 4 \times -3 + 1$
  $q = -11 \div 4 = -3$ y $r = -11 \mod 4 = 1$
- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$
  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$
- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$
  $-11 = 4 \times 0 + (-11)$
  $-11 = 4 \times -1 + (-7)$
  $-11 = 4 \times -2 + (-3)$
  $-11 = 4 \times -3 + 1$
  $q = -11 \div 4 = -3$ y $r = -11 \mod 4 = 1$
- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$
  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$
- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$
  $-11 = 4 \times 0 + (-11)$
  $-11 = 4 \times -1 + (-7)$
  $-11 = 4 \times -2 + (-3)$
  $-11 = 4 \times -3 + 1$
  $q = -11 \div 4 = -3$ y $r = -11 \mod 4 = 1$
- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$
  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$
- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$
  $-11 = 4 \times 0 + (-11)$
  $-11 = 4 \times -1 + (-7)$
  $-11 = 4 \times -2 + (-3)$
  $-11 = 4 \times -3 + 1$
  $q = -11 \div 4 = -3$ y $r = -11 \mod 4 = 1$
- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$
  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$
- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$
  $-11 = 4 \times 0 + (-11)$
  $-11 = 4 \times -1 + (-7)$
  $-11 = 4 \times -2 + (-3)$
  $-11 = 4 \times -3 + 1$
  $q = -11 \div 4 = -3$ y $r = -11 \mod 4 = 1$
- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^{+}$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$
  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$
- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$
  $-11 = 4 \times 0 + (-11)$
  $-11 = 4 \times -1 + (-7)$
  $-11 = 4 \times -2 + (-3)$
  $-11 = 4 \times -3 + 1$
  $q = -11 \div 4 = -3$ y $r = -11 \mod 4 = 1$
- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$
  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$
- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$
  $-11 = 4 \times 0 + (-11)$
  $-11 = 4 \times -1 + (-7)$
  $-11 = 4 \times -2 + (-3)$
  $-11 = 4 \times -3 + 1$
  $q = -11 \div 4 = -3$ y $r = -11 \mod 4 = 1$
- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$
  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$
- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$
  $-11 = 4 \times 0 + (-11)$
  $-11 = 4 \times -1 + (-7)$
  $-11 = 4 \times -2 + (-3)$
  $-11 = 4 \times -3 + 1$
  $q = -11 \div 4 = -3$ y $r = -11 \mod 4 = 1$
- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Divisibilidad: Algoritmo de la división (2)

Dados $n \in \mathbb{Z}, d \in \mathbb{N}^+$.

$$\exists q, r | 0 \leq r < d : n = qd + r$$

y q y r son únicos

- Si $n = 35$ y $d = 11$, calcule $q = n \div d$ y $r = n \mod d$
  $35 = 11 \times 0 + 35$
  $35 = 11 \times 1 + 24$
  $35 = 11 \times 2 + 13$
  $35 = 11 \times 3 + 2$
  $q = 35 \div 11 = 3$ y $r = 35 \mod 11 = 2$
- Si $n = -11$ y $d = 4$, calcule $q = n \div d$ y $r = n \mod d$
  $-11 = 4 \times 0 + (-11)$
  $-11 = 4 \times -1 + (-7)$
  $-11 = 4 \times -2 + (-3)$
  $-11 = 4 \times -3 + 1$
  $q = -11 \div 4 = -3$ y $r = -11 \mod 4 = 1$
- ¿Se les ocurre un algoritmo para calcular q y r dados n y d?

Cómo calcular la representación de $\mathbb{N}$ en base b

Con el algoritmo de la división, podemos calcular la representación de n en base b así:

- Aplicar el algoritmo de la división a n y b:

$$n = q_0 * b + a_0, 0 \leq a_0 < b$$

  a_0 es el símbolo más a la derecha de la expansión de n en base b

- Aplicar el algoritmo de la división a q_0 y b:

$$q_0 = q_1 * b + a_1, 0 \leq a_1 < b$$

  a_1 es el segundo símbolo de derecha a izquierda de la expansión de n en base b

- Continuar el proceso encontrando:

$$(q_0, a_0), (q_1, a_1), \ldots (q_k, a_k)$$

  donde $q_k = 0$. Entonces

$$n = (a_k a_{k-1} \ldots a_0)_b$$

Cómo calcular la representación de $\mathbb{N}$ en base b

Con el algoritmo de la división, podemos calcular la representación de n en base b así:

- Aplicar el algoritmo de la división a n y b:

$$n = q_0 * b + a_0, 0 \leq a_0 < b$$

  a_0 es el símbolo más a la derecha de la expansión de n en base b

- Aplicar el algoritmo de la división a q_0 y b:

$$q_0 = q_1 * b + a_1, 0 \leq a_1 < b$$

  a_1 es el segundo símbolo de derecha a izquierda de la expansión de n en base b

- Continuar el proceso encontrando:

$$(q_0, a_0), (q_1, a_1), \ldots (q_k, a_k)$$

  donde $q_k = 0$. Entonces

$$n = (a_k a_{k-1} \ldots a_0)_b$$

Cómo calcular la representación de $\mathbb{N}$ en base b

Con el algoritmo de la división, podemos calcular la representación de n en base b así:

- Aplicar el algoritmo de la división a n y b:

  $$n = q_0 * b + a_0, 0 \leq a_0 < b$$

  a_0 es el símbolo más a la derecha de la expansión de n en base b
- Aplicar el algoritmo de la división a q_0 y b:

  $$q_0 = q_1 * b + a_1, 0 \leq a_1 < b$$

  a_1 es el segundo símbolo de derecha a izquierda de la expansión de n en base b
- Continuar el proceso encontrando:

  $$(q_0, a_0), (q_1, a_1), \ldots (q_k, a_k)$$

  donde $q_k = 0$. Entonces

  $$n = (a_k a_{k-1} \ldots a_0)_b$$

Ejemplos de cálculos de representaciones en diferentes bases

12345 en base 8
$12345 = 8 \times (1543) + 1$
$1543 = 8 \times (192) + 7$
$192 = 8 \times (24) + 0$
$24 = 8 \times (3) + 0$
$3 = 8 \times (0) + 3$
Por tanto $12345 = (30071)_8$

177130 en base 16
$177130 = 16 \times (11070) + 10$
$11070 = 16 \times (691) + 14$
$691 = 16 \times (43) + 3$
$43 = 16 \times (2) + 11$
$2 = 16 \times (0) + 2$
Por tanto $177130 = (2B3EA)_{16}$

241 en base 2
$241 = 2 \times (120) + 1$
$120 = 2 \times (60) + 0$
$60 = 2 \times (30) + 0$
$30 = 2 \times (15) + 0$
$15 = 2 \times (7) + 1$
$7 = 2 \times (3) + 1$
$3 = 2 \times (1) + 1$
$1 = 2 \times (0) + 1$
Por tanto $241 = (11110001)_2$
[Socrative]

Ejemplos de cálculos de representaciones en diferentes bases

12345 en base 8
$12345 = 8 \times (1543) + 1$
$1543 = 8 \times (192) + 7$
$192 = 8 \times (24) + 0$
$24 = 8 \times (3) + 0$
$3 = 8 \times (0) + 3$
Por tanto $12345 = (30071)_8$
177130 en base 16
$177130 = 16 \times (11070) + 10$
$11070 = 16 \times (691) + 14$
$691 = 16 \times (43) + 3$
$43 = 16 \times (2) + 11$
$2 = 16 \times (0) + 2$
Por tanto $177130 = (2B3EA)_{16}$

241 en base 2
$241 = 2 \times (120) + 1$
$120 = 2 \times (60) + 0$
$60 = 2 \times (30) + 0$
$30 = 2 \times (15) + 0$
$15 = 2 \times (7) + 1$
$7 = 2 \times (3) + 1$
$3 = 2 \times (1) + 1$
$1 = 2 \times (0) + 1$
Por tanto $241 = (11110001)_2$
[Socrative]

Ejemplos de cálculos de representaciones en diferentes bases

12345 en base 8

$12345 = 8 \times (1543) + 1$
$1543 = 8 \times (192) + 7$
$192 = 8 \times (24) + 0$
$24 = 8 \times (3) + 0$
$3 = 8 \times (0) + 3$

Por tanto $12345 = (30071)_8$

177130 en base 16

$177130 = 16 \times (11070) + 10$
$11070 = 16 \times (691) + 14$
$691 = 16 \times (43) + 3$
$43 = 16 \times (2) + 11$
$2 = 16 \times (0) + 2$

Por tanto $177130 = (2B3EA)_{16}$

241 en base 2

$241 = 2 \times (120) + 1$
$120 = 2 \times (60) + 0$
$60 = 2 \times (30) + 0$
$30 = 2 \times (15) + 0$
$15 = 2 \times (7) + 1$
$7 = 2 \times (3) + 1$
$3 = 2 \times (1) + 1$
$1 = 2 \times (0) + 1$

Por tanto $241 = (11110001)_2$

[Socrative]

Ejemplos de cálculos de representaciones en diferentes bases

12345 en base 8
$12345 = 8 \times (1543) + 1$
$1543 = 8 \times (192) + 7$
$192 = 8 \times (24) + 0$
$24 = 8 \times (3) + 0$
$3 = 8 \times (0) + 3$
Por tanto $12345 = (30071)_8$
177130 en base 16
$177130 = 16 \times (11070) + 10$
$11070 = 16 \times (691) + 14$
$691 = 16 \times (43) + 3$
$43 = 16 \times (2) + 11$
$2 = 16 \times (0) + 2$
Por tanto $177130 = (2B3EA)_{16}$

241 en base 2
$241 = 2 \times (120) + 1$
$120 = 2 \times (60) + 0$
$60 = 2 \times (30) + 0$
$30 = 2 \times (15) + 0$
$15 = 2 \times (7) + 1$
$7 = 2 \times (3) + 1$
$3 = 2 \times (1) + 1$
$1 = 2 \times (0) + 1$
Por tanto $241 = (11110001)_2$
[Socrative]

Plan

Números primos

- Un número primo es un número natural, mayor que 1 que solo es divisible por 1 y por él mismo:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- $2, 3, 5, 7, 11, 13, 17, 19$ son números primos.
- Si un número n no es primo, se dice que es un número compuesto. $4, 6, 8, 9, 10, 12, 14, 15, 16, 18$ son números compuestos.
- Muchas de las aplicaciones prácticas de los primos se basan en decidir, de manera eficiente, si un número es o no primo y, de manera relacionada, cuando un número no es primo, descubrir cómo puede factorizarse.

Números primos

- Un número primo es un número natural, mayor que 1 que solo es divisible por 1 y por él mismo:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d | p : d = 1 \vee d = p)$$

- $2, 3, 5, 7, 11, 13, 17, 19$ son números primos.
- Si un número n no es primo, se dice que es un número compuesto. $4, 6, 8, 9, 10, 12, 14, 15, 16, 18$ son números compuestos.
- Muchas de las aplicaciones prácticas de los primos se basan en decidir, de manera eficiente, si un número es o no primo y, de manera relacionada, cuando un número no es primo, descubrir cómo puede factorizarse.

Números primos

- Un número primo es un número natural, mayor que 1 que solo es divisible por 1 y por él mismo:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- $2, 3, 5, 7, 11, 13, 17, 19$ son números primos.
- Si un número n no es primo, se dice que es un número compuesto. $4, 6, 8, 9, 10, 12, 14, 15, 16, 18$ son números compuestos.
- Muchas de las aplicaciones prácticas de los primos se basan en decidir, de manera eficiente, si un número es o no primo y, de manera relacionada, cuando un número no es primo, descubrir cómo puede factorizarse.

Números primos

- Un número primo es un número natural, mayor que 1 que solo es divisible por 1 y por él mismo:

$$p \text{ es primo} \equiv p > 1 \land (\forall d \in \mathbb{N} | d > 0 \land d | p : d = 1 \lor d = p)$$

- $2, 3, 5, 7, 11, 13, 17, 19$ son números primos.
- Si un número n no es primo, se dice que es un número compuesto. $4, 6, 8, 9, 10, 12, 14, 15, 16, 18$ son números compuestos.
- Muchas de las aplicaciones prácticas de los primos se basan en decidir, de manera eficiente, si un número es o no primo y, de manera relacionada, cuando un número no es primo, descubrir cómo puede factorizarse.

¿Cómo verificar si un número es primo?

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d | p : d = 1 \vee d = p)$$

- Observemos lo siguiente:
  - $d | m \wedge d \neq 0 \implies d \leq m$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d < p : \neg(d|p)$$

  - $p \neq 2$ es primo $\implies$ p es impar

- ¿29 es primo?
- Y 123? Y 9827? Y 87789456785423451? Y 87789456785432343?

¿Cómo verificar si un número es primo?

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \land (\forall d \in \mathbb{N} | d > 0 \land d | p : d = 1 \lor d = p)$$

- Observemos lo siguiente:
  - $d|m \land d \neq 0 \implies d \leq m$. O sea,

$$p \text{ es primo} \equiv p = 2 \lor \forall d \in \mathbb{N} | 2 \leq d < p : \neg(d|p)$$

  - $p \neq 2$ es primo $\implies p$ es impar
  - $d * k | n \implies d | n$. O sea,

$$p \text{ es primo} \equiv p = 2 \lor \forall d \in \mathbb{N} | 2 \leq d < p \land primo(d) : \neg(d|p)$$

  - $n = d * k \land d \leq k \implies d \leq \sqrt{n}$. O sea,

$$p \text{ es primo} \equiv p = 2 \lor \forall d \in \mathbb{N} | 2 \leq d \leq \sqrt{n} \land primo(d) : \neg(d|p)$$

- ¿29 es primo?
- Y 123? Y 9827? Y 8778945678543234511? Y 877894567854323437?

¿Cómo verificar si un número es primo?

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Observemos lo siguiente:
  - $d|m \wedge d \neq 0 \implies d \leq m$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N}|2 \leq d < p : \neg(d|p)$$

  - $p \neq 2$ es primo $\implies$ p es impar
  - $d * k|n \implies d|n$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N}|2 \leq d < p \wedge primo(d) : \neg(d|p)$$

  - $n = d * k \wedge d \leq k \implies d \leq \sqrt{n}$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N}|2 \leq d \leq \sqrt{n} \wedge primo(d) : \neg(d|p)$$

- ¿29 es primo?
- Y 123? Y 9827? Y 877894567854323451? Y 87789456785432343?

¿Cómo verificar si un número es primo?

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Observemos lo siguiente:
  - $d|m \wedge d \neq 0 \implies d \leq m$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d < p : \neg(d|p)$$

  - $p \neq 2$ es primo $\implies p$ es impar
  - $d * k | n \implies d | n$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d < p \wedge primo(d) : \neg(d|p)$$

  - $n = d * k \wedge d \leq k \implies d \leq \sqrt{n}$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d \leq \sqrt{n} \wedge primo(d) : \neg(d|p)$$

    Nótese que si $(d > \sqrt{n} \wedge k \geq d) \implies n = d * k > \sqrt{n} * \sqrt{n} = n$ es falso por tanto $d \leq \sqrt{n}$

- ¿29 es primo?
- Y 123? Y 9827? Y 877894567854323451? Y 877894567854323437?

¿Cómo verificar si un número es primo?

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \land (\forall d \in \mathbb{N} | d > 0 \land d|p : d = 1 \lor d = p)$$

- Observemos lo siguiente:
  - $d|m \land d \neq 0 \implies d \leq m$. O sea,

  $$p \text{ es primo} \equiv p = 2 \lor \forall d \in \mathbb{N} | 2 \leq d < p : \neg(d|p)$$

  - $p \neq 2$ es primo $\implies p$ es impar
  - $d * k | n \implies d|n$. O sea,

  $$p \text{ es primo} \equiv p = 2 \lor \forall d \in \mathbb{N} | 2 \leq d < p \land primo(d) : \neg(d|p)$$

  - $n = d * k \land d \leq k \implies d \leq \sqrt{n}$. O sea,

  $$p \text{ es primo} \equiv p = 2 \lor \forall d \in \mathbb{N} | 2 \leq d \leq \sqrt{n} \land primo(d) : \neg(d|p)$$

  Nótese que si $(d > \sqrt{n} \land k \geq d) \implies n = d * k > \sqrt{n} * \sqrt{n} = n \equiv false$

  por tanto $d \leq \sqrt{n}$

- ¿29 es primo?
- Y 123? Y 9827? Y 87789456785423451? Y 87789456785432343?

¿Cómo verificar si un número es primo?

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Observemos lo siguiente:
  - $d|m \wedge d \neq 0 \implies d \leq m$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d < p : \neg(d|p)$$

  - $p \neq 2$ es primo $\implies p$ es impar
  - $d * k|n \implies d|n$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d < p \wedge primo(d) : \neg(d|p)$$

  - $n = d * k \wedge d \leq k \implies d \leq \sqrt{n}$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d \leq \sqrt{n} \wedge primo(d) : \neg(d|p)$$

    Nótese que si $(d > \sqrt{n} \wedge k \geq d) \implies n = d * k > \sqrt{n} * \sqrt{n} = n \equiv false$

    por tanto $d \leq \sqrt{n}$

- ¿29 es primo?
- Y 123? Y 9827? Y 877894567854323451? Y 87789456785432343?

¿Cómo verificar si un número es primo?

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Observemos lo siguiente:
  - $d|m \wedge d \neq 0 \implies d \leq m$. O sea,

    $$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d < p : \neg(d|p)$$

  - $p \neq 2$ es primo $\implies p$ es impar
  - $d * k|n \implies d|n$. O sea,

    $$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d < p \wedge primo(d) : \neg(d|p)$$

  - $n = d * k \wedge d \leq k \implies d \leq \sqrt{n}$. O sea,

    $$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d \leq \sqrt{n} \wedge primo(d) : \neg(d|p)$$

    Nótese que si $(d > \sqrt{n} \wedge k \geq d) \implies n = d * k > \sqrt{n} * \sqrt{n} = n \equiv false$

    por tanto $d \leq \sqrt{n}$
- ¿29 es primo? Basta con mirar si es divisible por algún primo menor o igual a 5
- Y 123? Y 9827? Y 877894567854323451? Y 87789456785432343?

¿Cómo verificar si un número es primo?

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Observemos lo siguiente:
  - $d|m \wedge d \neq 0 \implies d \leq m$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d < p : \neg(d|p)$$

  - $p \neq 2$ es primo $\implies p$ es impar
  - $d * k|n \implies d|n$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d < p \wedge primo(d) : \neg(d|p)$$

  - $n = d * k \wedge d \leq k \implies d \leq \sqrt{n}$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d \leq \sqrt{n} \wedge primo(d) : \neg(d|p)$$

  Nótese que si $(d > \sqrt{n} \wedge k \geq d) \implies n = d * k > \sqrt{n} * \sqrt{n} = n \equiv false$

  por tanto $d \leq \sqrt{n}$

- ¿29 es primo? Basta con mirar si es divisible por algún primo menor o igual a 5
- Y 123? Y 9827? Y 877894567854323451? Y 87789456785432343?

¿Cómo verificar si un número es primo?

- Recordemos:

$$p \text{ es primo } \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d | p : d = 1 \vee d = p)$$

- Observemos lo siguiente:
  - $d|m \wedge d \neq 0 \implies d \leq m$. O sea,

$$p \text{ es primo } \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d < p : \neg(d|p)$$

  - $p \neq 2$ es primo $\implies p$ es impar
  - $d * k | n \implies d | n$. O sea,

$$p \text{ es primo } \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d < p \wedge primo(d) : \neg(d|p)$$

  - $n = d * k \wedge d \leq k \implies d \leq \sqrt{n}$. O sea,

$$p \text{ es primo } \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d \leq \sqrt{n} \wedge primo(d) : \neg(d|p)$$

  Nótese que si $(d > \sqrt{n} \wedge k \geq d) \implies n = d * k > \sqrt{n} * \sqrt{n} = n \equiv false$

  por tanto $d \leq \sqrt{n}$

- ¿29 es primo? Basta con mirar si es divisible por algún primo menor o igual a 5
- Y 123? Y 9827? Y 877894567854323451? Y 87789456785432343?

¿Cómo verificar si un número es primo?

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Observemos lo siguiente:
  - $d|m \wedge d \neq 0 \implies d \leq m$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d < p : \neg(d|p)$$

  - $p \neq 2$ es primo $\implies p$ es impar
  - $d * k|n \implies d|n$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d < p \wedge primo(d) : \neg(d|p)$$

  - $n = d * k \wedge d \leq k \implies d \leq \sqrt{n}$. O sea,

$$p \text{ es primo} \equiv p = 2 \vee \forall d \in \mathbb{N} | 2 \leq d \leq \sqrt{n} \wedge primo(d) : \neg(d|p)$$

  Nótese que si $(d > \sqrt{n} \wedge k \geq d) \implies n = d * k > \sqrt{n} * \sqrt{n} = n \equiv false$

  por tanto $d \leq \sqrt{n}$

- ¿29 es primo? Basta con mirar si es divisible por algún primo menor o igual a 5
- Y 123? Y 9827? Y 877894567854323451? Y 877894567854323437?

El teorema fundamental de la aritmética

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Teorema fundamental de la aritmética: Todo número natural mayor que 1, se puede expresar de manera única como producto de números primos. Si los primos se presentan en orden ascendente, esta descomposición es única.

$$\forall n \in \mathbb{N} \exists k \in \mathbb{N} \exists p_1, p_2, \ldots, p_k \in \mathbb{N} | primo(p_1) \wedge \ldots \wedge primo(p_k) :$$

$$(p_1 \leq p_2 \leq \ldots \leq p_k) \wedge (n = p_1 p_2 \ldots p_k)$$

- Por ejemplo:
  - $100 = 2 \ast 2 \ast 5 \ast 5 = 2^2 \ast 5^2$
    $641 = 641$
    $999 = 3 \ast 3 \ast 3 \ast 37 = 3^3 \ast 37$
    $1024 = 2 \ast 2 \ast 2 \ast 2 \ast 2 \ast 2 \ast 2 \ast 2 \ast 2 \ast 2 = 2^{10}$
- ¿Y 7007?

El teorema fundamental de la aritmética

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Teorema fundamental de la aritmética: Todo número natural mayor que 1, se puede expresar de manera única como producto de números primos. Si los primos se presentan en orden ascendente, esta descomposición es única.

$$\forall n \in \mathbb{N} \exists k \in \mathbb{N} \exists p_1, p_2, \ldots, p_k \in \mathbb{N} | primo(p_1) \wedge \ldots \wedge primo(p_k) :$$

$$(p_1 \leq p_2 \leq \ldots \leq p_k) \wedge (n = p_1 p_2 \ldots p_k)$$

- Por ejemplo:
  - $100 = 2 * 2 * 5 * 5 = 2^2 * 5^2$
  - $641 = 641$
  - $999 = 3 * 3 * 3 * 37 = 3^3 * 37$
  - $1024 = 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 = 2^{10}$
- ¿Y 7007?

El teorema fundamental de la aritmética

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Teorema fundamental de la aritmética: Todo número natural mayor que 1, se puede expresar de manera única como producto de números primos. Si los primos se presentan en orden ascendente, esta descomposición es única.

$$\forall n \in \mathbb{N} \exists k \in \mathbb{N} \exists p_1, p_2, \ldots, p_k \in \mathbb{N} | primo(p_1) \wedge \ldots \wedge primo(p_k) :$$

$$(p_1 \leq p_2 \leq \ldots \leq p_k) \wedge (n = p_1 p_2 \ldots p_k)$$

- Por ejemplo:
  - $100 = 2 * 2 * 5 * 5 = 2^2 * 5^2$
  - $641 = 641$
  - $999 = 3 * 3 * 3 * 37 = 3^3 * 37$
  - $1024 = 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 = 2^{10}$
- ¿Y 7007?

El teorema fundamental de la aritmética

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Teorema fundamental de la aritmética: Todo número natural mayor que 1, se puede expresar de manera única como producto de números primos. Si los primos se presentan en orden ascendente, esta descomposición es única.

$$\forall n \in \mathbb{N} \exists k \in \mathbb{N} \exists p_1, p_2, \ldots, p_k \in \mathbb{N} | primo(p_1) \wedge \ldots \wedge primo(p_k) :$$

$$(p_1 \leq p_2 \leq \ldots \leq p_k) \wedge (n = p_1 p_2 \ldots p_k)$$

- Por ejemplo:
  - $100 = 2 * 2 * 5 * 5 = 2^2 * 5^2$
  - $641 = 641$
  - $999 = 3 * 3 * 3 * 37 = 3^3 * 37$
  - $1024 = 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 = 2^{10}$
- ¿Y 7007?

El teorema fundamental de la aritmética

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Teorema fundamental de la aritmética: Todo número natural mayor que 1, se puede expresar de manera única como producto de números primos. Si los primos se presentan en orden ascendente, esta descomposición es única.

$$\forall n \in \mathbb{N} \exists k \in \mathbb{N} \exists p_1, p_2, \ldots, p_k \in \mathbb{N} | primo(p_1) \wedge \ldots \wedge primo(p_k) :$$

$$(p_1 \leq p_2 \leq \ldots \leq p_k) \wedge (n = p_1 p_2 \ldots p_k)$$

- Por ejemplo:
  - $100 = 2 * 2 * 5 * 5 = 2^2 * 5^2$
  - $641 = 641$
  - $999 = 3 * 3 * 3 * 37 = 3^3 * 37$
  - $1024 = 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 = 2^{10}$
- ¿Y 7007?

El teorema fundamental de la aritmética

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Teorema fundamental de la aritmética: Todo número natural mayor que 1, se puede expresar de manera única como producto de números primos. Si los primos se presentan en orden ascendente, esta descomposición es única.

$$\forall n \in \mathbb{N} \exists k \in \mathbb{N} \exists p_1, p_2, \ldots, p_k \in \mathbb{N} | primo(p_1) \wedge \ldots \wedge primo(p_k) :$$

$$(p_1 \leq p_2 \leq \ldots \leq p_k) \wedge (n = p_1 p_2 \ldots p_k)$$

- Por ejemplo:
  - $100 = 2 * 2 * 5 * 5 = 2^2 * 5^2$
  - $641 = 641$
  - $999 = 3 * 3 * 3 * 37 = 3^3 * 37$
  - $1024 = 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 = 2^{10}$
- ¿Y 7007? ¿Se les ocurre algún método para encontrar los factores primos?

El teorema fundamental de la aritmética

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d | p : d = 1 \vee d = p)$$

- Teorema fundamental de la aritmética: Todo número natural mayor que 1, se puede expresar de manera única como producto de números primos. Si los primos se presentan en orden ascendente, esta descomposición es única.

$$\forall n \in \mathbb{N} \exists k \in \mathbb{N} \exists p_1, p_2, \ldots, p_k \in \mathbb{N} | primo(p_1) \wedge \ldots \wedge primo(p_k) :$$

$$(p_1 \leq p_2 \leq \ldots \leq p_k) \wedge (n = p_1 p_2 \ldots p_k)$$

- Por ejemplo:
  - $100 = 2 * 2 * 5 * 5 = 2^2 * 5^2$
  - $641 = 641$
  - $999 = 3 * 3 * 3 * 37 = 3^3 * 37$
  - $1024 = 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 = 2^{10}$
- ¿Y 7007? ¿Se les ocurre algún método para encontrar los factores primos?

El teorema fundamental de la aritmética

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Teorema fundamental de la aritmética: Todo número natural mayor que 1, se puede expresar de manera única como producto de números primos. Si los primos se presentan en orden ascendente, esta descomposición es única.

$$\forall n \in \mathbb{N} \exists k \in \mathbb{N} \exists p_1, p_2, \ldots, p_k \in \mathbb{N} | primo(p_1) \wedge \ldots \wedge primo(p_k) :$$

$$(p_1 \leq p_2 \leq \ldots \leq p_k) \wedge (n = p_1 p_2 \ldots p_k)$$

- Por ejemplo:
  - $100 = 2 * 2 * 5 * 5 = 2^2 * 5^2$
  - $641 = 641$
  - $999 = 3 * 3 * 3 * 37 = 3^3 * 37$
  - $1024 = 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 = 2^{10}$
- ¿Y 7007? ¿Se les ocurre algún método para encontrar los factores primos?

El teorema fundamental de la aritmética

- Recordemos:

$$p \text{ es primo} \equiv p > 1 \wedge (\forall d \in \mathbb{N} | d > 0 \wedge d|p : d = 1 \vee d = p)$$

- Teorema fundamental de la aritmética: Todo número natural mayor que 1, se puede expresar de manera única como producto de números primos. Si los primos se presentan en orden ascendente, esta descomposición es única.

$$\forall n \in \mathbb{N} \exists k \in \mathbb{N} \exists p_1, p_2, \ldots, p_k \in \mathbb{N} | primo(p_1) \wedge \ldots \wedge primo(p_k) :$$

$$(p_1 \leq p_2 \leq \ldots \leq p_k) \wedge (n = p_1 p_2 \ldots p_k)$$

- Por ejemplo:
  - $100 = 2 * 2 * 5 * 5 = 2^2 * 5^2$
  - $641 = 641$
  - $999 = 3 * 3 * 3 * 37 = 3^3 * 37$
  - $1024 = 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 = 2^{10}$
- ¿Y 7007? ¿Se les ocurre algún método para encontrar los factores primos?

¿Cuántos primos hay?

- Teorema: Hay infinitos primos.
- Demostración: Por contradicción.
  Suponga que hay un número finito de primos: $p_1 < p_2 < \ldots < p_r$
  La idea es construir un número q que no pueda ser dividido por ninguno de esos primos. Entonces, usando el teorema fundamental de la aritmética concluimos que debe existir al menos otro primo distinto a esos r que supusimos que eran todos. Por tanto hay una contradicción.

¿Cuántos primos hay?

- Teorema: Hay infinitos primos.
- Demostración: Por contradicción.

  Suponga que hay un número finito de primos: $p_1 < p_2 < \ldots < p_r$
  La idea es construir un número q que no pueda ser dividido por ninguno de esos primos. Entonces, usando el teorema fundamental de la aritmética concluimos que debe existir al menos otro primo distinto a esos r que supusimos que eran todos. Por tanto hay una contradicción.
  Sea $q = (p_1 * p_2 * \ldots * p_r) + 1$
  Nótese que $p_j | (p_1 * p_2 * \ldots * p_r)$ para $1 \leq j \leq r$
  Entonces $p_j \not| q$. Porque si $p_j | q$ entonces $p_j | (q - (p_1 * p_2 * \ldots * p_r))$, es decir, $p_j | 1$ lo cual es imposible por ser primo.
  Por tanto, q es primo o q es divisible por un número primo distinto de $p_1, p_2, \ldots, p_r$
  En cualquier caso, existe al menos un primo más. Contradicción

¿Cuántos primos hay?

- Teorema: Hay infinitos primos.
- Demostración: Por contradicción.
  Suponga que hay un número finito de primos: $p_1 < p_2 < \ldots < p_r$
  La idea es construir un número q que no pueda ser dividido por ninguno de esos primos. Entonces, usando el teorema fundamental de la aritmética concluimos que debe existir al menos otro primo distinto a esos r que supusimos que eran todos. Por tanto hay una contradicción.
  Sea $q = (p_1 * p_2 * \ldots * p_r) + 1$
  Nótese que $p_j | (p_1 * p_2 * \ldots * p_r)$ para $1 \leq j \leq r$
  Entonces $p_j \not| q$. Porque si $p_j | q$ entonces $p_j | (q - (p_1 * p_2 * \ldots * p_r))$, es decir, $p_j | 1$ lo cual es imposible por ser primo.
  Por tanto, q es primo o q es divisible por un número primo distinto de $p_1, p_2, \ldots, p_r$
  En cualquier caso, existe al menos un primo más. Contradicción

¿Cuántos primos hay?

- Teorema: Hay infinitos primos.
- Demostración: Por contradicción.
  Suponga que hay un número finito de primos: $p_1 < p_2 < \ldots < p_r$
  La idea es construir un número q que no pueda ser dividido por ninguno de esos primos. Entonces, usando el teorema fundamental de la aritmética concluimos que debe existir al menos otro primo distinto a esos r que supusimos que eran todos. Por tanto hay una contradicción.
  Sea $q = (p_1 * p_2 * \ldots * p_r) + 1$
  Nótese que $p_j | (p_1 * p_2 * \ldots * p_r)$ para $1 \leq j \leq r$
  Entonces $p_j \not| q$ Porque si $p_j | q$ entonces $p_j | (q - (p_1 * p_2 * \ldots * p_r))$, es decir, $p_j | 1$ lo cual es imposible por ser primo.
  Por tanto, q es primo o q es divisible por un número primo distinto de $p_1, p_2, \ldots, p_r$
  En cualquier caso, existe al menos un primo más. Contradicción

¿Cuántos primos hay?

- Teorema: Hay infinitos primos.
- Demostración: Por contradicción.
  Suponga que hay un número finito de primos: $p_1 < p_2 < \ldots < p_r$
  La idea es construir un número q que no pueda ser dividido por ninguno de esos primos. Entonces, usando el teorema fundamental de la aritmética concluimos que debe existir al menos otro primo distinto a esos r que supusimos que eran todos. Por tanto hay una contradicción.
  Sea $q = (p_1 * p_2 * \ldots * p_r) + 1$
  Nótese que $p_j | (p_1 * p_2 * \ldots * p_r)$ para $1 \leq j \leq r$
  Entonces $p_j \not| q$ Porque si $p_j | q$ entonces $p_j | (q - (p_1 * p_2 * \ldots * p_r))$, es decir, $p_j | 1$ lo cual es imposible por ser primo.
  Por tanto, q es primo o q es divisible por un número primo distinto de $p_1, p_2, \ldots, p_r$
  En cualquier caso, existe al menos un primo más. Contradicción

¿Cuántos primos hay?

- Teorema: Hay infinitos primos.
- Demostración: Por contradicción.
  Suponga que hay un número finito de primos: $p_1 < p_2 < \ldots < p_r$
  La idea es construir un número q que no pueda ser dividido por ninguno de esos primos. Entonces, usando el teorema fundamental de la aritmética concluimos que debe existir al menos otro primo distinto a esos r que supusimos que eran todos. Por tanto hay una contradicción.
  Sea $q = (p_1 * p_2 * \ldots * p_r) + 1$
  Nótese que $p_j | (p_1 * p_2 * \ldots * p_r)$ para $1 \leq j \leq r$
  Entonces $p_j \not| q$ Porque si $p_j | q$ entonces $p_j | (q - (p_1 * p_2 * \ldots * p_r))$, es decir, $p_j | 1$ lo cual es imposible por ser primo.
  Por tanto, q es primo o q es divisible por un número primo distinto de $p_1, p_2, \ldots, p_r$
  En cualquier caso, existe al menos un primo más. Contradicción

¿Cuántos primos hay?

- Teorema: Hay infinitos primos.
- Demostración: Por contradicción.
  Suponga que hay un número finito de primos: $p_1 < p_2 < \ldots < p_r$
  La idea es construir un número q que no pueda ser dividido por ninguno de esos primos. Entonces, usando el teorema fundamental de la aritmética concluimos que debe existir al menos otro primo distinto a esos r que supusimos que eran todos. Por tanto hay una contradicción.
  Sea $q = (p_1 * p_2 * \ldots * p_r) + 1$
  Nótese que $p_j | (p_1 * p_2 * \ldots * p_r)$ para $1 \leq j \leq r$
  Entonces $p_j \not| q$ Porque si $p_j | q$ entonces $p_j | (q - (p_1 * p_2 * \ldots * p_r))$, es decir, $p_j | 1$ lo cual es imposible por ser primo.
  Por tanto, q es primo o q es divisible por un número primo distinto de $p_1, p_2, \ldots, p_r$
  En cualquier caso, existe al menos un primo más. Contradicción

¿Cuántos primos hay?

- Teorema: Hay infinitos primos.
- Demostración: Por contradicción.
  Suponga que hay un número finito de primos: $p_1 < p_2 < \ldots < p_r$
  La idea es construir un número q que no pueda ser dividido por ninguno de esos primos. Entonces, usando el teorema fundamental de la aritmética concluimos que debe existir al menos otro primo distinto a esos r que supusimos que eran todos. Por tanto hay una contradicción.
  Sea $q = (p_1 * p_2 * \ldots * p_r) + 1$
  Nótese que $p_j | (p_1 * p_2 * \ldots * p_r)$ para $1 \leq j \leq r$
  Entonces $p_j \not| q$ Porque si $p_j | q$ entonces $p_j | (q - (p_1 * p_2 * \ldots * p_r))$, es decir, $p_j | 1$ lo cual es imposible por ser primo.
  Por tanto, q es primo o q es divisible por un número primo distinto de $p_1, p_2, \ldots, p_r$
  En cualquier caso, existe al menos un primo más. Contradicción

¿Cuántos primos hay?

- Teorema: Hay infinitos primos.
- Demostración: Por contradicción.
  Suponga que hay un número finito de primos: $p_1 < p_2 < \ldots < p_r$
  La idea es construir un número q que no pueda ser dividido por ninguno de esos primos. Entonces, usando el teorema fundamental de la aritmética concluimos que debe existir al menos otro primo distinto a esos r que supusimos que eran todos. Por tanto hay una contradicción.
  Sea $q = (p_1 * p_2 * \ldots * p_r) + 1$
  Nótese que $p_j|(p_1 * p_2 * \ldots * p_r)$ para $1 \leq j \leq r$
  Entonces $p_j \not| q$ Porque si $p_j|q$ entonces $p_j|(q - (p_1 * p_2 * \ldots * p_r))$, es decir, $p_j|1$ lo cual es imposible por ser primo.
  Por tanto, q es primo o q es divisible por un número primo distinto de $p_1, p_2, \ldots, p_r$
  En cualquier caso, existe al menos un primo más. Contradicción

¿Cuántos primos hay?

- Teorema: Hay infinitos primos.
- Demostración: Por contradicción.
  Suponga que hay un número finito de primos: $p_1 < p_2 < \ldots < p_r$
  La idea es construir un número q que no pueda ser dividido por ninguno de esos primos. Entonces, usando el teorema fundamental de la aritmética concluimos que debe existir al menos otro primo distinto a esos r que supusimos que eran todos. Por tanto hay una contradicción.
  Sea $q = (p_1 * p_2 * \ldots * p_r) + 1$
  Nótese que $p_j|(p_1 * p_2 * \ldots * p_r)$ para $1 \leq j \leq r$
  Entonces $p_j \not| q$ Porque si $p_j|q$ entonces $p_j|(q - (p_1 * p_2 * \ldots * p_r))$, es decir, $p_j|1$ lo cual es imposible por ser primo.
  Por tanto, q es primo o q es divisible por un número primo distinto de $p_1, p_2, \ldots, p_r$
  En cualquier caso, existe al menos un primo más. Contradicción

¿Cuántos primos hay?

- Teorema: Hay infinitos primos.
- Demostración: Por contradicción.
  Suponga que hay un número finito de primos: $p_1 < p_2 < \ldots < p_r$
  La idea es construir un número q que no pueda ser dividido por ninguno de esos primos. Entonces, usando el teorema fundamental de la aritmética concluimos que debe existir al menos otro primo distinto a esos r que supusimos que eran todos. Por tanto hay una contradicción.
  Sea $q = (p_1 * p_2 * \ldots * p_r) + 1$
  Nótese que $p_j | (p_1 * p_2 * \ldots * p_r)$ para $1 \leq j \leq r$
  Entonces $p_j \not| q$ Porque si $p_j | q$ entonces $p_j | (q - (p_1 * p_2 * \ldots * p_r))$, es decir, $p_j | 1$ lo cual es imposible por ser primo.
  Por tanto, q es primo o q es divisible por un número primo distinto de $p_1, p_2, \ldots, p_r$
  En cualquier caso, existe al menos un primo más. Contradicción

Plan

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} |\ \ d|n \wedge d|m : d)$$

- ¿mcd es total? Sí, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) =$
- $mcd(6, 14) =$
- $mcd(6, 25) =$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} |\ \ n|q \wedge m|q : q)$$

- ¿mcm es total?
- $mcm(6, 18)$
- $mcm(6, 14)$
- En general, ¿se imaginan un algoritmo para calcular $mcm(n, m)$?

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} \mid \ d|n \wedge d|m : d)$$

- ¿mcd es total? Sí, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) =$ 6, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) =$
- $mcd(6, 25) =$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} \mid \ n|q \wedge m|q : q)$$

- ¿mcm es total?
- $mcm(6, 18) =$
- $mcm(6, 14) =$
- En general, ¿se imaginan un algoritmo para calcular $mcm(n, m)$?

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N}|\ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) =$
- $mcd(6, 25) =$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N}|\ \ n|q \wedge m|q : q)$$

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n,m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ tal que:

$$mcd(n,m) = (max\ d \in \mathbb{N} |\ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6,18) = 6$, porque $D_6 = \{1,2,3,6\}$, $D_{18} = \{1,2,3,6,9,18\}$, $D_6 \cap D_{18} = \{1,2,3,6\}$
- $mcd(6,14) =$
- $mcd(6,25) =$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n,m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n,m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ tal que:

$$mcm(n,m) = (min\ q \in \mathbb{N} |\ \ n|q \wedge m|q : q)$$

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} |\ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) =$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} |\ \ n|q \wedge m|q : q)$$

- ¿mcm es total?

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} |\ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) = 1$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{25} = \{1, 5, 25\}$, $D_6 \cap D_{25} = \{1\}$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} |\ \ n|q \wedge m|q : q)$$

- ¿mcm es total?
- $mcm(6, 18) =$
- $mcm(6, 14) =$
- En general, ¿se imaginan un algoritmo para calcular $mcm(n, m)$?

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} \mid \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) = 1$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{25} = \{1, 5, 25\}$, $D_6 \cap D_{25} = \{1\}$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} \mid \ n|q \wedge m|q : q)$$

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} | \ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) = 1$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{25} = \{1, 5, 25\}$, $D_6 \cap D_{25} = \{1\}$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} | \ \ n|q \wedge m|q : q)$$

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} |\ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) = 1$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{25} = \{1, 5, 25\}$, $D_6 \cap D_{25} = \{1\}$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} |\ \ n|q \wedge m|q : q)$$

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} |\ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) = 1$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{25} = \{1, 5, 25\}$, $D_6 \cap D_{25} = \{1\}$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} |\ \ n|q \wedge m|q : q)$$

- ¿mcm es total?

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} |\ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) = 1$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{25} = \{1, 5, 25\}$, $D_6 \cap D_{25} = \{1\}$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} |\ \ n|q \wedge m|q : q)$$

- ¿mcm es total?Si, porque el número de múltiplos comunes de n y m es no vacío y tiene que tener un mínimo
- $mcm(6, 18) =$
- $mcm(6, 14) =$
- En general, ¿se imaginan un algoritmo para calcular $mcm(n, m)$?

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} |\ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) = 1$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{25} = \{1, 5, 25\}$, $D_6 \cap D_{25} = \{1\}$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} |\ \ n|q \wedge m|q : q)$$

- ¿mcm es total?Si, porque el número de múltiplos comunes de n y m es no vacío y tiene que tener un mínimo
- $mcm(6, 18) =$
- $mcm(6, 14) =$
- En general, ¿se imaginan un algoritmo para calcular $mcm(n, m)$?

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} |\ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) = 1$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{25} = \{1, 5, 25\}$, $D_6 \cap D_{25} = \{1\}$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} |\ \ n|q \wedge m|q : q)$$

- ¿mcm es total?Si, porque el número de múltiplos comunes de n y m es no vacío y tiene que tener un mínimo
- $mcm(6, 18) = 18$, porque $18 = 6 \times 3 = 18 \times 1 \wedge 18 \not| 6 \times 1 \wedge 18 \not| 6 \times 2$
- $mcm(6, 14) =$
- En general, ¿se imaginan un algoritmo para calcular $mcm(n, m)$?

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N}|\ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) = 1$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{25} = \{1, 5, 25\}$, $D_6 \cap D_{25} = \{1\}$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N}|\ \ n|q \wedge m|q : q)$$

- ¿mcm es total?Si, porque el número de múltiplos comunes de n y m es no vacío y tiene que tener un mínimo
- $mcm(6, 18) = 18$, porque $18 = 6 \times 3 = 18 \times 1 \wedge 18 \not| 6 \times 1 \wedge 18 \not| 6 \times 2$
- $mcm(6, 14) =$
- En general, ¿se imaginan un algoritmo para calcular $mcm(n, m)$?

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} |\ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) = 1$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{25} = \{1, 5, 25\}$, $D_6 \cap D_{25} = \{1\}$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} |\ \ n|q \wedge m|q : q)$$

- ¿mcm es total?Si, porque el número de múltiplos comunes de n y m es no vacío y tiene que tener un mínimo
- $mcm(6, 18) = 18$, porque $18 = 6 \times 3 = 18 \times 1 \wedge 18 \nmid 6 \times 1 \wedge 18 \nmid 6 \times 2$
- $mcm(6, 14) = 42$, porque $42 = 6 \times 7 = 14 \times 3 \wedge 14 \nmid 6 \times 1 \wedge 14 \nmid 6 \times 2 \wedge 14 \nmid 6 \times 3 \wedge 14 \nmid 6 \times 4 \wedge 14 \nmid 6 \times 5 \wedge 14 \nmid 6 \times 6$
- En general, ¿se imaginan un algoritmo para calcular $mcm(n, m)$?

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} | \ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) = 1$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{25} = \{1, 5, 25\}$, $D_6 \cap D_{25} = \{1\}$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} | \ \ n|q \wedge m|q : q)$$

- ¿mcm es total?Si, porque el número de múltiplos comunes de n y m es no vacío y tiene que tener un mínimo
- $mcm(6, 18) = 18$, porque $18 = 6 \times 3 = 18 \times 1 \wedge 18 \not| 6 \times 1 \wedge 18 \not| 6 \times 2$
- $mcm(6, 14) = 42$, porque $42 = 6 \times 7 = 14 \times 3 \wedge 14 \not| 6 \times 1 \wedge 14 \not| 6 \times 2 \wedge 14 \not| 6 \times 3 \wedge 14 \not| 6 \times 4 \wedge 14 \not| 6 \times 5 \wedge 14 \not| 6 \times 6$
- En general, ¿se imaginan un algoritmo para calcular $mcm(n, m)$?

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} |\ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) = 1$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{25} = \{1, 5, 25\}$, $D_6 \cap D_{25} = \{1\}$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} |\ \ n|q \wedge m|q : q)$$

- ¿mcm es total?Si, porque el número de múltiplos comunes de n y m es no vacío y tiene que tener un mínimo
- $mcm(6, 18) = 18$, porque $18 = 6 \times 3 = 18 \times 1 \wedge 18 \nmid 6 \times 1 \wedge 18 \nmid 6 \times 2$
- $mcm(6, 14) = 42$, porque $42 = 6 \times 7 = 14 \times 3 \wedge 14 \nmid 6 \times 1 \wedge 14 \nmid 6 \times 2 \wedge 14 \nmid 6 \times 3 \wedge 14 \nmid 6 \times 4 \wedge 14 \nmid 6 \times 5 \wedge 14 \nmid 6 \times 6$
- En general, ¿se imaginan un algoritmo para calcular $mcm(n, m)$?

Divisores y múltiplos comunes

Máximo común divisor

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El máximo común divisor de n y m, $mcd(n, m)$, es el número natural d más grande que divide tanto a n como a m. Formalmente:
$mcd : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcd(n, m) = (max\ d \in \mathbb{N} |\ \ d|n \wedge d|m : d)$$

- ¿mcd es total?Si, porque el número de divisores comunes de n y m es finito y no vacío
- $mcd(6, 18) = 6$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{18} = \{1, 2, 3, 6, 9, 18\}$, $D_6 \cap D_{18} = \{1, 2, 3, 6\}$
- $mcd(6, 14) = 2$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{14} = \{1, 2, 7\}$, $D_6 \cap D_{14} = \{1, 2\}$
- $mcd(6, 25) = 1$, porque $D_6 = \{1, 2, 3, 6\}$, $D_{25} = \{1, 5, 25\}$, $D_6 \cap D_{25} = \{1\}$
- En general, ¿se imaginan un algoritmo para calcular $mcd(n, m)$?

Mínimo común múltiplo

Sean $n, m \in \mathbb{Z} \setminus \{0\}$. El mínimo común múltiplo de n y m, $mcm(n, m)$, es el número natural q más pequeño que es a la vez divisible por n y por m. Formalmente:
$mcm : \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ tal que:

$$mcm(n, m) = (min\ q \in \mathbb{N} |\ \ n|q \wedge m|q : q)$$

- ¿mcm es total?Si, porque el número de múltiplos comunes de n y m es no vacío y tiene que tener un mínimo
- $mcm(6, 18) = 18$, porque $18 = 6 \times 3 = 18 \times 1 \wedge 18 \not| 6 \times 1 \wedge 18 \not| 6 \times 2$
- $mcm(6, 14) = 42$, porque $42 = 6 \times 7 = 14 \times 3 \wedge 14 \not| 6 \times 1 \wedge 14 \not| 6 \times 2 \wedge 14 \not| 6 \times 3 \wedge 14 \not| 6 \times 4 \wedge 14 \not| 6 \times 5 \wedge 14 \not| 6 \times 6$
- En general, ¿se imaginan un algoritmo para calcular $mcm(n, m)$?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (1)

Por el teorema fundamental de la aritmética, podemos escribir cualquier n como:

$$(n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}) \wedge (p_1 < p_2 < \dots < p_k) \wedge (\forall j| : k_j > 0)$$

Por ejemplo, $120 = 2^3 * 3 * 5$ y $500 = 2^2 * 5^3$
Nótese que $3 \not| 500$, pero podríamos escribir $500 = 2^2 * 3^0 * 5^3$, y así usaríamos los mismos primos en ambas descomposiciones Entonces, sin pérdida de generalidad podemos escribir:

$$(n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}) \wedge (\forall j | 1 \leq j \leq k : i_j \geq 0)$$

donde agregamos primos elevados a la cero si los necesitamos.

$120 = 2^3 * 3^1 * 5^1$ no agregamos
$500 = 2^2 * 3^0 * 5^3$ si agregamos

$mcd(120, 500) = 2^2 * 3^0 * 5^1 = 20$ $mcm(120, 500) = 2^3 * 3^1 * 5^3 = 3000$

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (1)

Por el teorema fundamental de la aritmética, podemos escribir cualquier n como:

$$(n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}) \wedge (p_1 < p_2 < \dots < p_k) \wedge (\forall j| : k_j > 0)$$

Por ejemplo, $120 = 2^3 * 3 * 5$ y $500 = 2^2 * 5^3$
Nótese que $3 \not| 500$, pero podríamos escribir $500 = 2^2 * 3^0 * 5^3$, y así usaríamos los mismos primos en ambas descomposiciones Entonces, sin pérdida de generalidad podemos escribir:

$$(n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}) \wedge (\forall j | 1 \leq j \leq k : i_j \geq 0)$$

donde agregamos primos elevados a la cero si los necesitamos.

$120 = 2^3 * 3^1 * 5^1$ no agregamos
$500 = 2^2 * 3^0 * 5^3$ si agregamos

$mcd(120, 500) = 2^2 * 3^0 * 5^1 = 20$ $mcm(120, 500) = 2^3 * 3^1 * 5^3 = 3000$

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (1)

Por el teorema fundamental de la aritmética, podemos escribir cualquier n como:

$$(n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}) \wedge (p_1 < p_2 < \dots < p_k) \wedge (\forall j| : k_j > 0)$$

Por ejemplo, $120 = 2^3 * 3 * 5$ y $500 = 2^2 * 5^3$
Nótese que $3 \nmid 500$, pero podríamos escribir $500 = 2^2 * 3^0 * 5^3$, y así usaríamos los mismos primos en ambas descomposiciones Entonces, sin pérdida de generalidad podemos escribir:

$$(n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}) \wedge (\forall j | 1 \leq j \leq k : i_j \geq 0)$$

donde agregamos primos elevados a la cero si los necesitamos.
$120 = 2^3 * 3^1 * 5^1$ no agregamos
$500 = 2^2 * 3^0 * 5^3$ si agregamos

$mcd(120, 500) = 2^2 * 3^0 * 5^1 = 20$ $mcm(120, 500) = 2^3 * 3^1 * 5^3 = 3000$

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (1)

Por el teorema fundamental de la aritmética, podemos escribir cualquier n como:

$$(n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}) \wedge (p_1 < p_2 < \ldots < p_k) \wedge (\forall j| : k_j > 0)$$

Por ejemplo, $120 = 2^3 * 3 * 5$ y $500 = 2^2 * 5^3$
Nótese que $3 \not| 500$, pero podríamos escribir $500 = 2^2 * 3^0 * 5^3$, y así usaríamos los mismos primos en ambas descomposiciones Entonces, sin pérdida de generalidad podemos escribir:

$$(n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}) \wedge (\forall j|1 \leq j \leq k : i_j \geq 0)$$

donde agregamos primos elevados a la cero si los necesitamos.

$120 = 2^3 * 3^1 * 5^1$ no agregamos

$500 = 2^2 * 3^0 * 5^3$ si agregamos

$mcd(120, 500) = 2^2 * 3^0 * 5^1 = 20$ $mcm(120, 500) = 2^3 * 3^1 * 5^3 = 3000$

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (1)

Por el teorema fundamental de la aritmética, podemos escribir cualquier n como:

$$(n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}) \wedge (p_1 < p_2 < \ldots < p_k) \wedge (\forall j| : k_j > 0)$$

Por ejemplo, $120 = 2^3 * 3 * 5$ y $500 = 2^2 * 5^3$
Nótese que $3 \not| 500$, pero podríamos escribir $500 = 2^2 * 3^0 * 5^3$, y así usaríamos los mismos primos en ambas descomposiciones Entonces, sin pérdida de generalidad podemos escribir:

$$(n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}) \wedge (\forall j | 1 \leq j \leq k : i_j \geq 0)$$

donde agregamos primos elevados a la cero si los necesitamos.

$120 = 2^3 * 3^1 * 5^1$ no agregamos
$500 = 2^2 * 3^0 * 5^3$ si agregamos

$mcd(120, 500) = 2^2 * 3^0 * 5^1 = 20$ $mcm(120, 500) = 2^3 * 3^1 * 5^3 = 3000$

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (1)

Por el teorema fundamental de la aritmética, podemos escribir cualquier n como:

$$(n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}) \wedge (p_1 < p_2 < \dots < p_k) \wedge (\forall j| : k_j > 0)$$

Por ejemplo, $120 = 2^3 * 3 * 5$ y $500 = 2^2 * 5^3$
Nótese que $3 \not| 500$, pero podríamos escribir $500 = 2^2 * 3^0 * 5^3$, y así usaríamos los mismos primos en ambas descomposiciones Entonces, sin pérdida de generalidad podemos escribir:

$$(n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}) \wedge (\forall j|1 \leq j \leq k : i_j \geq 0)$$

donde agregamos primos elevados a la cero si los necesitamos.

$120 = 2^3 * 3^1 * 5^1$ no agregamos
$500 = 2^2 * 3^0 * 5^3$ si agregamos

$mcd(120, 500) = 2^2 * 3^0 * 5^1 = 20$

$mcm(120, 500) = 2^3 * 3^1 * 5^3 = 3000$

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (1)

Por el teorema fundamental de la aritmética, podemos escribir cualquier n como:

$$(n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}) \wedge (p_1 < p_2 < \dots < p_k) \wedge (\forall j| : k_j > 0)$$

Por ejemplo, $120 = 2^3 * 3 * 5$ y $500 = 2^2 * 5^3$
Nótese que $3 \not| 500$, pero podríamos escribir $500 = 2^2 * 3^0 * 5^3$, y así usaríamos los mismos primos en ambas descomposiciones Entonces, sin pérdida de generalidad podemos escribir:

$$(n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}) \wedge (\forall j|1 \leq j \leq k : i_j \geq 0)$$

donde agregamos primos elevados a la cero si los necesitamos.
$120 = 2^3 * 3^1 * 5^1$ no agregamos
$500 = 2^2 * 3^0 * 5^3$ si agregamos

$mcd(120, 500) = 2^2 * 3^0 * 5^1 = 20$ $mcm(120, 500) = 2^3 * 3^1 * 5^3 = 3000$

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

Sean $n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$ y $m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \dots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
- Calculemos $mcd(15, 28)$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \dots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
- Calculemos $mcm(15, 28)$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

Sean $n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$ y $m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$

$mcd(n,m) = p_1^{min(i_1,j_1)} p_2^{min(i_2,j_2)} \dots p_k^{min(i_k,j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$

$mcm(n,m) = p_1^{max(i_1,j_1)} p_2^{max(i_2,j_2)} \dots p_k^{max(i_k,j_k)}$

Teorema: $n * m = mcd(n,m) * mcm(n,m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

Sean $n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$ y $m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \dots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \dots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
- Calculemos $mcm(15, 28)$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

Sean $n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$ y $m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \dots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \dots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
- Calculemos $mcm(15, 28)$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

Sean $n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$ y $m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \dots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \dots p_k^{max(i_k, j_k)}$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

Sean $n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$ y $m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \dots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

Sean $n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$ y $m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \dots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \dots p_k^{max(i_k, j_k)}$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

Sean $n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}$ y $m = p_1^{j_1} p_2^{j_2} \ldots p_k^{j_k}$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \ldots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \ldots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
- Calculemos $mcm(15, 28)$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

Sean $n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}$ y $m = p_1^{j_1} p_2^{j_2} \ldots p_k^{j_k}$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \ldots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \ldots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
- Calculemos $mcm(15, 28)$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

$$\text{Sean } n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k} \text{ y } m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$$

$$mcd(n,m) = p_1^{min(i_1,j_1)} p_2^{min(i_2,j_2)} \dots p_k^{min(i_k,j_k)}$$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$$mcm(n,m) = p_1^{max(i_1,j_1)} p_2^{max(i_2,j_2)} \dots p_k^{max(i_k,j_k)}$$

- Calculemos $mcm(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
- Calculemos $mcm(15, 28)$

Teorema: $n * m = mcd(n,m) * mcm(n,m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

$$\text{Sean } n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k} \text{ y } m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \dots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \dots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcm(100, 222) = 2^2 * 3^1 * 5^2 * 37^1 = 11100$
- Calculemos $mcm(15, 28)$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

$$\text{Sean } n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k} \text{ y } m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \dots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \dots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcm(100, 222) = 2^2 * 3^1 * 5^2 * 37^1 = 11100$
- Calculemos $mcm(15, 28)$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

$$\text{Sean } n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k} \text{ y } m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \dots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \dots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcm(100, 222) = 2^2 * 3^1 * 5^2 * 37^1 = 11100$
- Calculemos $mcm(15, 28)$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

Sean $n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}$ y $m = p_1^{j_1} p_2^{j_2} \ldots p_k^{j_k}$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \ldots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \ldots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcm(100, 222) = 2^2 * 3^1 * 5^2 * 37^1 = 11100$
- Calculemos $mcm(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

$$\text{Sean } n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k} \text{ y } m = p_1^{j_1} p_2^{j_2} \ldots p_k^{j_k}$$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \ldots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \ldots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcm(100, 222) = 2^2 * 3^1 * 5^2 * 37^1 = 11100$
- Calculemos $mcm(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcm(15, 28) = 2^2 * 3^1 * 5^1 * 7^1 = 420$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

$$\text{Sean } n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k} \text{ y } m = p_1^{j_1} p_2^{j_2} \ldots p_k^{j_k}$$

$mcd(n,m) = p_1^{min(i_1,j_1)} p_2^{min(i_2,j_2)} \ldots p_k^{min(i_k,j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$mcm(n,m) = p_1^{max(i_1,j_1)} p_2^{max(i_2,j_2)} \ldots p_k^{max(i_k,j_k)}$

- Calculemos $mcm(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcm(100, 222) = 2^2 * 3^1 * 5^2 * 37^1 = 11100$
- Calculemos $mcm(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcm(15, 28) = 2^2 * 3^1 * 5^1 * 7^1 = 420$

Teorema: $n * m = mcd(n,m) * mcm(n,m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

Sean $n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$ y $m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \dots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \dots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcm(100, 222) = 2^2 * 3^1 * 5^2 * 37^1 = 11100$
- Calculemos $mcm(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcm(15, 28) = 2^2 * 3^1 * 5^1 * 7^1 = 420$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular mcd?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

$$\text{Sean } n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k} \text{ y } m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \dots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \dots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcm(100, 222) = 2^2 * 3^1 * 5^2 * 37^1 = 11100$
- Calculemos $mcm(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcm(15, 28) = 2^2 * 3^1 * 5^1 * 7^1 = 420$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular *mcd*?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

Sean $n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$ y $m = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \dots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \dots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcm(100, 222) = 2^2 * 3^1 * 5^2 * 37^1 = 11100$
- Calculemos $mcm(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcm(15, 28) = 2^2 * 3^1 * 5^1 * 7^1 = 420$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular *mcd*?

Divisores y múltiplos comunes usando el teorema fundamental de la aritmética (2)

Sean $n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}$ y $m = p_1^{j_1} p_2^{j_2} \ldots p_k^{j_k}$

$mcd(n, m) = p_1^{min(i_1, j_1)} p_2^{min(i_2, j_2)} \ldots p_k^{min(i_k, j_k)}$

- Calculemos $mcd(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcd(100, 222) = 2^1 * 3^0 * 5^0 * 37^0 = 2$
- Calculemos $mcd(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcd(15, 28) = 2^0 * 3^0 * 5^0 * 7^0 = 1$

$mcm(n, m) = p_1^{max(i_1, j_1)} p_2^{max(i_2, j_2)} \ldots p_k^{max(i_k, j_k)}$

- Calculemos $mcm(100, 222)$
  $100 = 2^2 * 5^2$ y $222 = 2^1 * 3^1 * 37^1$
  $100 = 2^2 * 3^0 * 5^2 * 37^0$ y $222 = 2^1 * 3^1 * 5^0 * 37^1$
  $mcm(100, 222) = 2^2 * 3^1 * 5^2 * 37^1 = 11100$
- Calculemos $mcm(15, 28)$
  $15 = 3^1 * 5^1$ y $28 = 2^2 * 7^1$
  $15 = 2^0 * 3^1 * 5^1 * 7^0$ y $28 = 2^2 * 3^0 * 5^0 * 7^1$
  $mcm(15, 28) = 2^2 * 3^1 * 5^1 * 7^1 = 420$

Teorema: $n * m = mcd(n, m) * mcm(n, m)$

¿Se imaginan un algoritmo basado en este teorema para calcular *mcd*?

Plan

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m,n) = mcd(n,m)$
2. $(m,n) \neq (0,0) \implies mcd(m,n) = (min\ x,y \mid mx+ny > 0 \ : \ mx+ny)$
3. $mcd(m,n) = d \implies \exists x,y| : d = mx+ny$
4. $mcd(m, mcd(n,q)) = mcd(mcd(m,n),q)$
5. $d|m \wedge d|n \implies d|mcd(m,n)$
6. $mcd(m,m) = |m|$
7. $mcd(m,1) = 1$
8. $mcd(m,0) = |m|$

1. $mcd(m,n) = mcd(|m|,|n|)$
2. $mcd(m,n) = mcd(m-n,n) = mcd(m,n-m)$
3. $d > 0 \implies mcd(dm,dn) = dmcd(m,n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d, n/d) = mcd(m,n)/d$
5. $d|m*n \wedge mcd(d,n) = 1 \implies d|m$
6. $n = mq+r \implies mcd(n,m) = mcd(m,r)$

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m, n) = mcd(n, m)$
2. $(m, n) \neq (0, 0) \implies mcd(m, n) = (min\ x, y \mid mx + ny > 0 \ : \ mx + ny)$
3. $mcd(m, n) = d \implies \exists x, y| : d = mx + ny$
4. $mcd(m, mcd(n, q)) = mcd(mcd(m, n), q)$
5. $d|m \wedge d|n \implies d|mcd(m, n)$
6. $mcd(m, m) = |m|$
7. $mcd(m, 1) = 1$
8. $mcd(m, 0) = |m|$

1. $mcd(m, n) = mcd(|m|, |n|)$
2. $mcd(m, n) = mcd(m - n, n) = mcd(m, n - m)$
3. $d > 0 \implies mcd(dm, dn) = dmcd(m, n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d, n/d) = mcd(m, n)/d$
5. $d|m * n \wedge mcd(d, n) = 1 \implies d|m$
6. $n = mq + r \implies mcd(n, m) = mcd(m, r)$

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m,n) = mcd(n,m)$
2. $(m,n) \neq (0,0) \implies mcd(m,n) = (min\ x, y \mid mx + ny > 0 \ : \ mx + ny)$
3. $mcd(m,n) = d \implies \exists x, y| : d = mx + ny$
4. $mcd(m, mcd(n,q)) = mcd(mcd(m,n), q)$
5. $d|m \wedge d|n \implies d|mcd(m,n)$
6. $mcd(m,m) = |m|$
7. $mcd(m,1) = 1$
8. $mcd(m,0) = |m|$

1. $mcd(m,n) = mcd(|m|,|n|)$
2. $mcd(m,n) = mcd(m-n,n) = mcd(m,n-m)$
3. $d > 0 \implies mcd(dm,dn) = dmcd(m,n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d, n/d) = mcd(m,n)/d$
5. $d|m * n \wedge mcd(d,n) = 1 \implies d|m$
6. $n = mq + r \implies mcd(n,m) = mcd(m,r)$

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m,n) = mcd(n,m)$
2. $(m,n) \neq (0,0) \implies mcd(m,n) = (min\ x,y \mid mx+ny > 0\ :\ mx+ny)$
3. $mcd(m,n) = d \implies \exists x,y| : d = mx+ny$
4. $mcd(m, mcd(n,q)) = mcd(mcd(m,n),q)$
5. $d|m \wedge d|n \implies d|mcd(m,n)$
6. $mcd(m,m) = |m|$
7. $mcd(m,1) = 1$
8. $mcd(m,0) = |m|$

1. $mcd(m,n) = mcd(|m|,|n|)$
2. $mcd(m,n) = mcd(m-n,n) = mcd(m,n-m)$
3. $d > 0 \implies mcd(dm,dn) = dmcd(m,n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d,n/d) = mcd(m,n)/d$
5. $d|m*n \wedge mcd(d,n) = 1 \implies d|m$
6. $n = mq + r \implies mcd(n,m) = mcd(m,r)$

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m,n) = mcd(n,m)$
2. $(m,n) \neq (0,0) \implies mcd(m,n) = (min\ x,y \mid mx+ny > 0 \ :\ mx+ny)$
3. $mcd(m,n) = d \implies \exists x,y| : d = mx+ny$
4. $mcd(m, mcd(n,q)) = mcd(mcd(m,n),q)$
5. $d|m \wedge d|n \implies d|mcd(m,n)$
6. $mcd(m,m) = |m|$
7. $mcd(m,1) = 1$
8. $mcd(m,0) = |m|$

1. $mcd(m,n) = mcd(|m|,|n|)$
2. $mcd(m,n) = mcd(m-n,n) = mcd(m,n-m)$
3. $d > 0 \implies mcd(dm,dn) = dmcd(m,n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d,n/d) = mcd(m,n)/d$
5. $d|m*n \wedge mcd(d,n) = 1 \implies d|m$
6. $n = mq+r \implies mcd(n,m) = mcd(m,r)$

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m,n) = mcd(n,m)$
2. $(m,n) \neq (0,0) \implies mcd(m,n) = (min\ x,y \mid mx+ny > 0 \ :\ mx+ny)$
3. $mcd(m,n) = d \implies \exists x,y| : d = mx+ny$
4. $mcd(m, mcd(n,q)) = mcd(mcd(m,n),q)$
5. $d|m \wedge d|n \implies d|mcd(m,n)$
6. $mcd(m,m) = |m|$
7. $mcd(m,1) = 1$
8. $mcd(m,0) = |m|$

1. $mcd(m,n) = mcd(|m|,|n|)$
2. $mcd(m,n) = mcd(m-n,n) = mcd(m,n-m)$
3. $d > 0 \implies mcd(dm,dn) = dmcd(m,n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d,n/d) = mcd(m,n)/d$
5. $d|m*n \wedge mcd(d,n) = 1 \implies d|m$
6. $n = mq + r \implies mcd(n,m) = mcd(m,r)$

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m, n) = mcd(n, m)$
2. $(m, n) \neq (0, 0) \implies mcd(m, n) = (min\ x, y \mid mx + ny > 0 \ :\ mx + ny)$
3. $mcd(m, n) = d \implies \exists x, y| : d = mx+ny$
4. $mcd(m, mcd(n, q)) = mcd(mcd(m, n), q)$
5. $d|m \wedge d|n \implies d|mcd(m, n)$
6. $mcd(m, m) = |m|$
7. $mcd(m, 1) = 1$
8. $mcd(m, 0) = |m|$

1. $mcd(m, n) = mcd(|m|, |n|)$
2. $mcd(m, n) = mcd(m - n, n) = mcd(m, n - m)$
3. $d > 0 \implies mcd(dm, dn) = dmcd(m, n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d, n/d) = mcd(m, n)/d$
5. $d|m * n \wedge mcd(d, n) = 1 \implies d|m$
6. $n = mq + r \implies mcd(n, m) = mcd(m, r)$

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m, n) = mcd(n, m)$
2. $(m, n) \neq (0, 0) \implies mcd(m, n) = (min\ x, y \mid mx + ny > 0 \ :\ mx + ny)$
3. $mcd(m, n) = d \implies \exists x, y| : d = mx + ny$
4. $mcd(m, mcd(n, q)) = mcd(mcd(m, n), q)$
5. $d|m \wedge d|n \implies d|mcd(m, n)$
6. $mcd(m, m) = |m|$
7. $mcd(m, 1) = 1$
8. $mcd(m, 0) = |m|$

1. $mcd(m, n) = mcd(|m|, |n|)$
2. $mcd(m, n) = mcd(m - n, n) = mcd(m, n - m)$
3. $d > 0 \implies mcd(dm, dn) = dmcd(m, n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d, n/d) = mcd(m, n)/d$
5. $d|m * n \wedge mcd(d, n) = 1 \implies d|m$
6. $n = mq + r \implies mcd(n, m) = mcd(m, r)$

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m, n) = mcd(n, m)$
2. $(m, n) \neq (0, 0) \implies mcd(m, n) = (min\ x, y \mid mx + ny > 0 \ : \ mx + ny)$
3. $mcd(m, n) = d \implies \exists x, y| : d = mx+ny$
4. $mcd(m, mcd(n, q)) = mcd(mcd(m, n), q)$
5. $d|m \wedge d|n \implies d|mcd(m, n)$
6. $mcd(m, m) = |m|$
7. $mcd(m, 1) = 1$
8. $mcd(m, 0) = |m|$

1. $mcd(m, n) = mcd(|m|, |n|)$
2. $mcd(m, n) = mcd(m - n, n) = mcd(m, n - m)$
3. $d > 0 \implies mcd(dm, dn) = dmcd(m, n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d, n/d) = mcd(m, n)/d$
5. $d|m * n \wedge mcd(d, n) = 1 \implies d|m$
6. $n = mq + r \implies mcd(n, m) = mcd(m, r)$

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m,n) = mcd(n,m)$
2. $(m,n) \neq (0,0) \implies mcd(m,n) = (min\ x,y \mid mx+ny > 0 \ : \ mx+ny)$
3. $mcd(m,n) = d \implies \exists x,y| : d = mx+ny$
4. $mcd(m, mcd(n,q)) = mcd(mcd(m,n),q)$
5. $d|m \wedge d|n \implies d|mcd(m,n)$
6. $mcd(m,m) = |m|$
7. $mcd(m,1) = 1$
8. $mcd(m,0) = |m|$

1. $mcd(m,n) = mcd(|m|,|n|)$
2. $mcd(m,n) = mcd(m-n,n) = mcd(m,n-m)$
3. $d > 0 \implies mcd(dm,dn) = dmcd(m,n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d, n/d) = mcd(m,n)/d$
5. $d|m*n \wedge mcd(d,n) = 1 \implies d|m$
6. $n = mq + r \implies mcd(n,m) = mcd(m,r)$

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m,n) = mcd(n,m)$
2. $(m,n) \neq (0,0) \implies mcd(m,n) = (min\ x,y \mid mx+ny > 0\ :\ mx+ny)$
3. $mcd(m,n) = d \implies \exists x,y| : d = mx+ny$
4. $mcd(m, mcd(n,q)) = mcd(mcd(m,n),q)$
5. $d|m \wedge d|n \implies d|mcd(m,n)$
6. $mcd(m,m) = |m|$
7. $mcd(m,1) = 1$
8. $mcd(m,0) = |m|$

1. $mcd(m,n) = mcd(|m|,|n|)$
2. $mcd(m,n) = mcd(m-n,n) = mcd(m,n-m)$
3. $d > 0 \implies mcd(dm,dn) = dmcd(m,n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d, n/d) = mcd(m,n)/d$
5. $d|m*n \wedge mcd(d,n) = 1 \implies d|m$
6. $n = mq+r \implies mcd(n,m) = mcd(m,r)$

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m, n) = mcd(n, m)$
2. $(m, n) \neq (0, 0) \implies mcd(m, n) = (min\ x, y \mid mx + ny > 0 \ : \ mx + ny)$
3. $mcd(m, n) = d \implies \exists x, y| : d = mx + ny$
4. $mcd(m, mcd(n, q)) = mcd(mcd(m, n), q)$
5. $d|m \wedge d|n \implies d|mcd(m, n)$
6. $mcd(m, m) = |m|$
7. $mcd(m, 1) = 1$
8. $mcd(m, 0) = |m|$

1. $mcd(m, n) = mcd(|m|, |n|)$
2. $mcd(m, n) = mcd(m - n, n) = mcd(m, n - m)$
3. $d > 0 \implies mcd(dm, dn) = dmcd(m, n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d, n/d) = mcd(m, n)/d$
5. $d|m * n \wedge mcd(d, n) = 1 \implies d|m$
6. $n = mq + r \implies mcd(n, m) = mcd(m, r)$

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m,n) = mcd(n,m)$
2. $(m,n) \neq (0,0) \implies mcd(m,n) = (min\ x,y \mid mx+ny>0 \ :\ mx+ny)$
3. $mcd(m,n) = d \implies \exists x,y| : d = mx+ny$
4. $mcd(m, mcd(n,q)) = mcd(mcd(m,n),q)$
5. $d|m \wedge d|n \implies d|mcd(m,n)$
6. $mcd(m,m) = |m|$
7. $mcd(m,1) = 1$
8. $mcd(m,0) = |m|$

1. $mcd(m,n) = mcd(|m|,|n|)$
2. $mcd(m,n) = mcd(m-n,n) = mcd(m,n-m)$
3. $d > 0 \implies mcd(dm,dn) = dmcd(m,n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d, n/d) = mcd(m,n)/d$
5. $d|m*n \wedge mcd(d,n) = 1 \implies d|m$
6. $n = mq + r \implies mcd(n,m) = mcd(m,r)$

Propiedades del *mcd*

Estudiamos un poco más el *mcd* para ver si podemos calcularlo más eficientemente:

1. $mcd(m, n) = mcd(n, m)$
2. $(m, n) \neq (0, 0) \implies mcd(m, n) = (min\ x, y \mid mx + ny > 0 \ :\ mx + ny)$
3. $mcd(m, n) = d \implies \exists x, y| : d = mx+ny$
4. $mcd(m, mcd(n, q)) = mcd(mcd(m, n), q)$
5. $d|m \wedge d|n \implies d|mcd(m, n)$
6. $mcd(m, m) = |m|$
7. $mcd(m, 1) = 1$
8. $mcd(m, 0) = |m|$

1. $mcd(m, n) = mcd(|m|, |n|)$
2. $mcd(m, n) = mcd(m - n, n) = mcd(m, n - m)$
3. $d > 0 \implies mcd(dm, dn) = dmcd(m, n)$
4. $d > 0 \wedge d|m \wedge d|n \implies mcd(m/d, n/d) = mcd(m, n)/d$
5. $d|m * n \wedge mcd(d, n) = 1 \implies d|m$
6. $n = mq + r \implies mcd(n, m) = mcd(m, r)$

Algoritmo de Euclides: Restas (Video 3.1)

Basado en la siguiente propiedad:

$$mcd(m, n) = mcd(m - n, n) = mcd(m, n - m)$$

Entonces,

$$mcd(m,n) = \begin{cases} m & \text{Si } m = n \\ mcd(m-n, n) & \text{Si } m > n \\ mcd(m, n-m) & \text{Si } m < n \end{cases}$$

Por ejemplo, calculemos $mcd(963, 657)$:

Paso	m	n
0	963	657
1	306	657
2	306	351
3	306	45
4	261	45
5	216	45
6	171	45

Paso	m	n
7	126	45
8	81	45
9	36	45
10	36	9
11	27	9
12	18	9
13	9	9

Algoritmo de Euclides: Restas (Video 3.1)

Basado en la siguiente propiedad:

$$mcd(m, n) = mcd(m - n, n) = mcd(m, n - m)$$

Entonces,

$$mcd(m, n) = \begin{cases} m & \text{Si } m = n \\ mcd(m - n, n) & \text{Si } m > n \\ mcd(m, n - m) & \text{Si } m < n \end{cases}$$

Por ejemplo, calculemos $mcd(963, 657)$:

Paso	m	n
0	963	657
1	306	657
2	306	351
3	306	45
4	261	45
5	216	45
6	171	45

Paso	m	n
7	126	45
8	81	45
9	36	45
10	36	9
11	27	9
12	18	9
13	9	9

Algoritmo de Euclides: Restas (Video 3.1)

Basado en la siguiente propiedad:

$$mcd(m,n) = mcd(m-n,n) = mcd(m,n-m)$$

Entonces,

$$mcd(m,n) = \begin{cases} m & \text{Si } m = n \\ mcd(m-n,n) & \text{Si } m > n \\ mcd(m,n-m) & \text{Si } m < n \end{cases}$$

Por ejemplo, calculemos $mcd(963, 657)$:

Paso	m	n
0	963	657
1	306	657
2	306	351
3	306	45
4	261	45
5	216	45
6	171	45

Paso	m	n
7	126	45
8	81	45
9	36	45
10	36	9
11	27	9
12	18	9
13	9	9

Algoritmo de Euclides: Divisiones (Video 3.2)

Basado en la siguiente propiedad (suponemos $n \geq m$):

$$n = mq + r \implies mcd(n, m) = mcd(m, r)$$

Entonces,

$$mcd(n, m) = \begin{cases} n & \text{Si } m = 0 \\ mcd(m, r) & \text{Si, por algoritmo de la división } n = mq + r \end{cases}$$

Por ejemplo, calculemos $mcd(963, 657)$:

Paso	n	m	q	r
0	963	657	1	306
1	657	306	2	45
2	306	45	6	36
3	45	36	1	9
4	36	9	4	0
5	9	0		

Nótese que el algoritmo de divisiones es una aceleración del algoritmo de restas

Algoritmo de Euclides: Divisiones (Video 3.2)

Basado en la siguiente propiedad (suponemos $n \geq m$):

$$n = mq + r \implies mcd(n,m) = mcd(m,r)$$

Entonces,

$$mcd(n,m) = \begin{cases} n & \text{Si } m = 0 \\ mcd(m,r) & \text{Si, por algoritmo de la división } n = mq + r \end{cases}$$

Por ejemplo, calculemos $mcd(963, 657)$:

Paso	n	m	q	r
0	963	657	1	306
1	657	306	2	45
2	306	45	6	36
3	45	36	1	9
4	36	9	4	0
5	9	0		

Nótese que el algoritmo de divisiones es una aceleración del algoritmo de restas

Algoritmo de Euclides: Divisiones (Video 3.2)

Basado en la siguiente propiedad (suponemos $n \geq m$):

$$n = mq + r \implies mcd(n, m) = mcd(m, r)$$

Entonces,

$$mcd(n,m) = \begin{cases} n & \text{Si } m = 0 \\ mcd(m,r) & \text{Si, por algoritmo de la división } n = mq + r \end{cases}$$

Por ejemplo, calculemos $mcd(963, 657)$:

Paso	n	m	q	r
0	963	657	1	306
1	657	306	2	45
2	306	45	6	36
3	45	36	1	9
4	36	9	4	0
5	9	0		

Nótese que el algoritmo de divisiones es una aceleración del algoritmo de restas

Algoritmo de Euclides: Divisiones - Corrección (Video 3.3)

El algoritmo anterior es correcto si la siguiente propiedad es un teorema (suponemos $n \geq m$):

$$n = mq + r \implies mcd(n, m) = mcd(m, r)$$

- $(d|n \wedge d|m) \implies (d|m \wedge d|r)$ (es decir, todo divisor común de n y m es divisor común de m y r).
  Por hipótesis, $n = mq + r$.
  Por lo tanto $r = n - mq$
  Como $d|n$ y $d|m$ entonces (teorema 4, divisibilidad) $d|nb + mc$ para cualquier b y c. Particularmente, $d|n * 1 + m * (-q)$, o sea $d|r$.
- $(d|m \wedge d|r) \implies (d|n \wedge d|m)$ (es decir, todo divisor común de m y r es divisor común de n y m).
  Por hipótesis, $n = mq + r$.
  Como $d|m$ y $d|r$ entonces (teorema 4, divisibilidad) $d|mb + rc$ para cualquier b y c. Particularmente, $d|m * q + r * 1$, o sea $d|n$.
- Por lo anterior, los divisores comunes de n y m son los mismos divisores comunes de m y r. Entonces, $mcd(n, m) = mcd(m, r)$

Algoritmo de Euclides: Divisiones - Corrección (Video 3.3)

El algoritmo anterior es correcto si la siguiente propiedad es un teorema (suponemos $n \geq m$):

$$n = mq + r \implies mcd(n, m) = mcd(m, r)$$

- $(d|n \wedge d|m) \implies (d|m \wedge d|r)$ (es decir, todo divisor común de n y m es divisor común de m y r).
  Por hipótesis, $n = mq + r$.
  Por lo tanto $r = n - mq$
  Como $d|n$ y $d|m$ entonces (teorema 4, divisibilidad) $d|nb + mc$ para cualquier b y c. Particularmente, $d|n * 1 + m * (-q)$, o sea $d|r$.
- $(d|m \wedge d|r) \implies (d|n \wedge d|m)$ (es decir, todo divisor común de m y r es divisor común de n y m).
  Por hipótesis, $n = mq + r$.
  Como $d|m$ y $d|r$ entonces (teorema 4, divisibilidad) $d|mb + rc$ para cualquier b y c. Particularmente, $d|m * q + r * 1$, o sea $d|n$.
- Por lo anterior, los divisores comunes de n y m son los mismos divisores comunes de m y r. Entonces, $mcd(n, m) = mcd(m, r)$

Algoritmo de Euclides: Divisiones - Corrección (Video 3.3)

El algoritmo anterior es correcto si la siguiente propiedad es un teorema (suponemos $n \geq m$):

$$n = mq + r \implies mcd(n, m) = mcd(m, r)$$

- $(d|n \wedge d|m) \implies (d|m \wedge d|r)$ (es decir, todo divisor común de n y m es divisor común de m y r).
  Por hipótesis, $n = mq + r$.
  Por lo tanto $r = n - mq$
  Como $d|n$ y $d|m$ entonces (teorema 4, divisibilidad) $d|nb + mc$ para cualquier b y c. Particularmente, $d|n * 1 + m * (-q)$, o sea $d|r$.
- $(d|m \wedge d|r) \implies (d|n \wedge d|m)$ (es decir, todo divisor común de m y r es divisor común de n y m).
  Por hipótesis, $n = mq + r$.
  Como $d|m$ y $d|r$ entonces (teorema 4, divisibilidad) $d|mb + rc$ para cualquier b y c. Particularmente, $d|m * q + r * 1$, o sea $d|n$.
- Por lo anterior, los divisores comunes de n y m son los mismos divisores comunes de m y r. Entonces, $mcd(n, m) = mcd(m, r)$

Algoritmo de Euclides: Terminación (Video 3.3)

La terminación de este algoritmo

$$mcd(n,m) = \begin{cases} n & \text{Si } m = 0 \\ mcd(m,r) & \text{Si, por algoritmo de la división } n = mq + r \end{cases}$$

depende de que en algún momento $r = 0$.

Miremos la forma de las iteraciones:

Paso	n	m	q	r	TFA
0	$n = r_0$	$m = r_1$	q_1	r_2	$0 \leq r_2 < r_1$
1	r_1	r_2	q_2	r_3	$0 \leq r_3 < r_2$
2	r_2	r_3	q_3	r_4	$0 \leq r_4 < r_3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$k-2$	r_{k-2}	r_{k-1}	q_{k-1}	r_k	$0 \leq r_k < r_{k-1}$
$k-1$	r_{k-1}	r_k	q_k	0	$r_{k+1} = 0$

Como $n = r_0 > r_1 > r_2 > \ldots > r_k > r_{k+1} = 0$ (no puede ser infinita esta secuencia)
$mcd(n,m) = mcd(r_0, r_1) = mcd(r_1, r_2) = \ldots = mcd(r_{k-1}, r_k) = mcd(r_k, 0) = r_k$

Algoritmo de Euclides: Terminación (Video 3.3)

La terminación de este algoritmo

$$mcd(n,m) = \begin{cases} n & \text{Si } m = 0 \\ mcd(m,r) & \text{Si, por algoritmo de la división } n = mq + r \end{cases}$$

depende de que en algún momento $r = 0$.

Miremos la forma de las iteraciones:

Paso	n	m	q	r	TFA
0	$n = r_0$	$m = r_1$	q_1	r_2	$0 \leq r_2 < r_1$
1	r_1	r_2	q_2	r_3	$0 \leq r_3 < r_2$
2	r_2	r_3	q_3	r_4	$0 \leq r_4 < r_3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$k-2$	r_{k-2}	r_{k-1}	q_{k-1}	r_k	$0 \leq r_k < r_{k-1}$
$k-1$	r_{k-1}	r_k	q_k	0	$r_{k+1} = 0$

Como $n = r_0 > r_1 > r_2 > \ldots > r_k > r_{k+1} = 0$ (no puede ser infinita esta secuencia)
$mcd(n,m) = mcd(r_0, r_1) = mcd(r_1, r_2) = \ldots = mcd(r_{k-1}, r_k) = mcd(r_k, 0) = r_k$

Algoritmo de Euclides: Terminación (Video 3.3)

La terminación de este algoritmo

$$mcd(n,m) = \begin{cases} n & \text{Si } m = 0 \\ mcd(m,r) & \text{Si, por algoritmo de la división } n = mq + r \end{cases}$$

depende de que en algún momento $r = 0$.

Miremos la forma de las iteraciones:

Paso	n	m	q	r	TFA
0	$n = r_0$	$m = r_1$	q_1	r_2	$0 \leq r_2 < r_1$
1	r_1	r_2	q_2	r_3	$0 \leq r_3 < r_2$
2	r_2	r_3	q_3	r_4	$0 \leq r_4 < r_3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$k-2$	r_{k-2}	r_{k-1}	q_{k-1}	r_k	$0 \leq r_k < r_{k-1}$
$k-1$	r_{k-1}	r_k	q_k	0	$r_{k+1} = 0$

Como $n = r_0 > r_1 > r_2 > \ldots > r_k > r_{k+1} = 0$ (no puede ser infinita esta secuencia)

$mcd(n,m) = mcd(r_0, r_1) = mcd(r_1, r_2) = \ldots = mcd(r_{k-1}, r_k) = mcd(r_k, 0) = r_k$

Algoritmo de Euclides: Terminación (Video 3.3)

La terminación de este algoritmo

$$mcd(n,m) = \begin{cases} n & \text{Si } m = 0 \\ mcd(m,r) & \text{Si, por algoritmo de la división } n = mq + r \end{cases}$$

depende de que en algún momento $r = 0$.

Miremos la forma de las iteraciones:

Paso	n	m	q	r	TFA
0	$n = r_0$	$m = r_1$	q_1	r_2	$0 \leq r_2 < r_1$
1	r_1	r_2	q_2	r_3	$0 \leq r_3 < r_2$
2	r_2	r_3	q_3	r_4	$0 \leq r_4 < r_3$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$k-2$	r_{k-2}	r_{k-1}	q_{k-1}	r_k	$0 \leq r_k < r_{k-1}$
$k-1$	r_{k-1}	r_k	q_k	0	$r_{k+1} = 0$

Como $n = r_0 > r_1 > r_2 > \ldots > r_k > r_{k+1} = 0$ (no puede ser infinita esta secuencia)
$mcd(n,m) = mcd(r_0, r_1) = mcd(r_1, r_2) = \ldots = mcd(r_{k-1}, r_k) = mcd(r_k, 0) = r_k$

Algoritmo de Euclides: Comb. lineal del *mcd* (Video 3.4)

Una de la propiedades del *mcd* era:

$$mcd(m, n) = d \implies \exists x, y | : d = mx + ny$$

El algoritmo de Euclides también permite calcular x y y tal que $mcd(n, m) = xm + yn$
Por ejemplo, cuando $mcd(963, 657)$, la tabla resultante fue:

Paso	n	m	q	r
0	963	657	1	306
1	657	306	2	45
2	306	45	6	36
3	45	36	1	9
4	36	9	4	0
5	9	0		

Del Paso	$r =$
3	$9 = 45 - 36 * 1$
2	$36 = 306 - 45 * 6$
1	$45 = 657 - 306 * 2$
0	$306 = 963 - 657 * 1$

$$9 = 45 - 36 * 1 = -306 + 45 * 7 = 657 * 7 - 306 * 15 = 963 * (-15) + 657 * 22$$

Algoritmo de Euclides: Comb. lineal del *mcd* (Video 3.4)

Una de la propiedades del *mcd* era:

$$mcd(m,n) = d \implies \exists x, y | : d = mx + ny$$

El algoritmo de Euclides también permite calcular x y y tal que $mcd(n,m) = xm + yn$
Por ejemplo, cuando $mcd(963, 657)$, la tabla resultante fue:

Paso	n	m	q	r
0	963	657	1	306
1	657	306	2	45
2	306	45	6	36
3	45	36	1	9
4	36	9	4	0
5	9	0		

Del Paso	$r =$
3	$9 = 45 - 36 * 1$
2	$36 = 306 - 45 * 6$
1	$45 = 657 - 306 * 2$
0	$306 = 963 - 657 * 1$

$9 = 45 - 36 * 1 = -306 + 45 * 7 = 657 * 7 - 306 * 15 = 963 * (-15) + 657 * 22$

Algoritmo de Euclides: Comb. lineal del *mcd* (Video 3.4)

Una de la propiedades del *mcd* era:

$$mcd(m,n) = d \implies \exists x, y| : d = mx + ny$$

El algoritmo de Euclides también permite calcular x y y tal que $mcd(n,m) = xm + yn$
Por ejemplo, cuando $mcd(963, 657)$, la tabla resultante fue:

Paso	n	m	q	r
0	963	657	1	306
1	657	306	2	45
2	306	45	6	36
3	45	36	1	9
4	36	9	4	0
5	9	0		

Del Paso	$r =$
3	$9 = 45 - 36 * 1$
2	$36 = 306 - 45 * 6$
1	$45 = 657 - 306 * 2$
0	$306 = 963 - 657 * 1$

$$9 = 45 - 36 * 1 = -306 + 45 * 7 = 657 * 7 - 306 * 15 = 963 * (-15) + 657 * 22$$

Algoritmo de Euclides: Comb. lineal del *mcd* (Video 3.4)

Una de la propiedades del *mcd* era:

$$mcd(m, n) = d \implies \exists x, y| : d = mx + ny$$

El algoritmo de Euclides también permite calcular x y y tal que $mcd(n, m) = xm + yn$
Por ejemplo, cuando $mcd(963, 657)$, la tabla resultante fue:

Paso	n	m	q	r
0	963	657	1	306
1	657	306	2	45
2	306	45	6	36
3	45	36	1	9
4	36	9	4	0
5	9	0		

Del Paso	$r =$
3	$9 = 45 - 36 * 1$
2	$36 = 306 - 45 * 6$
1	$45 = 657 - 306 * 2$
0	$306 = 963 - 657 * 1$

$9 = 45 - 36 * 1 = -306 + 45 * 7 = 657 * 7 - 306 * 15 = 963 * (-15) + 657 * 22$

Algoritmo de Euclides: Comb. lineal del *mcd* (Video 3.4)

Una de la propiedades del *mcd* era:

$$mcd(m, n) = d \implies \exists x, y| : d = mx + ny$$

El algoritmo de Euclides también permite calcular x y y tal que $mcd(n, m) = xm + yn$
Por ejemplo, cuando $mcd(963, 657)$, la tabla resultante fue:

Paso	n	m	q	r
0	963	657	1	306
1	657	306	2	45
2	306	45	6	36
3	45	36	1	9
4	36	9	4	0
5	9	0		

Del Paso	$r =$
3	$9 = 45 - 36 * 1$
2	$36 = 306 - 45 * 6$
1	$45 = 657 - 306 * 2$
0	$306 = 963 - 657 * 1$

$$9 = 45 - 36 * 1 = -306 + 45 * 7 = 657 * 7 - 306 * 15 = 963 * (-15) + 657 * 22$$

Algoritmo de Euclides: Ejercicios

[Socrative]Use el algoritmo de divisiones de Euclides para hallar el $mcd(n, m)$ y los coeficientes de Bezout cuando:

1. $n = 8, m = 9$
2. $n = 12, m = 18$
3. $n = 123, m = 277$
4. $n = 100, m = 101$
5. $n = 1001, m = 1331$

No olvide hacer las tablas para cada caso:

Paso	n	m	q	r
0				
1				
2				
3				
4				
5				

Del Paso	$r =$
5	
4	
3	
2	
1	
0	

Algoritmo de Euclides: Ejercicios

[Socrative]Use el algoritmo de divisiones de Euclides para hallar el $mcd(n, m)$ y los coeficientes de Bezout cuando:

1. $n = 8, m = 9$
2. $n = 12, m = 18$
3. $n = 123, m = 277$
4. $n = 100, m = 101$
5. $n = 1001, m = 1331$

No olvide hacer las tablas para cada caso:

Paso	n	m	q	r
0				
1				
2				
3				
4				
5				

Del Paso	$r =$
5	
4	
3	
2	
1	
0	

Algoritmo de Euclides: Ejercicios

[Socrative]Use el algoritmo de divisiones de Euclides para hallar el $mcd(n, m)$ y los coeficientes de Bezout cuando:

1. $n = 8, m = 9$
2. $n = 12, m = 18$
3. $n = 123, m = 277$
4. $n = 100, m = 101$
5. $n = 1001, m = 1331$

No olvide hacer las tablas para cada caso:

Paso	n	m	q	r
0				
1				
2				
3				
4				
5				

Del Paso	$r =$
5	
4	
3	
2	
1	
0	

Algoritmo de Euclides: Ejercicios

[Socrative]Use el algoritmo de divisiones de Euclides para hallar el $mcd(n, m)$ y los coeficientes de Bezout cuando:

1. $n = 8, m = 9$
2. $n = 12, m = 18$
3. $n = 123, m = 277$
4. $n = 100, m = 101$
5. $n = 1001, m = 1331$

No olvide hacer las tablas para cada caso:

Paso	n	m	q	r
0				
1				
2				
3				
4				
5				

Del Paso	$r =$
5	
4	
3	
2	
1	
0	

Algoritmo de Euclides: Ejercicios

[Socrative]Use el algoritmo de divisiones de Euclides para hallar el $mcd(n, m)$ y los coeficientes de Bezout cuando:

1. $n = 8, m = 9$
2. $n = 12, m = 18$
3. $n = 123, m = 277$
4. $n = 100, m = 101$
5. $n = 1001, m = 1331$

No olvide hacer las tablas para cada caso:

Paso	n	m	q	r
0				
1				
2				
3				
4				
5				

Del Paso	$r =$
5	
4	
3	
2	
1	
0	

Plan

1. Motivación
2. La naturaleza de $\mathbb{N}$ y sus representaciones
3. Divisibilidad
   - Definiciones
   - Teoremas
   - Algoritmo de la división
4. Divisores y múltiplos comunes y números Primos
   - Números primos
   - Divisores y múltiplos comunes
   - Algoritmo de Euclides
5. Congruencias
   - Definición y Propiedades
   - Aplicaciones

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$
  - $a \equiv_n a$
  - $a \equiv_n b \implies b \equiv_n a$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a * c) \equiv_n (b * d)$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$
  - $a \equiv_n a$
  - $a \equiv_n b \implies b \equiv_n a$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a \times c) \equiv_n (b \times d)$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$ $\qquad 17 \mod 6 = 5 \wedge 5 \mod 6 = 5$
  - $a \equiv_n a$
  - $a \equiv_n b \implies b \equiv_n a$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$ $\quad 17 \mod 6 = 5 \wedge 5 \mod 6 = 5$
  - $a \equiv_n a$
  - $a \equiv_n b \implies b \equiv_n a$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$ $\quad 17 \mod 6 = 5 \wedge 5 \mod 6 = 5$
  - $a \equiv_n a$ $\quad 17 \equiv_6 17$
  - $a \equiv_n b \implies b \equiv_n a$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$ $\quad$ $17 \mod 6 = 5 \wedge 5 \mod 6 = 5$
  - $a \equiv_n a$ $\quad$ $17 \equiv_6 17$
  - $a \equiv_n b \implies b \equiv_n a$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$ $\quad$ $17 \mod 6 = 5 \wedge 5 \mod 6 = 5$
  - $a \equiv_n a$ $\quad$ $17 \equiv_6 17$
  - $a \equiv_n b \implies b \equiv_n a$ $\quad$ $17 \equiv_6 5 \wedge 5 \equiv_6 17$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$ $\quad$ $17 \mod 6 = 5 \wedge 5 \mod 6 = 5$
  - $a \equiv_n a$ $\quad$ $17 \equiv_6 17$
  - $a \equiv_n b \implies b \equiv_n a$ $\quad$ $17 \equiv_6 5 \wedge 5 \equiv_6 17$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$ — $17 \mod 6 = 5 \wedge 5 \mod 6 = 5$
  - $a \equiv_n a$ — $17 \equiv_6 17$
  - $a \equiv_n b \implies b \equiv_n a$ — $17 \equiv_6 5 \wedge 5 \equiv_6 17$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$ — $17 \equiv_6 5 \wedge 5 \equiv_6 11 \implies 17 \equiv_6 11$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not| (24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$ $\quad 17 \mod 6 = 5 \wedge 5 \mod 6 = 5$
  - $a \equiv_n a$ $\quad 17 \equiv_6 17$
  - $a \equiv_n b \implies b \equiv_n a$ $\quad 17 \equiv_6 5 \wedge 5 \equiv_6 17$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$ $\quad 17 \equiv_6 5 \wedge 5 \equiv_6 11 \implies 17 \equiv_6 11$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$

    $17 \equiv_6 5 \wedge 4 \equiv_6 10 \implies 21 \equiv_6 15$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$ $\quad 17 \mod 6 = 5 \wedge 5 \mod 6 = 5$
  - $a \equiv_n a$ $\quad 17 \equiv_6 17$
  - $a \equiv_n b \implies b \equiv_n a$ $\quad 17 \equiv_6 5 \wedge 5 \equiv_6 17$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$ $\quad 17 \equiv_6 5 \wedge 5 \equiv_6 11 \implies 17 \equiv_6 11$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$

    $17 \equiv_6 5 \wedge 4 \equiv_6 10 \implies 21 \equiv_6 15$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$ $\qquad 17 \mod 6 = 5 \wedge 5 \mod 6 = 5$
  - $a \equiv_n a$ $\qquad 17 \equiv_6 17$
  - $a \equiv_n b \implies b \equiv_n a$ $\qquad 17 \equiv_6 5 \wedge 5 \equiv_6 17$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$ $\qquad 17 \equiv_6 5 \wedge 5 \equiv_6 11 \implies 17 \equiv_6 11$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$
    $17 \equiv_6 5 \wedge 4 \equiv_6 10 \implies 21 \equiv_6 15$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$ $\qquad 17 \equiv_6 5 \wedge 4 \equiv_6 10 \implies 68 \equiv_6 50$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$ $\quad 17 \mod 6 = 5 \wedge 5 \mod 6 = 5$
  - $a \equiv_n a$ $\quad 17 \equiv_6 17$
  - $a \equiv_n b \implies b \equiv_n a$ $\quad 17 \equiv_6 5 \wedge 5 \equiv_6 17$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$ $\quad 17 \equiv_6 5 \wedge 5 \equiv_6 11 \implies 17 \equiv_6 11$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$
    $17 \equiv_6 5 \wedge 4 \equiv_6 10 \implies 21 \equiv_6 15$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$ $\quad 17 \equiv_6 5 \wedge 4 \equiv_6 10 \implies 68 \equiv_6 50$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$ $\quad 17 \mod 6 = 5 \wedge 5 \mod 6 = 5$
  - $a \equiv_n a$ $\quad 17 \equiv_6 17$
  - $a \equiv_n b \implies b \equiv_n a$ $\quad 17 \equiv_6 5 \wedge 5 \equiv_6 17$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$ $\quad 17 \equiv_6 5 \wedge 5 \equiv_6 11 \implies 17 \equiv_6 11$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$
    $17 \equiv_6 5 \wedge 4 \equiv_6 10 \implies 21 \equiv_6 15$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$ $\quad 17 \equiv_6 5 \wedge 4 \equiv_6 10 \implies 68 \equiv_6 50$

Congruencias

- Dados $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}^+$, se dice que a es congruente a b módulo n, y se denota $a \equiv_n b$ si $n|(b-a)$

$$a \equiv_n b \equiv n|(b-a)$$

- $17 \equiv_6 5$ pues $6|(17-5) = 12$ y $24 \not\equiv_6 14$ pues $6 \not|(24-14) = 10$
- La relación $\equiv_n$ cumple las siguientes propiedades:
  - $a \equiv_n b \equiv (a \mod n) = (b \mod n)$ $\quad 17 \mod 6 = 5 \wedge 5 \mod 6 = 5$
  - $a \equiv_n a$ $\quad 17 \equiv_6 17$
  - $a \equiv_n b \implies b \equiv_n a$ $\quad 17 \equiv_6 5 \wedge 5 \equiv_6 17$
  - $a \equiv_n b \wedge b \equiv_n c \implies a \equiv_n c$ $\quad 17 \equiv_6 5 \wedge 5 \equiv_6 11 \implies 17 \equiv_6 11$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$
    $17 \equiv_6 5 \wedge 4 \equiv_6 10 \implies 21 \equiv_6 15$
  - $a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$ $\quad 17 \equiv_6 5 \wedge 4 \equiv_6 10 \implies 68 \equiv_6 50$

Probemos algunas propiedades (1)

Teorema: Dos enteros son congruentes módulo n si y solo si sus residuos módulo$n$ son iguales.

$$a \equiv_n b \equiv (a \mod n) = (b \mod n)$$

- Por el algoritmo de la division tenemos que: $a = nq_1 + r_1, 0 \leq r_1 < n, r_1 = a \mod n$, $b = nq_2 + r_2, 0 \leq r_2 < n, r_2 = b \mod n$
- Vamos a probar primero $a \equiv_n b \implies (a \mod n) = (b \mod n)$
- Ahora vamos a probar $(a \mod n) = (b \mod n) \implies a \equiv_n b$

Probemos algunas propiedades (1)

Teorema: Dos enteros son congruentes módulo n si y solo si sus residuos módulo$n$ son iguales.

$$a \equiv_n b \equiv (a \mod n) = (b \mod n)$$

- Por el algoritmo de la division tenemos que:
  $a = nq_1 + r_1, 0 \leq r_1 < n, r_1 = a \mod n$, $b = nq_2 + r_2, 0 \leq r_2 < n, r_2 = b \mod n$
- Vamos a probar primero $a \equiv_n b \implies (a \mod n) = (b \mod n)$
- Ahora vamos a probar $(a \mod n) = (b \mod n) \implies a \equiv_n b$

Probemos algunas propiedades (1)

Teorema: Dos enteros son congruentes módulo n si y solo si sus residuos módulo$n$ son iguales.

$$a \equiv_n b \equiv (a \mod n) = (b \mod n)$$

- Por el algoritmo de la division tenemos que:
  $a = nq_1 + r_1, 0 \leq r_1 < n, r_1 = a \mod n$, $b = nq_2 + r_2, 0 \leq r_2 < n, r_2 = b \mod n$
- Vamos a probar primero $a \equiv_n b \implies (a \mod n) = (b \mod n)$
  $a \equiv_n b \equiv n|(b - a) \equiv n|(n(q_2 - q_1) + (r_2 - r_1))$
- Ahora vamos a probar $(a \mod n) = (b \mod n) \implies a \equiv_n b$

Probemos algunas propiedades (1)

Teorema: Dos enteros son congruentes módulo n si y solo si sus residuos módulo$n$ son iguales.

$$a \equiv_n b \equiv (a \mod n) = (b \mod n)$$

- Por el algoritmo de la division tenemos que:
  $a = nq_1 + r_1, 0 \leq r_1 < n, r_1 = a \mod n$, $b = nq_2 + r_2, 0 \leq r_2 < n, r_2 = b \mod n$
- Vamos a probar primero $a \equiv_n b \implies (a \mod n) = (b \mod n)$
  $a \equiv_n b \equiv n|(b-a) \equiv n|(n(q_2 - q_1) + (r_2 - r_1)) \implies n|(r_2 - r_1)$
  Por otro lado, $-n < r_2 - r_1 < n$ y como $n|(r_2 - r_1)$ entonces $r_2 - r_1 = 0$
  O sea, $r_1 = a \mod n = r_2 = b \mod n$
- Ahora vamos a probar $(a \mod n) = (b \mod n) \implies a \equiv_n b$

Probemos algunas propiedades (1)

Teorema: Dos enteros son congruentes módulo n si y solo si sus residuos módulo$n$ son iguales.

$$a \equiv_n b \equiv (a \mod n) = (b \mod n)$$

- Por el algoritmo de la division tenemos que:
  $a = nq_1 + r_1, 0 \leq r_1 < n, r_1 = a \mod n$, $b = nq_2 + r_2, 0 \leq r_2 < n, r_2 = b \mod n$
- Vamos a probar primero $a \equiv_n b \implies (a \mod n) = (b \mod n)$
  $a \equiv_n b \equiv n|(b-a) \equiv n|(n(q_2 - q_1) + (r_2 - r_1)) \implies n|(r_2 - r_1)$
  Por otro lado, $-n < r_2 - r_1 < n$ y como $n|(r_2 - r_1)$ entonces $r_2 - r_1 = 0$
  O sea, $r_1 = a \mod n = r_2 = b \mod n$
- Ahora vamos a probar $(a \mod n) = (b \mod n) \implies a \equiv_n b$

Probemos algunas propiedades (1)

Teorema: Dos enteros son congruentes módulo n si y solo si sus residuos módulo$n$ son iguales.

$$a \equiv_n b \equiv (a \mod n) = (b \mod n)$$

- Por el algoritmo de la division tenemos que:
  $a = nq_1 + r_1, 0 \leq r_1 < n, r_1 = a \mod n$, $b = nq_2 + r_2, 0 \leq r_2 < n, r_2 = b \mod n$
- Vamos a probar primero $a \equiv_n b \implies (a \mod n) = (b \mod n)$
  $a \equiv_n b \equiv n|(b - a) \equiv n|(n(q_2 - q_1) + (r_2 - r_1)) \implies n|(r_2 - r_1)$
  Por otro lado, $-n < r_2 - r_1 < n$ y como $n|(r_2 - r_1)$ entonces $r_2 - r_1 = 0$
  O sea, $r_1 = a \mod n = r_2 = b \mod n$
- Ahora vamos a probar $(a \mod n) = (b \mod n) \implies a \equiv_n b$

Probemos algunas propiedades (1)

Teorema: Dos enteros son congruentes módulo n si y solo si sus residuos módulo$n$ son iguales.

$$a \equiv_n b \equiv (a \mod n) = (b \mod n)$$

- Por el algoritmo de la division tenemos que:
  $a = nq_1 + r_1, 0 \leq r_1 < n, r_1 = a \mod n$, $b = nq_2 + r_2, 0 \leq r_2 < n, r_2 = b \mod n$
- Vamos a probar primero $a \equiv_n b \implies (a \mod n) = (b \mod n)$
  $a \equiv_n b \equiv n|(b-a) \equiv n|(n(q_2 - q_1) + (r_2 - r_1)) \implies n|(r_2 - r_1)$
  Por otro lado, $-n < r_2 - r_1 < n$ y como $n|(r_2 - r_1)$ entonces $r_2 - r_1 = 0$
  O sea, $r_1 = a \mod n = r_2 = b \mod n$
- Ahora vamos a probar $(a \mod n) = (b \mod n) \implies a \equiv_n b$

Probemos algunas propiedades (1)

Teorema: Dos enteros son congruentes módulo n si y solo si sus residuos módulo$n$ son iguales.

$$a \equiv_n b \equiv (a \mod n) = (b \mod n)$$

- Por el algoritmo de la division tenemos que:
  $a = nq_1 + r_1, 0 \leq r_1 < n, r_1 = a \mod n$, $b = nq_2 + r_2, 0 \leq r_2 < n, r_2 = b \mod n$
- Vamos a probar primero $a \equiv_n b \implies (a \mod n) = (b \mod n)$
  $a \equiv_n b \equiv n|(b-a) \equiv n|(n(q_2 - q_1) + (r_2 - r_1)) \implies n|(r_2 - r_1)$
  Por otro lado, $-n < r_2 - r_1 < n$ y como $n|(r_2 - r_1)$ entonces $r_2 - r_1 = 0$
  O sea, $r_1 = a \mod n = r_2 = b \mod n$
- Ahora vamos a probar $(a \mod n) = (b \mod n) \implies a \equiv_n b$
  $(b-a) = n(q_2 - q_1) + (r_2 - r_1) = n(q_2 - q_1)$, pues $r_1 = r_2$.
  Por tanto, $n|(b-a)$, es decir, $a \equiv_n b$

Probemos algunas propiedades (1)

Teorema: Dos enteros son congruentes módulo n si y solo si sus residuos módulo$n$ son iguales.

$$a \equiv_n b \equiv (a \mod n) = (b \mod n)$$

- Por el algoritmo de la division tenemos que:
  $a = nq_1 + r_1, 0 \leq r_1 < n, r_1 = a \mod n$, $b = nq_2 + r_2, 0 \leq r_2 < n, r_2 = b \mod n$
- Vamos a probar primero $a \equiv_n b \implies (a \mod n) = (b \mod n)$
  $a \equiv_n b \equiv n|(b-a) \equiv n|(n(q_2 - q_1) + (r_2 - r_1)) \implies n|(r_2 - r_1)$
  Por otro lado, $-n < r_2 - r_1 < n$ y como $n|(r_2 - r_1)$ entonces $r_2 - r_1 = 0$
  O sea, $r_1 = a \mod n = r_2 = b \mod n$
- Ahora vamos a probar $(a \mod n) = (b \mod n) \implies a \equiv_n b$
  $(b-a) = n(q_2 - q_1) + (r_2 - r_1) = n(q_2 - q_1)$, pues $r_1 = r_2$.
  Por tanto, $n|(b-a)$, es decir, $a \equiv_n b$

Probemos algunas propiedades (1)

Teorema: Dos enteros son congruentes módulo n si y solo si sus residuos módulo$n$ son iguales.

$$a \equiv_n b \equiv (a \mod n) = (b \mod n)$$

- Por el algoritmo de la division tenemos que:
  $a = nq_1 + r_1, 0 \leq r_1 < n, r_1 = a \mod n$, $b = nq_2 + r_2, 0 \leq r_2 < n, r_2 = b \mod n$
- Vamos a probar primero $a \equiv_n b \implies (a \mod n) = (b \mod n)$
  $a \equiv_n b \equiv n|(b-a) \equiv n|(n(q_2 - q_1) + (r_2 - r_1)) \implies n|(r_2 - r_1)$
  Por otro lado, $-n < r_2 - r_1 < n$ y como $n|(r_2 - r_1)$ entonces $r_2 - r_1 = 0$
  O sea, $r_1 = a \mod n = r_2 = b \mod n$
- Ahora vamos a probar $(a \mod n) = (b \mod n) \implies a \equiv_n b$
  $(b-a) = n(q_2 - q_1) + (r_2 - r_1) = n(q_2 - q_1)$, pues $r_1 = r_2$.
  Por tanto, $n|(b-a)$, es decir, $a \equiv_n b$

Probemos algunas propiedades (1)

Teorema: Dos enteros son congruentes módulo n si y solo si sus residuos módulo$n$ son iguales.

$$a \equiv_n b \equiv (a \mod n) = (b \mod n)$$

- Por el algoritmo de la division tenemos que:
  $a = nq_1 + r_1, 0 \leq r_1 < n, r_1 = a \mod n$, $b = nq_2 + r_2, 0 \leq r_2 < n, r_2 = b \mod n$
- Vamos a probar primero $a \equiv_n b \implies (a \mod n) = (b \mod n)$
  $a \equiv_n b \equiv n|(b-a) \equiv n|(n(q_2-q_1)+(r_2-r_1)) \implies n|(r_2-r_1)$
  Por otro lado, $-n < r_2 - r_1 < n$ y como $n|(r_2-r_1)$ entonces $r_2 - r_1 = 0$
  O sea, $r_1 = a \mod n = r_2 = b \mod n$
- Ahora vamos a probar $(a \mod n) = (b \mod n) \implies a \equiv_n b$
  $(b-a) = n(q_2-q_1) + (r_2-r_1) = n(q_2-q_1)$, pues $r_1 = r_2$.
  Por tanto, $n|(b-a)$, es decir, $a \equiv_n b$

Probemos algunas propiedades (2)

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$$

- Por definición de $\equiv_n$ tenemos que:
  $n|(b-a)$, $n|(d-c)$
- Entonces, por teorema de divisibilidad, $n|(b-a)+(d-c)$ lo que es lo mismo que decir $n|(b+d)-(a+c)$, es decir $(a+c) \equiv_n (b+d)$

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$$

- Por definición de $\equiv_n$ tenemos que:
- Entonces, por teorema de divisibilidad, $n|(b-a)*c+(d-c)*b$ lo que es lo mismo que decir $n|(bc-ac+bd-bc)$, o sea $n|(bd-ac)$, es decir $(a*c) \equiv_n (b*d)$

Probemos algunas propiedades (2)

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a + c) \equiv_n (b + d)$$

- Por definición de $\equiv_n$ tenemos que:
  $n|(b - a)$, $n|(d - c)$
- Entonces, por teorema de divisibilidad, $n|(b - a) + (d - c)$ lo que es lo mismo que decir $n|(b + d) - (a + c)$, es decir $(a + c) \equiv_n (b + d)$

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a * c) \equiv_n (b * d)$$

- Por definición de $\equiv_n$ tenemos que:
- Entonces, por teorema de divisibilidad, $n|(b - a) * c + (d - c) * b$ lo que es lo mismo que decir $n|(bc - ac + bd - bc)$, o sea $n|(bd - ac)$, es decir $(a * c) \equiv_n (b * d)$

Probemos algunas propiedades (2)

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a + c) \equiv_n (b + d)$$

- Por definición de $\equiv_n$ tenemos que:
  $n|(b - a)$, $n|(d - c)$
- Entonces, por teorema de divisibilidad, $n|(b - a) + (d - c)$ lo que es lo mismo que decir $n|(b + d) - (a + c)$, es decir $(a + c) \equiv_n (b + d)$

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a * c) \equiv_n (b * d)$$

- Por definición de $\equiv_n$ tenemos que:
- Entonces, por teorema de divisibilidad, $n|(b - a) * c + (d - c) * b$ lo que es lo mismo que decir $n|(bc - ac + bd - bc)$, o sea $n|(bd - ac)$, es decir $(a * c) \equiv_n (b * d)$

Probemos algunas propiedades (2)

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a + c) \equiv_n (b + d)$$

- Por definición de $\equiv_n$ tenemos que:
  $n|(b - a)$, $n|(d - c)$
- Entonces, por teorema de divisibilidad, $n|(b - a) + (d - c)$ lo que es lo mismo que decir $n|(b + d) - (a + c)$, es decir $(a + c) \equiv_n (b + d)$

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a * c) \equiv_n (b * d)$$

- Por definición de $\equiv_n$ tenemos que:
  $n|(b - a)$, $n|(d - c)$
- Entonces, por teorema de divisibilidad, $n|(b - a) * c + (d - c) * b$ lo que es lo mismo que decir $n|(bc - ac + bd - bc)$, o sea $n|(bd - ac)$, es decir $(a * c) \equiv_n (b * d)$

Probemos algunas propiedades (2)

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$$

- Por definición de $\equiv_n$ tenemos que:
  $n|(b-a)$, $n|(d-c)$
- Entonces, por teorema de divisibilidad, $n|(b-a)+(d-c)$ lo que es lo mismo que decir $n|(b+d)-(a+c)$, es decir $(a+c) \equiv_n (b+d)$

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$$

- Por definición de $\equiv_n$ tenemos que:
  $n|(b-a)$, $n|(d-c)$
- Entonces, por teorema de divisibilidad, $n|(b-a)*c+(d-c)*b$ lo que es lo mismo que decir $n|(bc-ac+bd-bc)$, o sea $n|(bd-ac)$, es decir $(a*c) \equiv_n (b*d)$

Probemos algunas propiedades (2)

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a + c) \equiv_n (b + d)$$

- Por definición de $\equiv_n$ tenemos que:
  $n|(b - a)$, $n|(d - c)$
- Entonces, por teorema de divisibilidad, $n|(b - a) + (d - c)$ lo que es lo mismo que decir $n|(b + d) - (a + c)$, es decir $(a + c) \equiv_n (b + d)$

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a * c) \equiv_n (b * d)$$

- Por definición de $\equiv_n$ tenemos que:
  $n|(b - a)$, $n|(d - c)$
- Entonces, por teorema de divisibilidad, $n|(b - a) * c + (d - c) * b$ lo que es lo mismo que decir $n|(bc - ac + bd - bc)$, o sea $n|(bd - ac)$, es decir $(a * c) \equiv_n (b * d)$

Probemos algunas propiedades (2)

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$$

- Por definición de $\equiv_n$ tenemos que: $n|(b-a)$, $n|(d-c)$
- Entonces, por teorema de divisibilidad, $n|(b-a)+(d-c)$ lo que es lo mismo que decir $n|(b+d)-(a+c)$, es decir $(a+c) \equiv_n (b+d)$

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$$

- Por definición de $\equiv_n$ tenemos que: $n|(b-a)$, $n|(d-c)$
- Entonces, por teorema de divisibilidad, $n|(b-a)*c+(d-c)*b$ lo que es lo mismo que decir $n|(bc-ac+bd-bc)$, o sea $n|(bd-ac)$, es decir $(a*c) \equiv_n (b*d)$

Probemos algunas propiedades (2)

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a+c) \equiv_n (b+d)$$

- Por definición de $\equiv_n$ tenemos que:
  $n|(b-a)$, $n|(d-c)$
- Entonces, por teorema de divisibilidad, $n|(b-a)+(d-c)$ lo que es lo mismo que decir $n|(b+d)-(a+c)$, es decir $(a+c) \equiv_n (b+d)$

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a*c) \equiv_n (b*d)$$

- Por definición de $\equiv_n$ tenemos que:
  $n|(b-a)$, $n|(d-c)$
- Entonces, por teorema de divisibilidad, $n|(b-a)*c+(d-c)*b$ lo que es lo mismo que decir $n|(bc-ac+bd-bc)$, o sea $n|(bd-ac)$, es decir $(a*c) \equiv_n (b*d)$

Probemos algunas propiedades (2)

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a + c) \equiv_n (b + d)$$

- Por definición de $\equiv_n$ tenemos que: $n|(b-a)$, $n|(d-c)$
- Entonces, por teorema de divisibilidad, $n|(b-a)+(d-c)$ lo que es lo mismo que decir $n|(b+d)-(a+c)$, es decir $(a+c) \equiv_n (b+d)$

Teorema:

$$a \equiv_n b \wedge c \equiv_n d \implies (a * c) \equiv_n (b * d)$$

- Por definición de $\equiv_n$ tenemos que: $n|(b-a)$, $n|(d-c)$
- Entonces, por teorema de divisibilidad, $n|(b-a)*c+(d-c)*b$ lo que es lo mismo que decir $n|(bc-ac+bd-bc)$, o sea $n|(bd-ac)$, es decir $(a*c) \equiv_n (b*d)$

Propiedades de las congruencias que cambian el módulo

Sean, $a, x, y, d, m, n \in \mathbb{Z}$; $d, n \neq 0$; $a, m > 0$

- $a * x \equiv_m a * y \equiv x \equiv_{\frac{m}{mcd(a,m)}} y$ $\qquad 20 \equiv_{10} 30 \equiv 4 \equiv_2 6$
- $a * x \equiv_m a * y \wedge mcd(a, m) = 1 \implies x \equiv_m y$
  $mcd(6, 5) = 1$
- $x \equiv_m y \wedge d|m \implies x \equiv_d y$
- $x \equiv_m y \wedge x \equiv_n y \equiv x \equiv_{mcm(m,n)} y$

Propiedades de las congruencias que cambian el módulo

Sean, $a, x, y, d, m, n \in \mathbb{Z}$; $d, n \neq 0$; $a, m > 0$

- $a * x \equiv_m a * y \equiv x \equiv_{\frac{m}{mcd(a,m)}} y$ $\quad 20 \equiv_{10} 30 \equiv 4 \equiv_2 6$
- $a * x \equiv_m a * y \wedge mcd(a, m) = 1 \implies x \equiv_m y$ $\quad 30 \equiv_5 60 \implies 5 \equiv_5 10$ pues $mcd(6, 5) = 1$
- $x \equiv_m y \wedge d|m \implies x \equiv_d y$
- $x \equiv_m y \wedge x \equiv_n y \equiv x \equiv_{mcm(m,n)} y$

Propiedades de las congruencias que cambian el módulo

Sean, $a, x, y, d, m, n \in \mathbb{Z}; d, n \neq 0; a, m > 0$

- $a * x \equiv_m a * y \equiv x \equiv_{\frac{m}{mcd(a,m)}} y$ $\quad$ $20 \equiv_{10} 30 \equiv 4 \equiv_2 6$
- $a * x \equiv_m a * y \wedge mcd(a, m) = 1 \implies x \equiv_m y$ $\quad$ $30 \equiv_5 60 \implies 5 \equiv_5 10$ pues $mcd(6, 5) = 1$
- $x \equiv_m y \wedge d|m \implies x \equiv_d y$ $\quad$ $20 \equiv_{10} 30 \implies 20 \equiv_5 30 \wedge 20 \equiv_2 30$ pues $2|10 \wedge 5|10$
- $x \equiv_m y \wedge x \equiv_n y \equiv x \equiv_{mcm(m,n)} y$

Propiedades de las congruencias que cambian el módulo

Sean, $a, x, y, d, m, n \in \mathbb{Z}$; $d, n \neq 0$; $a, m > 0$

- $a * x \equiv_m a * y \equiv x \equiv_{\frac{m}{mcd(a,m)}} y$ $\quad$ $20 \equiv_{10} 30 \equiv 4 \equiv_2 6$
- $a * x \equiv_m a * y \wedge mcd(a, m) = 1 \implies x \equiv_m y$ $\quad$ $30 \equiv_5 60 \implies 5 \equiv_5 10$ pues $mcd(6, 5) = 1$
- $x \equiv_m y \wedge d|m \implies x \equiv_d y$ $\quad$ $20 \equiv_{10} 30 \implies 20 \equiv_2 30 \wedge 20 \equiv_5 30$ pues $2|10 \wedge 5|10$
- $x \equiv_m y \wedge x \equiv_n y \equiv x \equiv_{mcm(m,n)} y$

Propiedades de las congruencias que cambian el módulo

Sean, $a, x, y, d, m, n \in \mathbb{Z}$; $d, n \neq 0$; $a, m > 0$

- $a * x \equiv_m a * y \equiv x \equiv_{\frac{m}{mcd(a,m)}} y$ $\quad 20 \equiv_{10} 30 \equiv 4 \equiv_2 6$
- $a * x \equiv_m a * y \wedge mcd(a, m) = 1 \implies x \equiv_m y$ $\quad 30 \equiv_5 60 \implies 5 \equiv_5 10$ pues $mcd(6, 5) = 1$
- $x \equiv_m y \wedge d|m \implies x \equiv_d y$ $\quad 20 \equiv_{10} 30 \implies 20 \equiv_2 30 \wedge 20 \equiv_5 30$ pues $2|10 \wedge 5|10$
- $x \equiv_m y \wedge x \equiv_n y \equiv x \equiv_{mcm(m,n)} y$

Propiedades de las congruencias que cambian el módulo

Sean, $a, x, y, d, m, n \in \mathbb{Z}$; $d, n \neq 0$; $a, m > 0$

- $a * x \equiv_m a * y \equiv x \equiv_{\frac{m}{mcd(a,m)}} y$ $\quad 20 \equiv_{10} 30 \equiv 4 \equiv_2 6$
- $a * x \equiv_m a * y \wedge mcd(a, m) = 1 \implies x \equiv_m y$ $\quad 30 \equiv_5 60 \implies 5 \equiv_5 10$ pues $mcd(6, 5) = 1$
- $x \equiv_m y \wedge d|m \implies x \equiv_d y$ $\quad 20 \equiv_{10} 30 \implies 20 \equiv_2 30 \wedge 20 \equiv_5 30$ pues $2|10 \wedge 5|10$
- $x \equiv_m y \wedge x \equiv_n y \equiv x \equiv_{mcm(m,n)} y$ $\quad 2 \equiv_2 14 \wedge 2 \equiv_3 14 \equiv 2 \equiv_6 14$

Propiedades de las congruencias que cambian el módulo

Sean, $a, x, y, d, m, n \in \mathbb{Z}; d, n \neq 0; a, m > 0$

- $a * x \equiv_m a * y \equiv x \equiv_{\frac{m}{mcd(a,m)}} y$ $\quad 20 \equiv_{10} 30 \equiv 4 \equiv_2 6$
- $a * x \equiv_m a * y \wedge mcd(a, m) = 1 \implies x \equiv_m y$ $\quad 30 \equiv_5 60 \implies 5 \equiv_5 10$ pues $mcd(6, 5) = 1$
- $x \equiv_m y \wedge d|m \implies x \equiv_d y$ $\quad 20 \equiv_{10} 30 \implies 20 \equiv_2 30 \wedge 20 \equiv_5 30$ pues $2|10 \wedge 5|10$
- $x \equiv_m y \wedge x \equiv_n y \equiv x \equiv_{mcm(m,n)} y$ $\quad 2 \equiv_2 14 \wedge 2 \equiv_3 14 \equiv 2 \equiv_6 14$

Propiedades de las congruencias que cambian el módulo

Sean, $a, x, y, d, m, n \in \mathbb{Z}; d, n \neq 0; a, m > 0$

- $a * x \equiv_m a * y \equiv x \equiv_{\frac{m}{mcd(a,m)}} y$ $\quad 20 \equiv_{10} 30 \equiv 4 \equiv_2 6$
- $a * x \equiv_m a * y \wedge mcd(a, m) = 1 \implies x \equiv_m y$ $\quad 30 \equiv_5 60 \implies 5 \equiv_5 10$ pues $mcd(6, 5) = 1$
- $x \equiv_m y \wedge d|m \implies x \equiv_d y$ $\quad 20 \equiv_{10} 30 \implies 20 \equiv_2 30 \wedge 20 \equiv_5 30$ pues $2|10 \wedge 5|10$
- $x \equiv_m y \wedge x \equiv_n y \equiv x \equiv_{mcm(m,n)} y$ $\quad 2 \equiv_2 14 \wedge 2 \equiv_3 14 \equiv 2 \equiv_6 14$

Plan

1. Motivación
2. La naturaleza de $\mathbb{N}$ y sus representaciones
3. Divisibilidad
   - Definiciones
   - Teoremas
   - Algoritmo de la división
4. Divisores y múltiplos comunes y números Primos
   - Números primos
   - Divisores y múltiplos comunes
   - Algoritmo de Euclides
5. Congruencias
   - Definición y Propiedades
   - Aplicaciones

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5)
- $n \equiv_5 d_0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5)
- $n \equiv_5 d_0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5)
- $n \equiv_5 d_0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5)
- $n \equiv_5 d_0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5)
- $n \equiv_5 d_0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5) $10^i \equiv_3 1$
- $n \equiv_5 d_0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5) $10^i \equiv_3 1$
- $n \equiv_5 d_0$ $10^i \equiv_5 0, i > 0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5) $10^i \equiv_3 1$
- $n \equiv_5 d_0$ $10^i \equiv_5 0, i > 0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5) $\qquad 10^i \equiv_3 1$
- $n \equiv_5 d_0 \qquad 10^i \equiv_5 0, i > 0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5) $\quad 10^i \equiv_3 1$
- $n \equiv_5 d_0$ $\quad 10^i \equiv_5 0, i > 0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$ $\quad 10^i \equiv_9 1$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5) $\qquad 10^i \equiv_3 1$
- $n \equiv_5 d_0$ $\qquad 10^i \equiv_5 0, i > 0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$ $\qquad 10^i \equiv_9 1$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$ $\qquad 10^i \equiv_{11} 1, i$ es par $\wedge\ 10^i \equiv_{11} -1, i$ es impar

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5) $\qquad 10^i \equiv_3 1$
- $n \equiv_5 d_0$ $\qquad 10^i \equiv_5 0, i > 0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$ $\qquad 10^i \equiv_9 1$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$ $\qquad 10^i \equiv_{11} 1, i$ es par $\wedge$ $10^i \equiv_{11} -1, i$ es impar

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5) $10^i \equiv_3 1$
- $n \equiv_5 d_0$ $10^i \equiv_5 0, i > 0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$ $10^i \equiv_9 1$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$ $10^i \equiv_{11} 1, i$ es par $\wedge\ 10^i \equiv_{11} -1, i$ es impar

Pruebas de divisibilidad

Recuerde las reglas de divisibilidad que nos enseñaron en el colegio:

- Un número es divisible por 3 si la suma de sus dígitos es divisible por 3.
- Un número es divisible por 5 si el último dígito es 0 o 5.
- Un número es divisible por 9 si la suma de sus dígitos es divisible por 9.
- Un número es divisible por 11 si la suma de sus dígitos en posición par menos la suma de sus dígitos en posición impar es divisible por 11.

¿Porqué funcionan? $n = \sum_{i=0}^{k} d_i * 10^i$, donde los d_i son los dígitos con que se escribe n en notación decimal

- $n \equiv_3 \sum_{i=0}^{k} d_i$ (Video 3.5) $\quad 10^i \equiv_3 1$
- $n \equiv_5 d_0$ $\quad 10^i \equiv_5 0, i > 0$
- $n \equiv_9 \sum_{i=0}^{k} d_i$ $\quad 10^i \equiv_9 1$
- $n \equiv_{11} \sum_{i=0}^{k} (-1)^i d_i$ $\quad 10^i \equiv_{11} 1, i$ es par $\wedge\ 10^i \equiv_{11} -1, i$ es impar

Teoremas de Fermat y Euler

- Teorema de Fermat: p primo $\wedge \neg(p|a) \implies a^{p-1} \equiv_p 1$
- Calcule $7^{222} \mod 11$ Por el teorema de Fermat, $7^{10} \equiv_{11} 1$ Como $222 = 10 * 22 + 2$, entonces $7^{222} = 7^{10*22+2} = (7^{10})^{22} 7^2 \equiv_{11} 49 \equiv_{11} 5$
- Primos relativos. Dados $m, n \in \mathbb{N}$ se dice que m y n son primos relativos (y se escribirá $m \perp n$) si el único divisor común es 1.

$$m \perp n \equiv mcd(m, n) = 1$$

- Función φ de Euler. $\varphi : \mathbb{N} \to \mathbb{N}$ tal que $\varphi(n)$ es el número de primos relativos con n menores o iguales a n. $\varphi(n) = (+k|0 < k \leq n \wedge k \perp n : 1)$
  Por ejemplo, $\varphi(6) = 2$, $\varphi(10) = 4$.
- Teorema: $\varphi(n) = n * (*p| \ p|n \wedge p \text{ es primo} : 1 - 1/p)$
- Si p es primo, $\varphi(p) = p(1 - 1/p) = p(p-1)/p = p - 1$
- Teorema de Euler: $a \perp m \implies a^{\varphi(m)} \equiv_m 1$

Teoremas de Fermat y Euler

- Teorema de Fermat: p primo $\wedge \neg(p|a) \implies a^{p-1} \equiv_p 1$
- Calcule $7^{222} \mod 11$ Por el teorema de Fermat, $7^{10} \equiv_{11} 1$ Como $222 = 10 * 22 + 2$, entonces $7^{222} = 7^{10*22+2} = (7^{10})^{22} 7^2 \equiv_{11} 49 \equiv_{11} 5$
- Primos relativos. Dados $m, n \in \mathbb{N}$ se dice que m y n son primos relativos (y se escribirá $m \perp n$) si el único divisor común es 1.

$$m \perp n \equiv mcd(m, n) = 1$$

- Función φ de Euler. $\varphi : \mathbb{N} \to \mathbb{N}$ tal que $\varphi(n)$ es el número de primos relativos con n menores o iguales a n. $\varphi(n) = (+k|0 < k \leq n \wedge k \perp n : 1)$
  Por ejemplo, $\varphi(6) = 2$, $\varphi(10) = 4$.
- Teorema: $\varphi(n) = n * (*p| \ p|n \wedge p \text{ es primo} : 1 - 1/p)$
- Si p es primo, $\varphi(p) = p(1 - 1/p) = p(p-1)/p = p - 1$
- Teorema de Euler: $a \perp m \implies a^{\varphi(m)} \equiv_m 1$

Teoremas de Fermat y Euler

- Teorema de Fermat: p primo $\wedge \neg(p|a) \implies a^{p-1} \equiv_p 1$
- Calcule $7^{222} \mod 11$ Por el teorema de Fermat, $7^{10} \equiv_{11} 1$ Como $222 = 10 * 22 + 2$, entonces $7^{222} = 7^{10*22+2} = (7^{10})^{22} 7^2 \equiv_{11} 49 \equiv_{11} 5$
- Primos relativos. Dados $m, n \in \mathbb{N}$ se dice que m y n son primos relativos (y se escribirá $m \perp n$) si el único divisor común es 1.

$$m \perp n \equiv mcd(m, n) = 1$$

- Función φ de Euler. $\varphi : \mathbb{N} \to \mathbb{N}$ tal que $\varphi(n)$ es el número de primos relativos con n menores o iguales a n. $\varphi(n) = (+k|0 < k \leq n \wedge k \perp n : 1)$
Por ejemplo, $\varphi(6) = 2$, $\varphi(10) = 4$.
- Teorema: $\varphi(n) = n * (*p| \ p|n \wedge p \text{ es primo} : 1 - 1/p)$
- Si p es primo, $\varphi(p) = p(1 - 1/p) = p(p-1)/p = p - 1$
- Teorema de Euler: $a \perp m \implies a^{\varphi(m)} \equiv_m 1$

Teoremas de Fermat y Euler

- Teorema de Fermat: p primo $\wedge \neg(p|a) \implies a^{p-1} \equiv_p 1$
- Calcule $7^{222} \mod 11$ Por el teorema de Fermat, $7^{10} \equiv_{11} 1$ Como $222 = 10 * 22 + 2$, entonces $7^{222} = 7^{10*22+2} = (7^{10})^{22} 7^2 \equiv_{11} 49 \equiv_{11} 5$
- Primos relativos. Dados $m, n \in \mathbb{N}$ se dice que m y n son primos relativos (y se escribirá $m \perp n$) si el único divisor común es 1.

$$m \perp n \equiv mcd(m, n) = 1$$

- Función φ de Euler. $\varphi : \mathbb{N} \to \mathbb{N}$ tal que $\varphi(n)$ es el número de primos relativos con n menores o iguales a n. $\varphi(n) = (+k | 0 < k \leq n \wedge k \perp n : 1)$
  Por ejemplo, $\varphi(6) = 2$, $\varphi(10) = 4$.
- Teorema: $\varphi(n) = n * (*p| \ \ p|n \wedge p \text{ es primo} : 1 - 1/p)$
- Si p es primo, $\varphi(p) = p(1 - 1/p) = p(p-1)/p = p - 1$
- Teorema de Euler: $a \perp m \implies a^{\varphi(m)} \equiv_m 1$

Teoremas de Fermat y Euler

- Teorema de Fermat: p primo $\wedge \neg(p|a) \implies a^{p-1} \equiv_p 1$
- Calcule $7^{222} \mod 11$ Por el teorema de Fermat, $7^{10} \equiv_{11} 1$ Como $222 = 10 * 22 + 2$, entonces $7^{222} = 7^{10*22+2} = (7^{10})^{22} 7^2 \equiv_{11} 49 \equiv_{11} 5$
- Primos relativos. Dados $m, n \in \mathbb{N}$ se dice que m y n son primos relativos (y se escribirá $m \perp n$) si el único divisor común es 1.

$$m \perp n \equiv mcd(m, n) = 1$$

- Función φ de Euler. $\varphi : \mathbb{N} \to \mathbb{N}$ tal que $\varphi(n)$ es el número de primos relativos con n menores o iguales a n. $\varphi(n) = (+k|0 < k \leq n \wedge k \perp n : 1)$
  Por ejemplo, $\varphi(6) = 2$, $\varphi(10) = 4$.
- Teorema: $\varphi(n) = n * (*p| \quad p|n \wedge p \text{ es primo} : 1 - 1/p)$
- Si p es primo, $\varphi(p) = p(1 - 1/p) = p(p-1)/p = p - 1$
- Teorema de Euler: $a \perp m \implies a^{\varphi(m)} \equiv_m 1$

Teoremas de Fermat y Euler

- Teorema de Fermat: p primo $\wedge \neg(p|a) \implies a^{p-1} \equiv_p 1$
- Calcule $7^{222} \mod 11$ Por el teorema de Fermat, $7^{10} \equiv_{11} 1$ Como $222 = 10 * 22 + 2$, entonces $7^{222} = 7^{10*22+2} = (7^{10})^{22} 7^2 \equiv_{11} 49 \equiv_{11} 5$
- Primos relativos. Dados $m, n \in \mathbb{N}$ se dice que m y n son primos relativos (y se escribirá $m \perp n$) si el único divisor común es 1.

$$m \perp n \equiv mcd(m, n) = 1$$

- Función φ de Euler. $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ tal que $\varphi(n)$ es el número de primos relativos con n menores o iguales a n. $\varphi(n) = (+k | 0 < k \leq n \wedge k \perp n : 1)$
Por ejemplo, $\varphi(6) = 2$, $\varphi(10) = 4$.
- Teorema: $\varphi(n) = n * (*p| \ \ p|n \wedge p \text{ es primo} : 1 - 1/p)$
- Si p es primo, $\varphi(p) = p(1 - 1/p) = p(p-1)/p = p - 1$
- Teorema de Euler: $a \perp m \implies a^{\varphi(m)} \equiv_m 1$

Teoremas de Fermat y Euler

- Teorema de Fermat: p primo $\wedge \neg(p|a) \implies a^{p-1} \equiv_p 1$
- Calcule $7^{222} \mod 11$ Por el teorema de Fermat, $7^{10} \equiv_{11} 1$ Como $222 = 10 * 22 + 2$, entonces $7^{222} = 7^{10*22+2} = (7^{10})^{22}7^2 \equiv_{11} 49 \equiv_{11} 5$
- Primos relativos. Dados $m, n \in \mathbb{N}$ se dice que m y n son primos relativos (y se escribirá $m \perp n$) si el único divisor común es 1.

$$m \perp n \equiv mcd(m, n) = 1$$

- Función φ de Euler. $\varphi : \mathbb{N} \to \mathbb{N}$ tal que $\varphi(n)$ es el número de primos relativos con n menores o iguales a n. $\varphi(n) = (+k|0 < k \leq n \wedge k \perp n : 1)$
Por ejemplo, $\varphi(6) = 2$, $\varphi(10) = 4$.
- Teorema: $\varphi(n) = n * (*p| \ \ p|n \wedge p \text{ es primo} : 1 - 1/p)$
- Si p es primo, $\varphi(p) = p(1 - 1/p) = p(p-1)/p = p - 1$
- Teorema de Euler: $a \perp m \implies a^{\varphi(m)} \equiv_m 1$

Teoremas de Fermat y Euler

- Teorema de Fermat: p primo $\wedge \neg(p|a) \implies a^{p-1} \equiv_p 1$
- Calcule $7^{222} \mod 11$ Por el teorema de Fermat, $7^{10} \equiv_{11} 1$ Como $222 = 10 * 22 + 2$, entonces $7^{222} = 7^{10*22+2} = (7^{10})^{22} 7^2 \equiv_{11} 49 \equiv_{11} 5$
- Primos relativos. Dados $m, n \in \mathbb{N}$ se dice que m y n son primos relativos (y se escribirá $m \perp n$) si el único divisor común es 1.

$$m \perp n \equiv mcd(m, n) = 1$$

- Función φ de Euler. $\varphi : \mathbb{N} \to \mathbb{N}$ tal que $\varphi(n)$ es el número de primos relativos con n menores o iguales a n. $\varphi(n) = (+k | 0 < k \leq n \wedge k \perp n : 1)$
  Por ejemplo, $\varphi(6) = 2$, $\varphi(10) = 4$.
- Teorema: $\varphi(n) = n * (*p| \ \ p|n \wedge p \text{ es primo} : 1 - 1/p)$
- Si p es primo, $\varphi(p) = p(1 - 1/p) = p(p-1)/p = p - 1$
- Teorema de Euler: $a \perp m \implies a^{\varphi(m)} \equiv_m 1$

Teoremas de Fermat y Euler

- Teorema de Fermat: p primo $\wedge \neg(p|a) \implies a^{p-1} \equiv_p 1$
- Calcule $7^{222} \mod 11$ Por el teorema de Fermat, $7^{10} \equiv_{11} 1$ Como $222 = 10 * 22 + 2$, entonces $7^{222} = 7^{10*22+2} = (7^{10})^{22} 7^2 \equiv_{11} 49 \equiv_{11} 5$
- Primos relativos. Dados $m, n \in \mathbb{N}$ se dice que m y n son primos relativos (y se escribirá $m \perp n$) si el único divisor común es 1.

$$m \perp n \equiv mcd(m, n) = 1$$

- Función φ de Euler. $\varphi : \mathbb{N} \to \mathbb{N}$ tal que $\varphi(n)$ es el número de primos relativos con n menores o iguales a n. $\varphi(n) = (+k | 0 < k \leq n \wedge k \perp n : 1)$
  Por ejemplo, $\varphi(6) = 2$, $\varphi(10) = 4$.
- Teorema: $\varphi(n) = n * (*p| \ \ p|n \wedge p \text{ es primo} : 1 - 1/p)$
- Si p es primo, $\varphi(p) = p(1 - 1/p) = p(p-1)/p = p - 1$
- Teorema de Euler: $a \perp m \implies a^{\varphi(m)} \equiv_m 1$

Resolviendo congruencias lineales (Video 3.6)

- Una congruencia de la forma
$$ax \equiv_m b$$
donde $m \in \mathbb{N}, a, b \in \mathbb{Z}$ y x es una variable, se denomina una congruencia lineal.
- Resolver una congruencia consiste en encontrar los valores de x que la satisfacen.
Idea: Buscar $\overline{a} \in \mathbb{Z}$ tal que $\overline{a}a \equiv_m 1$ pues así $x \equiv_m \overline{a}b$
- Resolver $4x \equiv_5 3$.
- Si $a \perp m$, entonces $\overline{a} = a^{\varphi(m)-1}$.
- Otra forma de encontrar $\overline{a}$: Como $a \perp m$, entonces $mcd(a, m) = 1$. Por tanto, existen s, t tales que $as + mt = 1$. Como $mt \equiv_m 0$, entonces $as \equiv_m 1$. Por tanto $\overline{a} = s$.

[Socrative]

Resolviendo congruencias lineales (Video 3.6)

- Una congruencia de la forma
$$ax \equiv_m b$$
donde $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ y x es una variable, se denomina una congruencia lineal.
- Resolver una congruencia consiste en encontrar los valores de x que la satisfacen.
Idea: Buscar $\overline{a} \in \mathbb{Z}$ tal que $\overline{a}a \equiv_m 1$ pues así $x \equiv_m \overline{a}b$
- Resolver $4x \equiv_5 3$. Note que $4*4 = 16 \equiv_5 1$
Por tanto, $4*4x \equiv_5 4*3$, es decir $x \equiv_5 12 \equiv_5 2$
- Si $a \perp m$, entonces $\overline{a} = a^{\varphi(m)-1}$.
- Otra forma de encontrar $\overline{a}$: Como $a \perp m$, entonces $mcd(a, m) = 1$. Por tanto, existen s, t tales que $as + mt = 1$. Como $mt \equiv_m 0$, entonces $as \equiv_m 1$. Por tanto $\overline{a} = s$.

[Socrative]

Resolviendo congruencias lineales (Video 3.6)

- Una congruencia de la forma
$$ax \equiv_m b$$
donde $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ y x es una variable, se denomina una congruencia lineal.
- Resolver una congruencia consiste en encontrar los valores de x que la satisfacen. Idea: Buscar $\bar{a} \in \mathbb{Z}$ tal que $\bar{a}a \equiv_m 1$ pues así $x \equiv_m \bar{a}b$
- Resolver $4x \equiv_5 3$. Note que $4 * 4 = 16 \equiv_5 1$. Por tanto, $4 * 4x \equiv_5 4 * 3$, es decir $x \equiv_5 12 \equiv_5 2$.
- Si $a \perp m$, entonces $\bar{a} = a^{\varphi(m)-1}$.
- Otra forma de encontrar $\bar{a}$: Como $a \perp m$, entonces $mcd(a, m) = 1$. Por tanto, existen s, t tales que $as + mt = 1$. Como $mt \equiv_m 0$, entonces $as \equiv_m 1$. Por tanto $\bar{a} = s$.

[Socrative]

Resolviendo congruencias lineales (Video 3.6)

- Una congruencia de la forma
$$ax \equiv_m b$$
donde $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ y x es una variable, se denomina una congruencia lineal.
- Resolver una congruencia consiste en encontrar los valores de x que la satisfacen. Idea: Buscar $\bar{a} \in \mathbb{Z}$ tal que $\bar{a}a \equiv_m 1$ pues así $x \equiv_m \bar{a}b$
- Resolver $4x \equiv_5 3$. Note que $4 * 4 = 16 \equiv_5 1$
Por tanto, $4 * 4x \equiv_5 4 * 3$, es decir $x \equiv_5 12 \equiv_5 2$
- Si $a \perp m$, entonces $\bar{a} = a^{\varphi(m)-1}$.
- Otra forma de encontrar $\bar{a}$: Como $a \perp m$, entonces $mcd(a, m) = 1$. Por tanto, existen s, t tales que $as + mt = 1$. Como $mt \equiv_m 0$, entonces $as \equiv_m 1$. Por tanto $\bar{a} = s$.

[Socrative]

Resolviendo congruencias lineales (Video 3.6)

- Una congruencia de la forma
$$ax \equiv_m b$$
donde $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ y x es una variable, se denomina una congruencia lineal.
- Resolver una congruencia consiste en encontrar los valores de x que la satisfacen. Idea: Buscar $\overline{a} \in \mathbb{Z}$ tal que $\overline{a}a \equiv_m 1$ pues así $x \equiv_m \overline{a}b$
- Resolver $4x \equiv_5 3$. Note que $4 * 4 = 16 \equiv_5 1$
Por tanto, $4 * 4x \equiv_5 4 * 3$, es decir $x \equiv_5 12 \equiv_5 2$
- Si $a \perp m$, entonces $\overline{a} = a^{\varphi(m)-1}$.
- Otra forma de encontrar $\overline{a}$: Como $a \perp m$, entonces $mcd(a, m) = 1$. Por tanto, existen s, t tales que $as + mt = 1$. Como $mt \equiv_m 0$, entonces $as \equiv_m 1$. Por tanto $\overline{a} = s$.

[Socrative]

Resolviendo congruencias lineales (Video 3.6)

- Una congruencia de la forma

$$ax \equiv_m b$$

  donde $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ y x es una variable, se denomina una congruencia lineal.
- Resolver una congruencia consiste en encontrar los valores de x que la satisfacen.
  Idea: Buscar $\overline{a} \in \mathbb{Z}$ tal que $\overline{a}a \equiv_m 1$ pues así $x \equiv_m \overline{a}b$
- Resolver $4x \equiv_5 3$. Note que $4 * 4 = 16 \equiv_5 1$
  Por tanto, $4 * 4x \equiv_5 4 * 3$, es decir $x \equiv_5 12 \equiv_5 2$
- Si $a \perp m$, entonces $\overline{a} = a^{\varphi(m)-1}$. Para el caso anterior, $\overline{4} = 4^{\varphi(5)-1} = 4^3 \equiv_5 4$
- Otra forma de encontrar $\overline{a}$: Como $a \perp m$, entonces $mcd(a, m) = 1$. Por tanto, existen s, t tales que $as + mt = 1$. Como $mt \equiv_m 0$, entonces $as \equiv_m 1$. Por tanto $\overline{a} = s$.

[Socrative]

Resolviendo congruencias lineales (Video 3.6)

- Una congruencia de la forma
$$ax \equiv_m b$$
donde $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ y x es una variable, se denomina una congruencia lineal.
- Resolver una congruencia consiste en encontrar los valores de x que la satisfacen.
Idea: Buscar $\overline{a} \in \mathbb{Z}$ tal que $\overline{a}a \equiv_m 1$ pues así $x \equiv_m \overline{a}b$
- Resolver $4x \equiv_5 3$. Note que $4 * 4 = 16 \equiv_5 1$
Por tanto, $4 * 4x \equiv_5 4 * 3$, es decir $x \equiv_5 12 \equiv_5 2$
- Si $a \perp m$, entonces $\overline{a} = a^{\varphi(m)-1}$. Para el caso anterior, $\overline{4} = 4^{\varphi(5)-1} = 4^3 \equiv_5 4$
- Otra forma de encontrar $\overline{a}$: Como $a \perp m$, entonces $mcd(a, m) = 1$. Por tanto, existen s, t tales que $as + mt = 1$. Como $mt \equiv_m 0$, entonces $as \equiv_m 1$. Por tanto $\overline{a} = s$.
Para el caso anterior, $4(4) + 5(-3) = 1$, y entonces $\overline{4} = 4$.

[Socrative]

Resolviendo congruencias lineales (Video 3.6)

- Una congruencia de la forma
$$ax \equiv_m b$$
donde $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ y x es una variable, se denomina una congruencia lineal.
- Resolver una congruencia consiste en encontrar los valores de x que la satisfacen.
Idea: Buscar $\overline{a} \in \mathbb{Z}$ tal que $\overline{a}a \equiv_m 1$ pues así $x \equiv_m \overline{a}b$
- Resolver $4x \equiv_5 3$. Note que $4 * 4 = 16 \equiv_5 1$
Por tanto, $4 * 4x \equiv_5 4 * 3$, es decir $x \equiv_5 12 \equiv_5 2$
- Si $a \perp m$, entonces $\overline{a} = a^{\varphi(m)-1}$. Para el caso anterior, $\overline{4} = 4^{\varphi(5)-1} = 4^3 \equiv_5 4$
- Otra forma de encontrar $\overline{a}$: Como $a \perp m$, entonces $mcd(a, m) = 1$. Por tanto, existen s, t tales que $as + mt = 1$. Como $mt \equiv_m 0$, entonces $as \equiv_m 1$. Por tanto $\overline{a} = s$.
Para el caso anterior, $4(4) + 5(-3) = 1$, y entonces $\overline{4} = 4$.

[Socrative]

Resolviendo congruencias lineales (Video 3.6)

- Una congruencia de la forma
$$ax \equiv_m b$$
donde $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ y x es una variable, se denomina una congruencia lineal.
- Resolver una congruencia consiste en encontrar los valores de x que la satisfacen.
Idea: Buscar $\bar{a} \in \mathbb{Z}$ tal que $\bar{a}a \equiv_m 1$ pues así $x \equiv_m \bar{a}b$
- Resolver $4x \equiv_5 3$. Note que $4 * 4 = 16 \equiv_5 1$
Por tanto, $4 * 4x \equiv_5 4 * 3$, es decir $x \equiv_5 12 \equiv_5 2$
- Si $a \perp m$, entonces $\bar{a} = a^{\varphi(m)-1}$. Para el caso anterior, $\bar{4} = 4^{\varphi(5)-1} = 4^3 \equiv_5 4$
- Otra forma de encontrar $\bar{a}$: Como $a \perp m$, entonces $mcd(a, m) = 1$. Por tanto, existen s, t tales que $as + mt = 1$. Como $mt \equiv_m 0$, entonces $as \equiv_m 1$. Por tanto $\bar{a} = s$.
Para el caso anterior, $4(4) + 5(-3) = 1$, y entonces $\bar{4} = 4$.

[Socrative]

Resolviendo congruencias lineales (Video 3.6)

- Una congruencia de la forma
$$ax \equiv_m b$$
donde $m \in \mathbb{N}, a, b \in \mathbb{Z}$ y x es una variable, se denomina una congruencia lineal.
- Resolver una congruencia consiste en encontrar los valores de x que la satisfacen.
Idea: Buscar $\overline{a} \in \mathbb{Z}$ tal que $\overline{a}a \equiv_m 1$ pues así $x \equiv_m \overline{a}b$
- Resolver $4x \equiv_5 3$. Note que $4 * 4 = 16 \equiv_5 1$
Por tanto, $4 * 4x \equiv_5 4 * 3$, es decir $x \equiv_5 12 \equiv_5 2$
- Si $a \perp m$, entonces $\overline{a} = a^{\varphi(m)-1}$. Para el caso anterior, $\overline{4} = 4^{\varphi(5)-1} = 4^3 \equiv_5 4$
- Otra forma de encontrar $\overline{a}$: Como $a \perp m$, entonces $mcd(a, m) = 1$. Por tanto, existen s, t tales que $as + mt = 1$. Como $mt \equiv_m 0$, entonces $as \equiv_m 1$. Por tanto $\overline{a} = s$.
Para el caso anterior, $4(4) + 5(-3) = 1$, y entonces $\overline{4} = 4$.

[Socrative]

Resolviendo congruencias lineales (Video 3.6)

- Una congruencia de la forma
$$ax \equiv_m b$$
donde $m \in \mathbb{N}, a, b \in \mathbb{Z}$ y x es una variable, se denomina una congruencia lineal.
- Resolver una congruencia consiste en encontrar los valores de x que la satisfacen.
Idea: Buscar $\overline{a} \in \mathbb{Z}$ tal que $\overline{a}a \equiv_m 1$ pues así $x \equiv_m \overline{a}b$
- Resolver $4x \equiv_5 3$. Note que $4 * 4 = 16 \equiv_5 1$
Por tanto, $4 * 4x \equiv_5 4 * 3$, es decir $x \equiv_5 12 \equiv_5 2$
- Si $a \perp m$, entonces $\overline{a} = a^{\varphi(m)-1}$. Para el caso anterior, $\overline{4} = 4^{\varphi(5)-1} = 4^3 \equiv_5 4$
- Otra forma de encontrar $\overline{a}$: Como $a \perp m$, entonces $mcd(a, m) = 1$. Por tanto, existen s, t tales que $as + mt = 1$. Como $mt \equiv_m 0$, entonces $as \equiv_m 1$. Por tanto $\overline{a} = s$.
Para el caso anterior, $4(4) + 5(-3) = 1$, y entonces $\overline{4} = 4$.

[Socrative]