Máximo común divisor y aplicaciones

Clase 22

IIC 1253

Prof. Cristian Riveros

Outline

Outline

Máximo común divisor

Definición

Sea $a, b \in \mathbb{Z} - \{0\}$.
Se define el **máximo común divisor** $\gcd(a, b)$ de a, b como el mayor número d tal que $d \mid a$ y $d \mid b$.

Ejemplos

$$\gcd(8, 12) = 4 \qquad \gcd(24, 36) = 12 \qquad \gcd(54, 24) = 6$$

En otras palabras, $\gcd(a, b)$ es el $\leq$-máximo del conjunto:

$$D_{a,b} = \{c \in \mathbb{Z} \mid c \mid a \wedge c \mid b\}$$

Para $a, b \in \mathbb{Z} - \{0\}$, ¿siempre existe $\gcd(a, b)$?

¿cómo calculamos $\gcd(a, b)$ para a y b?

Supongamos que queremos calcular $\gcd(287, 91)$.

Si dividimos 287 por 91:

$$287 = 91 \cdot 3 + 14$$

¿cuál es la relación entre 287, 91 y 14?

- Si $d \mid 287$ y $d \mid 91$, entonces $d \mid 14$. (¿por qué?)

$$\{ d \in \mathbb{Z} \mid d \mid 287 \wedge d \mid 91 \} \subseteq \{ d \in \mathbb{Z} \mid d \mid 91 \wedge d \mid 14 \}$$

- Si $d \mid 91$ y $d \mid 14$, entonces $d \mid 287$. (¿por qué?)

$$\{ d \in \mathbb{Z} \mid d \mid 91 \wedge d \mid 14 \} \subseteq \{ d \in \mathbb{Z} \mid d \mid 287 \wedge d \mid 91 \}$$

Por lo tanto, $\gcd(287, 91) = \gcd(91, 14)$

¿cómo calculamos gcd(a, b) para a y b?

Teorema

Para todo $a, b \in \mathbb{Z} - \{0\}$, $\gcd(a,b) \;=\; \gcd(b,(a \ \mathbf{mod}\ b))$.

Demostración: ejercicio.

... ¿para qué nos sirve este resultado?

Ejemplo

$$
\begin{array}{rcl}
287 & = & 91 \cdot 3 + 14 \\
91 & = & 14 \cdot 6 + 7 \\
14 & = & 7 \cdot 2
\end{array}
\qquad
\begin{array}{rcl}
\gcd(287, 91) & = & \gcd(91, 14) \\
\gcd(91, 14) & = & \gcd(14, 7) \\
\gcd(14, 7) & = & 7
\end{array}
$$

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$$

¿cómo calculamos $\gcd(a, b)$ para a y b?

Si $r_0 = a$ y $r_1 = b$ con $a \geq b$, se tiene que:

$$\begin{array}{rcll} r_0 & = & r_1 \cdot q_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 & = & r_2 \cdot q_2 + r_3 & 0 \leq r_3 < r_2 \\ & \vdots & & \vdots \\ r_{n-2} & = & r_{n-1} \cdot q_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} & = & r_n \cdot q_n & \end{array}$$

Por el teorema anterior, tenemos que:

$$\gcd(r_0, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \cdots = \gcd(r_{n-1}, r_n) = r_n$$

Este es el **algoritmo de Euclides**.

Algoritmo de máximo común divisor

Algoritmo de Euclides

input : Números a y b con $a \geq b \geq 0$
output: Máximo común divisor entre a y b

Function `MaximoComúnDivisor` (a, b)
  $x := a$
  $y := b$
  while $y \neq 0$ **do**
    $r := x \textbf{ mod } y$
    $x := y$
    $y := r$
  return x

Demuestre que **tiempo** del algoritmo de Euclides esta en $\mathcal{O}(\log(b))$

Outline

Conjunto generadores

Definición

Sea $a, b \in \mathbb{Z} - \{0\}$.

Se define el conjunto $\langle a, b \rangle$ **generado** por a y b como:

$$\langle a, b \rangle \quad = \quad \{ \ c \in \mathbb{Z} \ \mid \ \exists s, t \in \mathbb{Z}. \ c = sa + tb \ \}$$

Ejemplo

$$\begin{aligned} \langle 2, 3 \rangle \quad &= \quad \{0, 1, 2, 3, 4, 5, 6, 7, 8, \ldots, -1, -2, -3, \ldots\} \\ \langle 6, 15 \rangle \quad &= \quad \{0, 6, 15, 12, 21, 3, \ldots, -6, -15, -12, \ldots\} \end{aligned}$$

¿es cierto que $\langle a, b \rangle = \mathbb{Z}$ para todo $a, b \in \mathbb{Z} - \{0\}$?

Conjunto generadores

Definición

Sea $a, b \in \mathbb{Z} - \{0\}$.
Se define el conjunto $\langle a, b \rangle$ **generado** por a y b como:

$$\langle a, b \rangle \quad = \quad \{ \ c \in \mathbb{Z} \ \mid \ \exists s, t \in \mathbb{Z}. \ c = sa + tb \ \}$$

Se define el conjunto $\langle a_1, \ldots, a_n \rangle$ **generado** por $a_1, \ldots, a_n$ como:

$$\langle a_1, \ldots, a_n \rangle \quad = \quad \{ \ c \in \mathbb{Z} \ \mid \ \exists s_1, \ldots, s_n \in \mathbb{Z}. \ c = s_1 a_1 + s_2 a_2 + \ldots + s_n a_n \ \}$$

¿qué representa el conjunto $\langle a \rangle$, generado por un elemento?

Menor elemento de un conjunto generador

Sea $a, b \in \mathbb{Z} - \{0\}$.
Defina g como el menor número positivo en $\langle a, b\rangle$:

$$g \;=\; \min\left\{\; c \in \langle a, b\rangle \;\middle|\; c > 0 \;\right\}$$

¿por qué existe g?

Preguntas

1. ¿es cierto que $\langle g\rangle \subseteq \langle a, b\rangle$? ✓
2. ¿es cierto que $\langle a, b\rangle \subseteq \langle g\rangle$? ✓

Por lo tanto, $\langle g\rangle = \langle a, b\rangle$.

Menor elemento de un conjunto generador

Sea $a, b \in \mathbb{Z} - \{0\}$.
Defina g como el menor número positivo en $\langle a, b \rangle$:

$$g \;=\; \min \left\{\; c \in \langle a, b \rangle \;\middle|\; c > 0 \;\right\}$$

¿quién es g con respecto a y b?

Como $\langle g \rangle = \langle a, b \rangle$ y $g = sa + tb$ para algún $s, t \in \mathbb{Z}$ tenemos que:

1. $g \mid a$ y $g \mid b$. ¿por qué?
2. Para todo $h \in \mathbb{Z}$, si $h \mid a$ y $h \mid b$, entonces $h \mid g$. ¿por qué?

Por lo tanto, g es el **máximo común divisor** de a y b.

Identidad de Bézout

Teorema

Para todo $a, b \in \mathbb{Z} - \{0\}$:

1. $\gcd(a, b)$ es el **menor número positivo** tal que existe $s, t \in \mathbb{Z}$:

$$\gcd(a, b) = sa + tb$$

2. $\langle a, b \rangle \ = \ \langle \gcd(a, b) \rangle$.

¿cómo podemos encontrar s y t tal que $\gcd(a, b) = sa + tb$?

¿cómo encontrar s, t tal que $\gcd(a,b) = sa + tb$?

Ejemplo

Para encontrar $\gcd(252, 198) = 18$ tenemos que:

$$\begin{array}{rcl} 252 & = & 1 \cdot 198 + 54 \\ 198 & = & 3 \cdot 54 + 36 \\ 54 & = & 1 \cdot 36 + 18 \\ 36 & = & 2 \cdot 18 \end{array} \qquad \begin{array}{rcl} 252 - 1 \cdot 198 & = & 54 \\ 198 - 3 \cdot 54 & = & 36 \\ 54 - 1 \cdot 36 & = & 18 \end{array}$$

$$\begin{array}{rcl} 18 & = & \mathbf{54} - 1 \cdot \mathbf{36} \\ 18 & = & \mathbf{54} - 1 \cdot (\mathbf{198} - 3 \cdot \mathbf{54}) \\ 18 & = & 4 \cdot \mathbf{54} - 1 \cdot \mathbf{198} \\ 18 & = & 4 \cdot (\mathbf{252} - 1 \cdot \mathbf{198}) - 1 \cdot \mathbf{198} \\ 18 & = & 4 \cdot \mathbf{252} - 5 \cdot \mathbf{198} \end{array}$$

Ejercicio: obtenga una regla general para encontrar s y t.

Outline

Ecuaciones de congruencias

Definición

Una **congruencia lineal** es una ecuación de la forma:

$$ax \equiv b \pmod{m}$$

donde $m \in \mathbb{N} - \{0\}$, $a, b \in \mathbb{Z}$ y x es una variable.

Ejemplos

$$3x \equiv 2 \pmod{7} \qquad 4x \equiv 3 \pmod{6}$$

¿cómo podemos resolver estas ecuaciones?

¿cómo resolver $ax \equiv b \pmod{m}$?

Una posibilidad es encontrar el **inverso** $a^{-1} \in \mathbb{Z}_m$ tal que: (ojo: $a^{-1} \neq \frac{1}{a}$)

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

Si a^{-1} existe para a, entonces podemos resolver la ecuación como:

$$\begin{aligned} ax &\equiv b \pmod{m} \\ (a^{-1} \cdot a)x &\equiv a^{-1} \cdot b \pmod{m} \\ x &\equiv a^{-1} \cdot b \pmod{m} \end{aligned}$$

¿cuál es el inverso?

$$3 \cdot x \equiv 1 \pmod{7} \qquad 4 \cdot x \equiv 3 \pmod{6}$$

¿cuándo existe el **inverso multiplicativo** de a en $\mathbb{Z}_m$?

Existencia de inverso multiplicativo

Definición

Decimos que a y b son **primos relativos** si $\gcd(a, b) = 1$.

Teorema

Sea $a \in \mathbb{Z}$ y $m \in \mathbb{N}$ con $m > 1$.
Si a y m son primos relativos, entonces existe un único $a^{-1} \in \mathbb{Z}_m$ tal que:

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

Existencia de inverso multiplicativo

Demostración

Suponga que a y m son primos relativos.

Por la identidad de Bézout, existen s y t en $\mathbb{Z}$ tal que:

$$\begin{aligned} sa + tm &= 1 \\ sa + tm &\equiv 1 \pmod{m} \qquad \text{(usando módulo)} \end{aligned}$$

Como $tm \equiv 0 \pmod{m}$ (¿por qué?) tenemos que:

$$sa \equiv 1 \pmod{m}$$

Por lo tanto, s es un inverso multiplicativo de a módulo m.

Demuestre que $a^{-1} \in \mathbb{Z}_m$ es único.

Existencia de inverso multiplicativo

Teorema

Sea $a \in \mathbb{Z}$ y $m \in \mathbb{N}$ con $m > 1$.
Si a y m son primos relativos, entonces existe un único $a^{-1} \in \mathbb{Z}_m$ tal que:

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

Corolario

1. Si a y m son primos relativos,
   entonces $ax \equiv b \pmod{m}$ tiene solución en $\mathbb{Z}_m$.
2. Si m es primo entonces,
   todo $a \in \mathbb{Z}_m - \{0\}$ tiene un **inverso multiplicativo**.

¿cómo encontramos el inverso multiplicativo de $a \in \mathbb{Z}_m$?