

Máximo común divisor

Clase 29

IIC 1253

Prof. Pedro Bahamondes

Outline

Teorema de Fermat

Máximo común divisor

Inversos modulares

Epílogo

Objetivos de la clase

- Demostrar teorema de Fermat para números primos
- Comprender concepto de MCD
- Comprender el algoritmo extendido de Euclides
- Comprender el concepto de inverso modular

Aritmética modular

Teorema (Fermat)

Si p es un número primo, para cualquier entero a se cumple que $a^p \equiv_p a$.

Aritmética modular

Corolario (Fermat)

Si p es un número primo y a es un entero que no es múltiplo de p , entonces $a^{p-1} \equiv_p 1$.

Ejercicio

Demuestre el corolario.

Aritmética modular

Corolario (Fermat)

Si p es un número primo y a es un entero que no es múltiplo de p , entonces $a^{p-1} \equiv_p 1$.

Por el teorema anterior:

$$a^p \equiv_p a \Rightarrow p \mid a^p - a \Rightarrow a^p - a = k \cdot p \quad (1)$$

Notemos que $a \mid a^p - a$, y por lo tanto $a \mid k \cdot p$. Como p es primo y a no es múltiplo de p , necesariamente $a \mid k$. Dividiendo (1) por a :

$$a^{p-1} - 1 = \frac{k}{a} \cdot p, \text{ con } \frac{k}{a} \in \mathbb{Z}.$$

Por lo tanto:

$$p \mid a^{p-1} - 1 \Rightarrow 1 \equiv_p a^{p-1} \Rightarrow a^{p-1} \equiv_p 1$$

Outline

Teorema de Fermat

Máximo común divisor

Inversos modulares

Epílogo



Máximo común divisor

Definición

Dados dos números a y b , su **máximo común divisor**, denotado como $MCD(a, b)$, es el máximo natural n tal que $n|a$ y $n|b$.

¿Cómo podemos calcularlo?

Máximo común divisor

Teorema

Si $a, b \in \mathbb{Z} \setminus \{0\}$, entonces $MCD(a, b) = MCD(b, a \bmod b)$.

Ejercicio

Demuestre el teorema.

Máximo común divisor

Teorema

Si $a, b \in \mathbb{Z} \setminus \{0\}$, entonces $MCD(a, b) = MCD(b, a \bmod b)$.

Demostraremos que un entero c divide a a y a b si y sólo si divide a b y $a \bmod b$. De esto se concluye el teorema.

Sabemos que $a = k \cdot b + a \bmod b$ (1).

(\Rightarrow) Suponemos que $c \mid a$ y $c \mid b$. Si despejamos $a \bmod b$ desde (1), obtenemos que $a \bmod b = a - k \cdot b$, de donde se concluye que $c \mid a \bmod b$.

(\Leftarrow) Suponemos que $c \mid b$ y $c \mid a \bmod b$. De (1) se concluye que $c \mid a$.

Máximo común divisor

Entonces:

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

A este método recursivo lo llamamos **Algoritmo de Euclides**

Ejercicio

Calcule $MCD(403, 156)$.

Algoritmo de Euclides

Entonces:

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

Ejercicio

Calcule $MCD(403, 156)$.

$$\begin{aligned} MCD(403, 156) &= MCD(156, 403 \bmod 156) = MCD(156, 91) \\ &= MCD(91, 156 \bmod 91) = MCD(91, 65) \\ &= MCD(65, 91 \bmod 65) = MCD(65, 26) \\ &= MCD(26, 65 \bmod 26) = MCD(26, 13) \\ &= MCD(13, 26 \bmod 13) = MCD(13, 0) \\ &= 13 \end{aligned}$$

Extenderemos este algoritmo para obtener más información sobre el MCD

Algoritmo de Euclides extendido

Algoritmo extendido del MCD

Sea $a \geq b$.

1. Definimos una sucesión $\{r_i\}$ como:

$$r_0 = a, r_1 = b, r_{i+1} = r_{i-1} \bmod r_i$$

2. Definimos sucesiones $\{s_i\}$, $\{t_i\}$ tales que:

$$s_0 = 1, t_0 = 0$$

$$s_1 = 0, t_1 = 1$$

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

3. Calculamos estas sucesiones hasta un k tal que $r_k = 0$.
4. Entonces, $MCD(a, b) = r_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot b$.

¿Cómo deducimos s_i y t_i en el paso 2.?

Algoritmo de Euclides extendido

Ejercicio (Propuesto ★)

Demuestre que

$$s_{i+1} = s_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot s_i$$

$$t_{i+1} = t_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot t_i$$

Algoritmo de Euclides extendido

En la sucesión definimos que $r_{i+1} = r_{i-1} \bmod r_i$. Escribimos r_{i-1} como división de r_i :

$$r_{i-1} = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i + r_{i+1} \bmod r_i \quad (1)$$

$$r_{i-1} = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i + r_{i+1} \quad (2)$$

En la sucesión también definimos que $r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$ (3).

Reemplazamos (3) en la parte izquierda de (2) y despejamos r_{i+1} :

$$\begin{aligned} s_{i-1} \cdot a + t_{i-1} \cdot b &= \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i + r_{i+1} \\ r_{i+1} &= s_{i-1} \cdot a + t_{i-1} \cdot b - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i \end{aligned}$$

Algoritmo de Euclides extendido

$$r_{i+1} = s_{i-1} \cdot a + t_{i-1} \cdot b - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i$$

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

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

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

Y como $r_{i+1} = s_{i+1} \cdot a + t_{i+1} \cdot b$:

$$s_{i+1} = s_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot s_i \qquad t_{i+1} = t_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot t_i$$

Algoritmo de Euclides extendido

Algoritmo extendido del MCD

Sea $a \geq b$.

1. Definimos una sucesión $\{r_i\}$ como:

$$r_0 = a, r_1 = b, r_{i+1} = r_{i-1} \bmod r_i$$

2. Definimos sucesiones $\{s_i\}$, $\{t_i\}$ tales que:

$$s_0 = 1, \quad t_0 = 0$$

$$s_1 = 0, \quad t_1 = 1$$

$$s_{i+1} = s_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot s_i, \quad t_{i+1} = t_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot t_i$$

3. Calculamos estas sucesiones hasta un k tal que $r_k = 0$.
4. Entonces, $MCD(a, b) = r_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot b$.

Tenemos todo para calcular el MCD y los pesos que lo expresan como combinación lineal de a y b

Algoritmo de Euclides extendido

Ejercicio

Dados $a = 8$ y $b = 5$, use el algoritmo para calcular $MCD(a, b)$ y $s, t \in \mathbb{Z}$ tales que $MCD(a, b) = s \cdot a + t \cdot b$.

Algoritmo de Euclides extendido

Usamos el algoritmo extendido sobre $a = 8$ y $b = 5$

i	r_i	s_i	t_i	combinación
0	8	1	0	$8 = 1 \cdot 8 + 0 \cdot 5$
1	5	0	1	$5 = 0 \cdot 8 + 1 \cdot 5$
2	$8 \bmod 5$ 3	$1 - \lfloor 8/5 \rfloor \cdot 0$ 1	$0 - \lfloor 8/5 \rfloor \cdot 1$ -1	$3 = 1 \cdot 8 - (-1) \cdot 5$
3	$5 \bmod 3$ 2	$0 - \lfloor 5/3 \rfloor \cdot 1$ -1	$1 - \lfloor 5/3 \rfloor \cdot (-1)$ 2	$2 = (-1) \cdot 8 + 2 \cdot 5$
4	$3 \bmod 2$ 1	$1 - \lfloor 3/2 \rfloor \cdot (-1)$ 2	$-1 - \lfloor 3/2 \rfloor \cdot 2$ -3	$1 = 2 \cdot 8 + (-3) \cdot 5$
5	$2 \bmod 1$ 0	— —	— —	

Concluimos que $MCD(8, 5) = 1 = 2 \cdot 8 + (-3) \cdot 5$, con $s = 2$ y $t = -3$.

Identidad de Bézout

El desarrollo algorítmico anterior muestra el siguiente resultado en acción

Identidad de Bézout

Para todo $a, b \in \mathbb{N} \setminus \{0\}$, existen $s, t \in \mathbb{Z}$ tales que

$$\text{MCD}(a, b) = sa + tb$$

Este es un resultado elemental en teoría de números

Outline

Teorema de Fermat

Máximo común divisor

Inversos modulares

Epílogo

Inversos modulares

Definición

b es **inverso** de a en módulo n si $a \cdot b \equiv_n 1$.

Podemos denotarlo como a^{-1} . Ojo: no es lo mismo que $\frac{1}{a}$.

Ejemplo

¿Cuál es el inverso de 5 en módulo 3?

¿Existe siempre inverso para todo a y módulo n ?

Inversos modulares

Teorema

a tiene inverso en módulo n si y sólo si $MCD(a, n) = 1$.

Ejercicio

Demuestre el teorema.

Si $MCD(a, n) = 1$, decimos que a y n son **primos relativos** o **coprimos**

Inversos modulares

Teorema

a tiene inverso en módulo n si y sólo si $MCD(a, n) = 1$.

(\Rightarrow) Supongamos que a tiene inverso en módulo n , digamos b . Por demostrar: $MCD(a, n) = 1$.

Como b es el inverso de a en módulo n , se cumple que $a \cdot b \equiv_n 1$, y por lo tanto $(a \cdot b) \bmod n = 1$. Entonces, tenemos que $a \cdot b = k \cdot n + 1$, y despejando 1 obtenemos que $1 = a \cdot b - k \cdot n$. Luego, necesariamente cualquier entero c tal que $c \mid a$ y $c \mid n$ debe cumplir que $c \mid 1$, por lo que la única posibilidad es que c sea 1, y por lo tanto necesariamente $MCD(a, n) = 1$.

Inversos modulares

Teorema

a tiene inverso en módulo n si y sólo si $MCD(a, n) = 1$.

(\Leftarrow) Supongamos que $MCD(a, n) = 1$. Por demostrar: a tiene inverso en módulo n .

Si ejecutamos el algoritmo extendido del MCD obtenemos s, t tales que

$$1 = s \cdot a + t \cdot n$$

$$\Leftrightarrow a \cdot s = (-t) \cdot n + 1$$

$$\Leftrightarrow a \cdot s \bmod n = 1$$

$$\Leftrightarrow a \cdot s \equiv_n 1$$

Y entonces a tiene inverso en módulo n , específicamente s . □

¡Podemos calcular el inverso con el algoritmo extendido!
En tal caso, el coeficiente s que acompaña a a es su inverso

Outline

Teorema de Fermat

Máximo común divisor

Inversos modulares

Epílogo

Objetivos de la clase

- Demostrar teorema de Fermat para números primos
- Comprender concepto de MCD
- Comprender el algoritmo extendido de Euclides
- Comprender el concepto de inverso modular