Introdução à Aritmética Modular

George Darmiton da Cunha Cavalcanti

CIn - UFPE

Teorema

Se ***a*** e ***b*** são inteiros positivos, então existem inteiros ***s*** e ***t*** de forma que $\boldsymbol{mdc(a,b)=sa+tb}$.

Exemplo

$\text{mdc}(6,14) = 2$

$2 = (-2)\times 6 + 1\times 14$

$s = -2 \quad \text{e} \quad t = 1$

Exemplo

Expresse o ***mdc(300,18)=6*** como uma combinação linear de ***300*** e ***18***.

Foi visto que mdc(300,18) = mdc(12,18) = mdc(12,6) = mdc(6,0) = 6

1. $300 = 18.16 + 12 \rightarrow$ **12 = 300 -18.16**
2. $18 = 12.1 + 6 \rightarrow$ **6 = 18-12**
3. $12 = 6.2 + 0$

Logo, $6 = 18 - (300 - 18.16)$

$$6 = 18 - 300 + 18.16$$

$$\mathbf{6 = 17.18 - 300}$$

Exemplo

Expresse o ***mdc(252,198)=18*** como uma combinação linear de ***252*** e ***198***.

O algoritmo de Euclides usa as seguintes divisões

$$252 = 1\times 198 + 54$$

$$198 = 3\times 54 + 36$$

$$54 = 1\times 36 + 18$$

$$36 = 2\times 18$$

$$36 = 198 - 3\times 54$$

$$18 = 54 - 1\times 36$$

$$18 = 54 - 1\times 36 =$$

$$54 - 1\times(198 - 3\times 54) =$$

$$4\times 54 - 1\times 198$$

$$54 = 252 - 1\times 198$$

$$18 = 4\times(252 - 1\times 198) - 1\times 198 =$$

$$\boxed{18 = 4\times 252 - 5\times 198}$$

Lema

Se a, b e c são inteiros positivos de forma que $mdc(a,b)=1$ e $a|bc$, então $a|c$.

Prova

1. a e b são primos entre si $\rightarrow$ $mdc(a,b) = 1$
2. $sa+tb = 1$
3. $sac + tbc = c$ (multiplicando por c)
4. se $a|bc \rightarrow a|tbc$
5. Como $a|sac$ e $a|tbc$ então $a|(sac+tbc)$, logo $a|c$

Teorema

Seja m um inteiro positivo e sejam a, b e c inteiros.
Se $ac \equiv bc \pmod{m}$ e $mdc(c,m)=1$,
então $a \equiv b \pmod{m}$

Prova

1. $ac \equiv bc \pmod{m}$
2. $m|(ac-bc)$
3. $m|c(a-b)$
4. Como $mdc(m,c)=1$, pelo lema anterior $m|(a-b)$, logo $a \equiv b \pmod{m}$

Resolvendo Congruência Linear

- Na aritmética usual temos $ax = b$, com $a \neq 0$, então $x = b/a$.
- Ou seja, multiplicando ambos os lados da equação pelo inverso de a, que é $1/a$, temos como calcular x.
- De forma semelhante, na aritmética modular quando queremos a solução de $ax \equiv b \pmod{m}$, sabendo que m é um inteiro positivo, e a e b são inteiros, precisamos calcular o inverso de a módulo m.
- Seja $\bar{a}$ um inteiro de forma que $\bar{a}a \equiv 1 \pmod{m}$. Dizemos que $\bar{a}$ é um inverso de a módulo m.

Teorema

Se a e m são inteiros primos entre si e $m > 1$, então um inverso de a módulo m existe.

Prova

1. como $mdc(a,m)=1 \rightarrow sa+tm = 1$
2. $sa + tm \equiv 1 \ (mod\ m)$
3. sabendo que $tm \equiv 0 \ (mod\ m)$
4. segue-se que $sa \equiv 1 \ (mod\ m)$
5. s é o inverso de a módulo m

Exemplo

Calcular o inverso de 3 módulo 7 usando o algoritmo de Euclides.

Sabendo que $mdc(3,7)=1$ o inverso $\bar{a}$ existe.

$\bar{a} \times 3 \equiv 1 \ (mod\ 7)$

(pelo algoritmo de Euclides) $7=2\times 3+1 \rightarrow -2\times 3+1\times 7=1$

Isso mostra que -2 é um inverso de 3 ***módulo 7***

Logo, todo inteiro congruente com -2 ***módulo 7*** é também inverso de ***3***, assim $\bar{a}$ pode ser ***-2, 5, 12,*** etc

Exemplo

Encontre um inverso de 4 módulo 9.

Ou seja, $4x \equiv 1 \pmod 9$

$9 = 2 \times 4 + 1 \quad \rightarrow \quad 1 = -2 \times 4 + 1 \times 9$

Resposta: ***-2, 7***

Passos para solucionar $ax \equiv b \pmod{m}$

Assim, para solucionar $ax \equiv b \pmod{m}$ os seguintes passos devem ser seguidos:

1. Encontrar $\bar{a}$
2. Como, $a\bar{a} \equiv 1 \pmod{m}$, multiplica-se ambos os lados da congruência por $\bar{a}$
3. $\bar{a}ax \equiv b\bar{a} \pmod{m}$
4. Então $x \equiv b\bar{a} \pmod{m}$

Exemplo

Foi visto que o inverso de $\boldsymbol{3x \equiv 2 \ (mod\ 7)}$, $\bar{a}$ é igual a $\mathbf{5}$.

Assim, pelo algoritmo anterior:

$$x \equiv 10 \ (mod\ 7)$$

$$x \equiv 3 \ (mod\ 7)$$

Exemplo

$3x \equiv 4 \pmod 7$?

Foi visto que ***5*** é um inverso de ***3 módulo 7***

Assim,

$$x \equiv 20 \pmod 7$$

$$x \equiv 6 \pmod 7$$

Exemplo

Encontre x para $4x \equiv 5 \ (mod\ 9)$.

1. O inverso de 4 módulo 9 é -2, 7, etc.
2. Logo, $x \equiv 35 \ (mod\ 9)$.
3. Ou $x \equiv 8 \ (mod\ 9)$.

Teorema Chinês do Resto

- No século um, o matemático chinês chamado Sun-Tsu se perguntou:
  - Que número será esse de forma que quando dividido por 3, o resto é 2; quando dividido por 5, o resto é 3; e quando dividido por 7, o resto é 2?
- A pergunta é:
  - Qual é a solução para o seguinte sistema de congruências?

$$x \equiv 2 \ (mod\ 3)$$
$$x \equiv 3 \ (mod\ 5)$$
$$x \equiv 2 \ (mod\ 7)?$$

Teorema Chinês do Resto

Sejam $\boldsymbol{m_1, m_2, ..., m_n}$ inteiros positivos primos entre si. O sistema

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1) \\ x &\equiv a_2 \ (mod\ m_2) \\ &\vdots \\ x &\equiv a_n \ (mod\ m_n) \end{aligned}$$

possui uma única solução módulo $\boldsymbol{m = m_1 m_2 ... m_n}$.

(Ou seja, existe uma solução x com $0 \leq x < m$, e todas as outras soluções são congruentes módulo m com essa solução).

Teorema Chinês do Resto

Como calcular x:

- faça $m = m_1 m_2 \ldots m_n$;
- para $k = 1, 2, \ldots, n$ faça $M_k = m / m_k$;
- chame Y_k o inverso de M_k módulo m_k e calcule Y_k.
  - *Ou seja,* $M_k Y_k \equiv 1 \pmod{m_k}$
- $x \equiv a_1 M_1 Y_1 + a_2 M_2 Y_2 + \ldots + a_n M_n Y_n \pmod{m}$

Exemplo

$x \equiv 2\ (mod\ 3)$

$x \equiv 3\ (mod\ 5)$

$x \equiv 2\ (mod\ 7)$?

1. $m = 3.5.7 = 105$;
2. $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, e $M_3 = m/7 = 15$
3. 2 é um inverso de M_1=35 módulo 3, pois $35 \equiv 2\ (mod\ 3)$;
4. 1 é um inverso de $M_2 = 21$ módulo 5, pois $21 \equiv 1\ (mod\ 5)$;
5. 1 é um inverso de $M_3 = 15$ módulo 7, pois $15 \equiv 1\ (mod\ 7)$;
6. $x \equiv 2.35.2 + 3.21.1 + 2.15.1\ (mod\ 106) \equiv 233 \equiv 23\ (mod\ 105)$.

Exemplo

Que inteiros deixam resto 1 quando divididos por 2 e resto 1 quando divididos por 3?

1. $x \equiv 1\ (mod\ 2)$ *e* $x \equiv 1\ (mod\ 3)$;
2. $m = 6$, $M_1 = 3$ *e* $M_2 = 2$;
3. Y_1 *é o inverso de 3 mod 2, como* $3 \equiv 1\ (mod\ 2) \rightarrow Y_1 \equiv 1\ (mod\ 2)$;
4. Y_2 *é o inverso de 2 mod 3, como 2 mod 3 = 2, logo* $Y_2 \equiv 2\ (mod\ 3)$;
5. $x \equiv 1.3.1 + 1.2.2\ (mod\ 6)$
6. $x \equiv 7\ (mod\ 6)$.