

Notas sobre teoria dos números (2)

Fonte: livros do L. Lóvasz e Kenneth Rosen (ref. completa na página)

Centro de Informática
Universidade Federal de Pernambuco

2007.1 / CIn-UFPE

Definição (Maior divisor comum)

Sejam a e b inteiros de forma que apenas um dels pode ser zero. O maior inteiro d de forma que $d \mid a$ e $d \mid b$ é chamado de maior divisor comum de a e b , denotado por $\text{mdc}(a, b)$.

- Uma maneira de encontrar o mdc de dois números é encontrar a fatoração prima desses números. Portanto sejam as fatorações de a e b dadas como a seguir:
 - $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$
 - $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$
- $\text{mdc}(a, b) = p_1^{\min(a_1, b_1)}, p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$

Definição (primos entre si)

Os inteiros a e b são primos entre si se seu mdc é 1.

Definição (primos entre si dois a dois)

Os inteiros a_1, a_2, \dots, a_n são primos entre si dois a dois se $\text{mdc}(a_i, a_j) = 1$ para $1 \leq i < j \leq n$.

Definição (o menor múltiplo comum)

O menor múltiplo comum de dois inteiros positivos a e b é o menor inteiro positivo que é divisível pelos dois, a e b . O menor múltiplo comum é denotado por $\text{mmc}(a, b)$.

- $\text{mmc}(a, b) = p_1^{\max(a_1, b_1)}, p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)}$

Exemplo

Prove que se a e b são inteiros positivos então
 $ab = \text{mdc}(a, b) \cdot \text{mmc}(a, b)$

Definição

Sejam a e b inteiros positivos. Nós denotamos $a \bmod m$ como o resto quando a é dividido por m .

- Temos que $15 \bmod 12 = 3 \bmod 12$, que é igual a 3.
- Usamos uma notação para indicar que dois inteiros possuem o mesmo resto quando divididos por um inteiro positivo m .

Definição

Se a e b são inteiros e m é um inteiro positivo, então a é congruente a b módulo m se m divide $a - b$. Usamos a notação $a \equiv b \pmod{m}$ para indicar que a é congruente a b módulo m . Se a e b não são congruentes módulo m , escrevemos $a \not\equiv b \pmod{m}$. Quando $a \equiv b \pmod{m}$, temos que $a \bmod m = b \bmod m$.

- Dizemos que $a \equiv b \pmod{m}$ se e somente se $a \bmod m = b \bmod m$.

Exemplo $7 \equiv 2 \pmod{5}$

- **Você pode provar que se $a \equiv b \pmod{m}$ então $m \mid (a - b)$.**

Teorema

Seja m um inteiro positivo. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$ e $ac \equiv bd \pmod{m}$.

Algumas aplicações de congruência

- Funções Hashing: $h(k) = k \bmod n$;
- Números pseudorandômicos:
- $x_{n+1} = (ax_n + c) \bmod m$.
- x_0 é chamado de semente, a multiplicador e c incremento, onde todos devem ser menores que m , e c e x_0 devem ser maiores ou iguais a zero; e a maior ou igual a 2.

Exemplo $m = 9$, $a = 7$, $c = 4$ e $x_0 = 3$, temos a sequência:



3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8...

- Criptografia: cifra de deslocamento:
 $f(x) = (x + 3) \bmod 26$.

O Algoritmo de Euclides

- O máximo divisor comum de dois inteiros positivos pode ser encontrado usando-se as suas fatorações primas. Mas esse método é ineficiente para inteiros grandes.
- O algoritmo de Euclides calcula o *mdc* de dois inteiros de modo eficiente, sem encontrar suas fatorações primas.
- Ele é baseado em alguns resultados simples, que podemos provar.

O Algoritmo de Euclides

- 1 Prove que $\text{mdc}(a, b) = \text{mdc}(a, b - a)$.
- 2 Seja r o resto se dividirmos b por a . Então prove que $\text{mdc}(a, b) = \text{mdc}(a, r)$.

O Algoritmo de Euclides

Suponha que nos são dados dois inteiros positivos a e b , e desejamos achar seu máximo divisor comum.

- 1 Se $a > b$ então trocamos a por b e vice-versa.
- 2 Se $a > 0$, dividimos b por a , para obter um resto r .
Substituímos b por r e retornamos ao passo 1.
- 3 Senão (se $a = 0$), retornamos b como o m.d.c. e paramos.

O Algoritmo de Euclides: exemplos

- $mdc(300, 18) = mdc(12, 18) = mdc(12, 6) = mdc(6, 0) = 6$
- E o mdc de 101 e 100?
- $mdc(101, 100) = mdc(1, 100) = mdc(1, 0) = 1$
- $mdc(89, 55)?$
- $mdc(89, 55) = mdc(34, 55) = mdc(34, 21) = mdc(13, 21) = mdc(13, 8) = mdc(5, 8) = mdc(5, 3) = mdc(2, 3) = mdc(2, 1) = mdc(1, 0) = 1$

- Qual o resultado de quinta-feira + sexta-feira?
- Vamos fazer a seguinte associação:

0	1	2	3	4	5	6
Dom	Seg	Ter	Qua	Qui	Sex	Sáb

- Assim, a pergunta pode ser formulada da seguinte maneira:

Qual o resultado de $(4 + 5) \bmod 7$?

Daí a resposta é terça-feira.

De modo semelhante, podemos facilmente calcular:

a) Quinta-feira.Sexta-feira;

Resp. Quinta-feira.Sexta-feira $\rightarrow (4.5) \bmod 7 = 6 = \text{Sábado}$;

b) (Sábado)²;

Resp. $(6)^2 \bmod 7 = 36 \bmod 7 = 1 = \text{Segunda-feira}$;

c) Segunda-feira - Sábado.

Resp. $(1 - 6) \bmod 7 = -5 \bmod 7 = 2 = \text{Terça-feira}$.

Propriedades

1) Comutatividade:

- 1 Seg + Sex = Sex + Seg. $((a + b) \bmod m = (b + a) \bmod m)$;
- 2 Ter.Qui = Qui.Terc;

2) Associatividade:

- 1 (Seg + Ter) + Qui = Seg + (Ter + Qui);
- 2 (Sex.Ter).Qua = Sex.(Ter.Qua).

Propriedades

3) Elemento neutro da adição:

① $\text{Seg} + \text{Dom} = \text{Seg}$; $\text{Ter} + \text{Dom} = \text{Ter}$. O “Dom” é o zero.

4) Elemento neutro da multiplicação:

① $\text{Seg} \cdot \text{Ter} = \text{Ter}$; $\text{Qua} \cdot \text{Seg} = \text{Qua}$. “Seg” funciona como um.

5) Subtração é o inverso da soma:

① $(\text{Seg} + \text{Ter}) - \text{Seg} = \text{Ter}$.

E a divisão ?

- Em alguns casos ela é óbvia. Sab/Ter = Qua. Temos Ter.Qua = Sab.
- Entretanto, Ter/Qua?
- Na aritmética usual isso seria $\frac{2}{3}$, que não é um inteiro. Dessa forma, os racionais foram introduzidos. Mas será que devemos introduzir *dias da semana fracionários*? Veremos que a resposta é não.

Calculando Ter/Qua

- $\frac{Ter}{Qua} = x$
- $x \cdot Qua = Ter$
- A resposta é $x = Qua$, $Qua \cdot Qua = Ter$, pois $3 \cdot 3 \equiv 2 \pmod{7}$.
- Na realidade solucionamos a **congruência linear** $x \cdot 3 \equiv 2 \pmod{7}$.
- Como encontrar uma solução para o caso geral $ax \equiv b \pmod{m}$?
- Além disso, temos que $14 \equiv 8 \pmod{6}$, $\frac{14}{2} = 7$, $\frac{8}{2} = 4$, mas $7 \not\equiv 4 \pmod{6}$. Por quê?
- Precisamos estudar primeiro alguns resultados.

Alguns Resultados

Teorema (pg. 137)

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

- Isso quer dizer que o mdc de a e b pode ser escrito como uma **combinação linear** com coeficientes inteiros de a e b .
- Para encontrar a **combinação linear** de dois inteiros que seja igual ao seu mdc usamos o algoritmo de Euclides.

Alguns Resultados

Exemplo

Expresse o $\text{mdc}(300, 18) = 6$ como uma combinação linear de 300 e 18.

Vimos que $\text{mdc}(300, 18) = \text{mdc}(12, 18) = \text{mdc}(12, 6) = \text{mdc}(6, 0) = 6$:

$$\textcircled{1} \quad 300 = 18 \cdot 16 + 12 \rightarrow \mathbf{12 = 300 - 18 \cdot 16}$$

$$\textcircled{2} \quad 18 = 12 \cdot 1 + 6 \rightarrow \mathbf{6 = 18 - 12}$$

$$\textcircled{3} \quad 12 = 6 \cdot 2 + 0$$

Logo, $6 = 18 - (300 - 18 \cdot 16) \rightarrow 6 = 18 - 300 + 18 \cdot 16 \rightarrow \mathbf{6 = 17 \cdot 18 - 300}$.

Outro exemplo

- Expresse o $\text{mdc}(252,198)$ como uma combinação linear de 252 e 198 .
- $\text{mdc}(252,198) = \text{mdc}(198, 54) = \text{mdc}(54, 36) = \text{mdc}(36, 18) = \text{mdc}(18, 0) = 18$.
 - ① $252 = 198 \cdot 1 + 54$
 - ② $198 = 54 \cdot 3 + 36$
 - ③ $54 = 36 \cdot 1 + 18$
 - ④ $36 = 18 \cdot 2 + 0$
- Assim,
 - ① $54 = 252 - 198$
 - ② $36 = 198 - 3 \cdot 54$
 - ③ $18 = 54 - 36$
- Logo, $18 = (252 - 198) - (198 - 3 \cdot 54) = 252 - 2 \cdot 198 + 3 \cdot (252 - 198) = 4 \cdot 252 - 5 \cdot 198$.

Lema (pg. 138)

Se a , b e c são inteiros positivos de forma que a e b são primos entre si e $a \mid bc$ então $a \mid c$.

Prova

- 1 a e b são primos entre si $\rightarrow \text{mdc}(a,b) = 1$;
- 2 $sa + tb = 1$;
- 3 $sac + tbc = c$;
- 4 Se $a \mid bc \rightarrow a \mid tbc$;
- 5 Como $a \mid sac$ e $a \mid tbc$ então $a \mid (sac + tbc)$, logo $a \mid c$

Teorema (pg. 139)

Seja m um inteiro positivo e sejam a, b e c inteiros. Se $ac \equiv bc \pmod{m}$ e c e m são primos entre si então $a \equiv b \pmod{m}$.

Prova

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

- Na aritmética usual se 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 $ax \equiv b \pmod{m}$, onde 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 $\bar{a} \cdot a \equiv 1 \pmod{m}$. Dizemos que \bar{a} é um *inverso de a módulo m* .
- O seguinte teorema garante que o inverso de a módulo m existe se a e m são primos entre si.

Teorema (pg. 140)

Se a e m são inteiros primos entre si e $m > 1$, então o inverso de a módulo m existe. Além disso, esse inverso é único módulo m .

Prova

- 1 como $\text{mdc}(a, m) = 1 \rightarrow sa + tm = 1$;
- 2 $sa + tm \equiv 1 \pmod{m}$;
- 3 $tm \equiv 0 \pmod{m}$;
- 4 $sa \equiv 1 \pmod{m}$.
- 5 s é o inverso de a módulo m .

Exemplos

Exemplo

Para calcular um inverso de 3 mod 7 usamos o algoritmo de Euclides.

$$\bar{a}.3 \equiv 1 \pmod{7}.$$

$$7 = 2.3 + 1 \rightarrow 1 = 7 - 2.3.$$

Logo \bar{a} é -2, 5, 12, etc.

- Encontre um inverso de 4 módulo 9.
- Ou seja, $4.x \equiv 1 \pmod{9}$
- $9 = 2.4 + 1 \rightarrow 1 = 9 - 2.4$
- Resposta: -2, 7, etc.

- Assim, para solucionar $ax \equiv b \pmod{m}$ fazemos os seguintes passos:
 - 1 encontramos \bar{a}
 - 2 como $\bar{a}.a \equiv 1 \pmod{m}$, multiplicamos ambos os lados da congruência por \bar{a} :
 - 3 $\bar{a}.a.x \equiv b.\bar{a} \pmod{m}$;
 - 4 então temos $x \equiv b.\bar{a} \pmod{m}$

Exemplos

Exemplo

Retomando o nosso exemplo: $x \cdot 3 \equiv 2 \pmod{7}$:

*Vimos que um inverso de $3 \pmod{7}$ é 5 . Daí $x \equiv 10 \pmod{7} \rightarrow$
 $x \equiv 3 \pmod{7}$.*

- $3x \equiv 4 \pmod{7}$?
- Vimos que 5 é um inverso de $3 \pmod{7}$.
- Assim, $x \equiv 20 \pmod{7}$, logo $x \equiv 6 \pmod{7}$.

Exemplos

Exemplo

Encontre x para $4x \equiv 5 \pmod{9}$.

- 1 O inverso de $4 \pmod{9}$ é $-2, 7$, etc.
- 2 Logo $x \equiv 35 \pmod{9}$ ou $x \equiv 8 \pmod{9}$.