Teoria dos números III
MDC e Congruências

André Gustavo dos Santos[1]

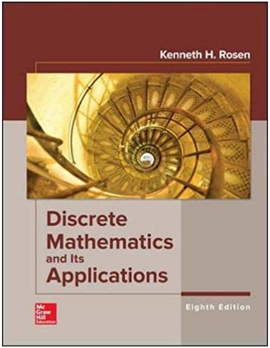
[1] Departamento de Informática
Universidade Federal de Viçosa

INF230 - 2021/1

UFV

Conteúdo

Os slides seguintes são baseados nas seções 4.3.6 a 4.4 do livro texto da disciplina:



ROSEN, Kenneth H.
Discrete mathematics and its applications.
McGraw-Hill Education, 8th edition, 2018

MDC

Definição

Sejam a e b dois inteiros diferentes de zero. O maior inteiro d tal que $d|a$ e $d|b$ é chamado **máximo divisor comum** de a e b e é denotado por $\text{mdc}(a, b)$.

- Note que se a e b são diferentes de zero, $\text{mdc}(a, b)$ existe, pois o conjunto de divisores comuns deles é finito
- Uma forma de encontrar o mdc é listar os divisores positivos comuns e selecionar o maior deles

Qual o máximo divisor comum entre 24 e 36?

- Divisores de 24: 1, 2, 3, 4, 6, 8, 12 e 24
- Divisores de 36: 1, 2, 3, 4, 6, 9, 12, 18, 36
- Máximo divisor comum: 12

Qual o máximo divisor comum entre 17 e 22?

- Divisores de 17: 1, 17
- Divisores de 22: 1, 2, 11,22
- Máximo divisor comum: 1

Primos entre si

- Frequentemente é importante salientar que dois números não têm divisor positivo comum além do 1.

Definição

Dois numeros inteiros são primos entre si se o mdc deles for 1.

17 e 22 são primos entre si?

- Sim, no exemplo anterior descobrimos que mdc(17,22)=1

- Também é importante salientar que cada par de dois números de um conjunto não tem divisor positivo comum além do 1.

Definição

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

Exemplos

- 10, 17 e 21 são primos entre si dois a dois?
  Sim, pois mdc(10,17) = 1, mdc(10,21) = 1 e mdc(17,21) = 1
- 10, 19 e 24 são primos entre si dois a dois?
  Não, pois mdc(10,24)$= 2 \neq 1$

MDC por fatoração

- Outra forma de encontrar o MDC entre dois números é usar a fatoração em primos desses números
- Suponha que as fatorações de a e b sejam dadas por:
  - $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$
  - $b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$
  - em que todos os expoentes são não negativos
  - e todos os primos das fatorações de a e b estão em ambas (expoente 0, se necessário)
- Então:
  - $\text{mdc}(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$

Qual o valor de mdc(120,500)?

- $120 = 2^3 \cdot 3 \cdot 5 = 2^3 \cdot 3^1 \cdot 5^1$
- $500 = 2^2 \cdot 5^3 \quad = 2^2 \cdot 3^0 \cdot 5^3$
- $\text{mdc}(120,500) \quad = 2^2 \cdot 3^0 \cdot 5^1 = 20$

MMC por fatoração

Definição

O mínimo múltiplo comum entre dois inteiros positivos a e b, denotado por $\text{mmc}(a, b)$ é o menor inteiro d que é divisível por ambos, ou seja, que $a|d$ e $b|d$.

- $\text{mmc}(a, b)$ existe porque o conjunto de valores divisíveis por a e b não é vazio (ab está neste conjunto)
- Uma forma de encontrar o MMC é encontrar a fatoração, como no MDC, e então:
  - $\text{mmc}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \ldots p_n^{\max(a_n, b_n)}$

Qual o valor de mmc(120,500)?

- $120 = 2^3 \cdot 3 \cdot 5 = 2^3 \cdot 3^1 \cdot 5^1$
- $500 = 2^2 \cdot 5^3 \quad = 2^2 \cdot 3^0 \cdot 5^3$
- $\text{mmc}(120{,}500) \quad = 2^3 \cdot 3^1 \cdot 5^3 = 3000$

Teorema

- $ab = \text{mdc}(a, b) \cdot \text{mmc}(a, b)$

Algoritmo de Euclides

- Encontrar mdc por fatoração é ineficiente, pois fatorar é custoso computacionalmente
- O algoritmo de Euclides[1], conhecido desde tempos remotos, é bem mais eficiente

Qual o valor de $\text{mdc}(287, 91)$?

- Pelo algoritmo da divisão, $287 = 91 \cdot 3 + 14$
- Qualquer divisor de 287 e 91 é divisor de $287 - 91 \cdot 3 = 14$
- E qualquer divisor de 91 e 14 é divisor de $91 \cdot 3 + 14 = 287$
- Então $\text{mdc}(287, 91)$ é o mesmo que $\text{mdc}(91, 14)$
- O problema de achar $\text{mdc}(287, 91)$ foi reduzido ao de achar $\text{mdc}(91, 14)$
- Pelo algoritmo da divisão, $91 = 14 \cdot 6 + 7$
- Usando o mesmo raciocínio anterior, $\text{mdc}(91, 14)$ é o mesmo que $\text{mdc}(14, 7)$
- Pelo algoritmo da divisão, $14 = 7 \cdot 2$
- Como $7|14$, $\text{mdc}(14, 7) = 7$; assim, $\text{mdc}(287, 91) = \text{mdc}(91, 14) = \text{mdc}(14, 7) = 7$

[1] O nome é homenagem ao matemático grego Euclides, que o incluiu em seu livro “Os elementos”, 300 a.C

Algoritmo de Euclides

- O algoritmo de Euclides é baseado no seguinte lema

Lema

Seja $a = bq + r$, em que a, b, q, r são números inteiros. Então $\text{mdc}(a, b) = \text{mdc}(b, r)$

- Considere $r_0 = a$ e $r_1 = b$. Então

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

- Note que um resto zero eventualmente aparece, pois a sequência de restos não pode ter mais que a termos: $a = r_0 > r_1 > r_2 > \cdots \ge 0$.
- Pela lema anterior,
  $\text{mdc}(a, b) = \text{mdc}(r_0, r_1) = \text{mdc}(r_1, r_2) = \cdots = \text{mdc}(r_{n-1}, r_n) = \text{mdc}(r_n, 0) = r_n$
- Portanto, o mdc é o último resto que aparece na sequência de divisões

Algoritmo de Euclides

Exemplos

- $$\begin{aligned}\mathrm{mdc}(120,500) &= \mathrm{mdc}(500, 120 \bmod 500) = \mathrm{mdc}(500,120)\\ &= \mathrm{mdc}(120, 500 \bmod 120) = \mathrm{mdc}(120,20)\\ &= \mathrm{mdc}(20, 120 \bmod 20) = \mathrm{mdc}(20,0) = 20.\end{aligned}$$
- $$\begin{aligned}\mathrm{mdc}(662,414) &= \mathrm{mdc}(414, 662 \bmod 414) = \mathrm{mdc}(414,248)\\ &= \mathrm{mdc}(248, 414 \bmod 248) = \mathrm{mdc}(248,166)\\ &= \mathrm{mdc}(166, 248 \bmod 166) = \mathrm{mdc}(166,82)\\ &= \mathrm{mdc}(82, 166 \bmod 82) = \mathrm{mdc}(82,2)\\ &= \mathrm{mdc}(2, 82 \bmod 2) = \mathrm{mdc}(2,0) = 2.\end{aligned}$$

Resumindo, em forma de tabela:

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	662	414	1	248
1	414	248	1	166
2	248	166	2	82
3	166	82	2	2
4	82	2	41	0

Combinação linear

- Um importante resultado é que $\text{mdc}(a, b)$ pode ser expresso como uma combinação linear de a e b

Teorema de Bézout

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

Exemplo

- $\text{mdc}(6, 14) = 2$
- $2 = (-2) \cdot 6 + 1 \cdot 14$

- Os inteiros s e t são chamados coeficientes de Bézout. Como encontrá-los?

Algoritmo de Euclides estendido

- É possível encontrar os coeficientes de Bézout analisando os resultados do algoritmo de Euclides no sentido inverso

Expresse o $\text{mdc}(252, 198) = 18$ como uma combinação linear de 252 e 198

Pelo algoritmo de Euclides

- $252 = 198 \cdot 1 + 54$
- $198 = 54 \cdot 3 + 36$
- $54 = 36 \cdot 1 + 18$
- $36 = 18 \cdot 2.$
- $\text{mdc}(252, 198) = 18$

Encontrando os coeficientes de Bézout:

- Na penúltima linha, $18 = 54 - 36 \cdot 1$
- Na linha anterior, $36 = 198 - 54 \cdot 3$
- Substituindo, $18 = 54 - (198 - 54 \cdot 3) \cdot 1 = 198 \cdot (-1) + 54 \cdot 4$
- Na primeira linha, $54 = 252 - 198 \cdot 1$
- Substituindo, $18 = 198 \cdot (-1) + (252 - 198 \cdot 1) \cdot 4 = 252 \cdot 4 + 198 \cdot (-5)$.

Algoritmo de Euclides estendido

- O algoritmo de Euclides estendido calcula os coeficientes enquanto calcula o mdc
- Inicie com os coeficientes $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$
- Em cada iteração, $s_j = s_{j-2} - q_{j-1}s_{j-1}$ e $t_j = t_{j-2} - q_{j-1}t_{j-1}$
  sendo q os quocientes em cada passo do algoritmo de Euclides

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0	-3	4
4					4	-5

Congruência - divisão

- Já vimos que se $a \equiv b (\text{mod } m)$ e $c \equiv d (\text{mod } m)$, então $ac \equiv bd (\text{mod } m)$
- Então podemos multiplicar os dois lados de uma congruência por um mesmo inteiro
- Mas será que dividir os dois lados por um inteiro produz uma congruência válida?

Contra-exemplo

- $14 \equiv 8 \pmod 6$
- Mas não vale dividir por 2, pois $7 \not\equiv 4 \pmod 6$

Teorema

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

- Podemos dividir por c se $\text{mdc}(c, m) = 1$, ou seja, se c e m são primos entre si.
- No exemplo acima, não podíamos dividir por 2, pois 2 e 6 não são primos entre si.

Congruência linear

- Congruência linear é uma equação da forma

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

em que m é um inteiro positivo, a e b são inteiros e x é uma variável.

- Como resolver esta equação? Como achar os valores de x que a satisfazem?
- Uma forma é achar um inteiro $\bar{a}$ tal que $a\bar{a} \equiv 1 \pmod{m}$, se existir
- Daí podemos multiplicar os dois lados por $\bar{a}$ e teremos $x \equiv \bar{a}b \pmod{m}$

- $\bar{a}$ é chamado inverso de a módulo m, e existe se a e m são primos entre si

UFV

Congruência linear

Teorema

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

Ou seja, há um único inteiro positivo $\bar{a}$ menor que m que é inverso de a módulo m, e todo outro inverso de a módulo m é congruente a $\bar{a}$ módulo m.)

Prova

- Como $\text{mdc}(a, m) = 1$, pelo Teorema de Bézout existem s e t tal que $sa + tm = 1$
- Então $sa + tm \equiv 1 \bmod m$
- Como $tm \equiv 0 \bmod m$, então $sa \equiv 1 \bmod m$
- Consequentemente, s é inverso de a módulo m.

UFV

Congruência linear

Encontre um inverso de 3 módulo 7

- Como $\text{mdc}(3, 7) = 1$, existe inverso de 3 módulo 7
- O algoritmo de Euclides termina rapidamente
- De $7 = 3 \cdot 2 + 1$ podemos ver que $(-2) \cdot 3 + 1 \cdot 7 = 1$
- Então -2 é um inverso de 3 módulo 7
- E qualquer valor congruente a -2 módulo 7, como 5, 12, etc.
- Note que $5 \cdot 3 = 15 \equiv 1 (\text{mod } 7)$, portanto 5 é um inverso de 3 módulo 7

Quais as soluções da congruência linear $3x \equiv 4 \pmod 7$?

- Vamos multiplicar os dois lados por 5, mas qualquer inverso de 3 serve
- $3x \equiv 4 \pmod 7$
  $5 \cdot 3x \equiv 5 \cdot 4 \pmod 7$
  $15 \cdot x \equiv 20 \pmod 7$
  $x \equiv 6 \pmod 7$
- 6 e qualquer valor congruente a 6 módulo 7 é solução

Sistemas de congruências lineares

- Sistemas de congruências lineares aparecem em vários contextos
- Por exemplo, são a base para um método de multiplicação de números inteiros grandes
- Também aparecem em enigmas nos escritos de antigos matemáticos chineses e hindus

Enigma de Sun-Tzu

No primeiro século, o matemático chinês Sun-Tzu perguntou:

- Há certas coisas cuja quantidade é desconhecida.
- Se contarmos de três em três, sobram 2.
- Se contarmos de cinco em cinco, sobram 3.
- Se contarmos de sete em sete cobram 2.
- Qual a quantidade dessas coisas?

- Pode ser transcrito como a pergunta: qual a solução do sistema de congruências

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}\ ?$$

Teorema chinês do resto

Teorema chinês do resto

Sejam $m1, m_2, \ldots, m_n$ um conjunto de inteiros primos entre si dois a dois e $a_1, a_2, \ldots, a_n$ inteiros quaisquer. Então, o sistema

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$\vdots$
$x \equiv a_n \pmod{m_n}$

tem solução única módulo $m = m_1 m_2 \ldots m_n$.
(isto é, existe uma solução x com $0 \leq x < m$ e todas as outras são congruentes a ela módulo m.)

Prova (por construção)

- Seja $M_k = m/m_k$ para $k = 1, 2, \ldots, m$, isto é, o produto de todos os módulos exceto m_k
- Temos que $\text{mdc}(m_k, M_k) = 1$, já que m_k e m_i são primos entre si para todo $i \neq k$
- Pelo teorema anterior, existe y_k, o inverso de M_k módulo m_k, tal que $y_k M_k \equiv 1 \pmod{m_k}$
- Uma solução simultânea para todas as congruências é $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots a_n M_n y_n$
- Note que, como $M_j \equiv 0 \pmod{m_k}$ para $j \neq k$, todos os termos da soma exceto o k-ésimo são congruentes a 0 módulo m_k. Como $M_k y_k \equiv 1 \pmod{m_k}$, $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$.

Teorema chinês do resto

Solução do enigma de Sun-Tzu

- Qual a solução do sistema de congruências

  $x \equiv 2 \pmod 3$
  $x \equiv 3 \pmod 5$
  $x \equiv 2 \pmod 7$?

- $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, $M_3 = m/7 = 15$
- O inverso de M_1 módulo 3 é 2, pois $2 \cdot 35 \equiv 2 \cdot 2 \equiv 1 \pmod 3$
- O inverso de M_2 módulo 5 é 1, pois $1 \cdot 21 \equiv 1 \cdot 1 \equiv 1 \pmod 5$
- O inverso de M_3 módulo 7 é 1, pois $1 \cdot 15 \equiv 1 \cdot 1 \equiv 1 \pmod 3$
- A solução é então
  $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$