M342 Álgebra Computacional

Christian Lomp

FCUP

21 de setembro de 2011

2.2 Os numeros reais

o algoritmo de Euclid

1. O algoritmo de Euclid para inteiros permite determinar o **máximo divisor comum** de dois inteiros.

2.2 Os numeros reais

o algoritmo de Euclid

1. O algoritmo de Euclid para inteiros permite determinar o **máximo divisor comum** de dois inteiros.
2. O algoritmo de Euclid permite reduzier quocientes de inteiros $\frac{a}{b} = \frac{a'}{b'}$ onde $\mathrm{mdc}(a', b') = 1$.

2.2 Os numeros reais

o algoritmo de Euclid

1. O algoritmo de Euclid para inteiros permite determinar o **máximo divisor comum** de dois inteiros.
2. O algoritmo de Euclid permite reduzier quocientes de inteiros $\frac{a}{b} = \frac{a'}{b'}$ onde $\mathrm{mdc}(a', b') = 1$.
3. O algotitmo aplica-se também para polinómios.

Definição

Um domínio integral R com uma função $d : R \to \mathbb{N} \cup \{-\infty\}$ chama-se um **Domínio Euclideano** se

$$\forall a, b \in R \text{ com } b \neq 0 : \qquad \exists q, r \in R \; a = qb + r \; \text{ com } d(r) < d(b).$$

Definição

Um domínio integral R com uma função $d : R \to \mathbb{N} \cup \{-\infty\}$ chama-se um **Domínio Euclideano** se

$$\forall a, b \in R \text{ com } b \neq 0 : \qquad \exists q, r \in R \; a = qb + r \; \text{ com } d(r) < d(b).$$

O elemento q, denotado por $q = a/b$ ou $q = a \operatorname{quo} b$, diz-se o **quociente** e r, denotado por $r = a\%b$ ou $q = a \operatorname{rem} b$ diz-se o **resto**.

Definição

Um domínio integral R com uma função $d : R \to \mathbb{N} \cup \{-\infty\}$ chama-se um **Domínio Euclideano** se

$$\forall a, b \in R \text{ com } b \neq 0 : \qquad \exists q, r \in R \; a = qb + r \;\text{ com } d(r) < d(b).$$

O elemento q, denotado por $q = a/b$ ou $q = a \operatorname{quo} b$, diz-se o **quociente** e r, denotado por $r = a\%b$ ou $q = a \operatorname{rem} b$ diz-se o **resto**. Em geral a/b e $a\%b$ não são necessáriamente únicos.

Exemplos

1. $R = \mathbb{Z}$ e $d : \mathbb{Z} \to \mathbb{N}$ é dado por $d(a) = |a|$, $\forall a \in \mathbb{Z}$.

Exemplos

1. $R = \mathbb{Z}$ e $d : \mathbb{Z} \to \mathbb{N}$ é dado por $d(a) = |a|$, $\forall a \in \mathbb{Z}$.
2. $R = F[x]$, F um corpo e $d : F[x] \to \mathbb{N} \cup \{-\infty\}$ dado por $d(f) = \mathrm{grau}(f)$ se $f \neq 0$ e $\mathrm{grau}(0) = -\infty$.

Exemplos

1. $R = \mathbb{Z}$ e $d : \mathbb{Z} \to \mathbb{N}$ é dado por $d(a) = |a|$, $\forall a \in \mathbb{Z}$.
2. $R = F[x]$, F um corpo e $d : F[x] \to \mathbb{N} \cup \{-\infty\}$ dado por $d(f) = \mathrm{grau}(f)$ se $f \neq 0$ e $\mathrm{grau}(0) = -\infty$.
3. $R = \mathbb{Z}[i] = \{a + \imath b \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$, os inteiros de Gauss, e $d(a + \imath b) = a^2 + b^2$.

Exemplos

1. $R = \mathbb{Z}$ e $d : \mathbb{Z} \to \mathbb{N}$ é dado por $d(a) = |a|$, $\forall a \in \mathbb{Z}$.
2. $R = F[x]$, F um corpo e $d : F[x] \to \mathbb{N} \cup \{-\infty\}$ dado por $d(f) = \mathrm{grau}(f)$ se $f \neq 0$ e $\mathrm{grau}(0) = -\infty$.
3. $R = \mathbb{Z}[i] = \{a + \imath b \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$, os inteiros de Gauss, e $d(a + \imath b) = a^2 + b^2$.
4. $R = F$ um corpo e $d(a) = 1$ se $a \neq 0$ e $d(a) = 0$ se $a = 0$.

Se $d(b) = -\infty$ então $b = 0$, pois se $d(b) = -\infty$ e $b \neq 0$, então existem $q, r \in R$ tais que

$$b = qb + r \qquad \text{com } d(r) < d(b) = -\infty$$

o que é impossível, pois $d(r) \geq -\infty$ para qualquer $r \in R$.

Definição

Sejam a e b elementos num domínio de integridade R. Digamos que a **divide** b, denotado por $a|b$ se e só se

$$\exists c \in R : \qquad b = ac.$$

Definição

Sejam a e b elementos num domínio de integridade R. Digamos que a **divide** b, denotado por $a|b$ se e só se

$$\exists c \in R : \qquad b = ac.$$

Exercício: Sejam a, b elementos de um domínio de integridade R.

1. $a|0$ se e só se $a = 0$;

Definição

Sejam a e b elementos num domínio de integridade R. Digamos que a **divide** b, denotado por $a|b$ se e só se

$$\exists c \in R: \qquad b = ac.$$

Exercício: Sejam a, b elementos de um domínio de integridade R.

1. $a|0$ se e só se $a = 0$;
2. $a|1$ se e só se a é invertível;

Definição

Sejam a e b elementos num domínio de integridade R. Digamos que a **divide** b, denotado por $a|b$ se e só se

$$\exists c \in R : \qquad b = ac.$$

Exercício: Sejam a, b elementos de um domínio de integridade R.

1. $a|0$ se e só se $a = 0$;
2. $a|1$ se e só se a é invertível;
3. $a|b$ e $b|a$ se e só se existe um elemento invertível $u \in R$ tais que $a = ub$.

Definição

Sejam a e b elementos num domínio de integridade R. Digamos que a **divide** b, denotado por $a|b$ se e só se

$$\exists c \in R : \qquad b = ac.$$

Exercício: Sejam a, b elementos de um domínio de integridade R.

1. $a|0$ se e só se $a = 0$;
2. $a|1$ se e só se a é invertível;
3. $a|b$ e $b|a$ se e só se existe um elemento invertível $u \in R$ tais que $a = ub$.

Definição

Dois elementos a e b chamam-se **associados** se $a = ub$ para um elemento invertível $u \in R$. Denotamos este facto por $a \sim b$.

Definição

Sejam a, b, c elementos dum domínio de integridade R. O elemento c diz-se **máximo divisor comum** de a e b, denotado por $c = \mathrm{mdc}(a, b)$ se

(i) $c|a$ e $c|b$;

(ii) se $d|a$ e $d|b$ então $d|c$, para todo $d \in R$.

Definição

Sejam a, b, c elementos dum domínio de integridade R. O elemento c diz-se **máximo divisor comum** de a e b, denotado por $c = \mathrm{mdc}(a, b)$ se

(i) $c|a$ e $c|b$;

(ii) se $d|a$ e $d|b$ então $d|c$, para todo $d \in R$.

O elemento c diz-se **mínimo múltiplo comum** de a e b, denotado por $c = \mathrm{mmc}(a, b)$ se

(i) $a|c$ e $b|c$;

(ii) se $a|d$ e $b|d$ então $c|d$, para todo $d \in R$.

Definição

Sejam a, b, c elementos dum domínio de integridade R. O elemento c diz-se **máximo divisor comum** de a e b, denotado por $c = \mathrm{mdc}(a, b)$ se

(i) $c|a$ e $c|b$;

(ii) se $d|a$ e $d|b$ então $d|c$, para todo $d \in R$.

O elemento c diz-se **mínimo múltiplo comum** de a e b, denotado por $c = \mathrm{mmc}(a, b)$ se

(i) $a|c$ e $b|c$;

(ii) se $a|d$ e $b|d$ então $c|d$, para todo $d \in R$.

Em $\mathbb{Z}$ define-se que $\mathrm{mdc}(a, b)$ e $\mathrm{mmc}(a, b)$ sejam também positivos e portanto únicos.

Propriedades de $\mathrm{mdc}(-,-)$ em $\mathbb{Z}$

Sejam $a, b, c \in \mathbb{Z}$:

(i) $\mathrm{mdc}(a, b) = |a| \iff a|b$;

(ii) $\mathrm{mdc}(a, a) = \mathrm{mdc}(a, 0) = |a|$ e $\mathrm{mdc}(a, 1) = 1$.

(iii) $\mathrm{mdc}(a, b) = \mathrm{mdc}(b, a)$ (comutatividade);

(iv) $\mathrm{mdc}(a, \mathrm{mdc}(b, c)) = \mathrm{mdc}(\mathrm{mdc}(a, b), c)$ (associatividade);

(v) $\mathrm{mdc}(ca, cb) = |c|\mathrm{mdc}(a, b)$ (distributividade);

(vi) $|a| = |b| \Rightarrow \mathrm{mdc}(a, c) = \mathrm{mdc}(b, c)$.

(vii) $\mathrm{mdc}(a, b) = \mathrm{mdc}(b, a\%b)$

Algoritmo de Euclid

Input: $a, b \in R$ onde R é um domínio de Euclid.
Output: Um máximo divisor comum c de a e b;

$r_0 \leftarrow a$
$r_1 \leftarrow b$
$i \leftarrow 1$
while $r_i \neq 0$ **do**
  $r_{i+1} \leftarrow (r_{i-1} \% r_i)$
  $i \leftarrow i + 1$
end while
return $r_i - 1$

Algoritmo de Euclid em C++

```
int mdc(int a, int b)
{
  int r0=a;
  int r1=b;
  while (r1!= 0)
  {
    int aux=r1;
    r1=r0%r1;
    r0=aux;
  }
  return r0;
}
```

Algoritmo de Euclid em C++

```
int mdc(int a, int b)
{
  int r0=a;
  int r1=b;
  while (r1!= 0)
  {
    int aux=r1;
    r1=r0%r1;
    r0=aux;
  }
  return r0;
}

int mdc(int a, int b)
{
  if (b==0)
    return a;
  else
    return mdc(b,a%b)    ;
};
```

Algoritmo de Euclid estendido

O máximo divisior comum $\mathrm{mdc}(a, b)$ de dois inteiro é combinação linear de a e b.

Exemplo

$$\begin{aligned} 126 &= 3 \times 35 + 21 \\ 35 &= 1 \times 21 + 14 \\ 21 &= 1 \times 14 + 7 \\ 14 &= 2 \times 7 + 0 \end{aligned}$$

$$7 = 21 - 1 \times 14 = 21 - 1 \times (35 - 1 \times 21) = 2 \times (126 - 3 \times 35) - 1 \times 35 = 2 \times 126 + (-7) \times 35.$$

Logo $\mathrm{mdc}(126, 35) = 7 = 2 \times 126 + (-7) \times 35$.

Algoritmo de Euclid estendido

Input: $a, b \in R$ onde R é um domínio de Euclid.
Output: $l \in \mathbb{N}, r_i, s_i, t_i \in R$ para $0 \leq i \leq l+1$ e $q_i \in R$ para $1 \leq i \leq l$.

$r_0 \leftarrow a,\ s_0 \leftarrow 1,\ t_0 \leftarrow 0$
$r_1 \leftarrow b,\ s_1 \leftarrow 0,\ t_1 \leftarrow 1$
$i \leftarrow 1$
while $r_i \neq 0$ **do**
  $q_i \leftarrow (r_{i-1}/r_i)$
  $r_{i+1} \leftarrow (r_{i-1} \% r_i)$
  $s_{i+1} \leftarrow s_{i-1} - q_i s_i$
  $t_{i+1} \leftarrow t_{i-1} - q_i t_i$
  $i \leftarrow i + 1$
end while
$l \leftarrow i - 1$
return l, r_i, s_i, t_i para $0 \leq i \leq l+1$ e q_i para $1 \leq i \leq l$.

Exemplo

$R = \mathbb{Z}$, $a = 126$ e $b = 35$:

i	q_i	r_i	s_i	t_i
0		126	1	0
1	3	35	0	1
2	1	21	1	-3
3	1	14	-1	4
4	2	7	$\mathbf{2}$	$-\mathbf{7}$
5		0	-5	18

$$7 = 2 \times 126 + (-7) \times 35.$$

Exemplo

$R = \mathbb{Q}[x]$, $a = 18x^3 - 42x^2 + 30x - 6$ e $b = -12x^2 + 10x - 2$:

i	q_i	r_i	s_i	t_i
0		$18x^3 - 42x^2 + 30x - 6$	1	0
1	$-\frac{3}{2}x + \frac{9}{4}$	$-12x^2 + 10x - 2$	0	1
2	$-\frac{8}{3}x + \frac{4}{3}$	$\frac{9}{2}x - \frac{3}{2}$	$\mathbf{1}$	$\mathbf{\frac{3}{2}x - \frac{9}{4}}$
3		0	$\frac{8}{3}x - \frac{4}{3}$	$4x^2 - 8x + 4$

$$\boxed{\frac{9}{2}x - \frac{3}{2} = 18x^3 - 42x^2 + 30x - 6 + \left(\frac{3}{2}x - \frac{9}{4}\right)\left(-12x^2 + 10x - 2\right)}$$