M342 Álgebra Computacional

Christian Lomp

FCUP

26 e 28 de setembro de 2011

2.2 Os numeros racionais

Seja R um domínio integral e Q o corpo das fracções, i.e.

$$Q = \left\{ \frac{a}{b} \mid a, b \in R \wedge b \neq 0 \right\}$$

onde $\frac{a}{b} := \{(x, y) \in R^2 \mid y \neq 0 \wedge ay = bx.\}$.

2.2 Os numeros racionais

Seja R um domínio integral e Q o corpo das fracções, i.e.

$$Q = \left\{ \frac{a}{b} \mid a, b \in R \wedge b \neq 0 \right\}$$

onde $\frac{a}{b} := \{(x, y) \in R^2 \mid y \neq 0 \wedge ay = bx.\}$.

1. $R = \mathbb{Z}$, $Q = \mathbb{Q}$;
2. $R = \mathbb{C}[x]$, $Q = \mathbb{C}(x) =$ funções racionais;

2.2 Os numeros racionais

Seja R um domínio Euclideano então

$$\frac{a}{b} = \frac{c}{d}$$

onde $a = c\mathrm{mdc}(a, b)$ e $b = d = \mathrm{mdc}(a, b)$.
Vamos supor que $\frac{a}{b}$ é sempre na forma reduzida, i.e. $\mathrm{mdc}(a, b) = 1$.

2.2 Os numeros racionais

Seja R um domínio Euclideano então

$$\frac{a}{b} = \frac{c}{d}$$

onde $a = c\,\mathrm{mdc}(a, b)$ e $b = d = \mathrm{mdc}(a, b)$.
Vamos supor que $\frac{a}{b}$ é sempre na forma reduzida, i.e. $\mathrm{mdc}(a, b) = 1$.

$$\frac{a}{b} + \frac{x}{y} = \frac{ay + bx}{xy}$$
$$\frac{a}{b} \cdot \frac{x}{y} = \frac{ax}{by}$$

A classe dos números racionais

```
#include "inteiro.h"

class racional
{
inteiro numerador;
inteiro denumerador;

public:
racional();
racional(inteiro,inteiro);
racional operator + (racional);
racional operator * (racional);
racional inverso();
...

}
```

A classe dos números racionais

```
racional racional::racional(inteiro n, inteiro d)
{
numerador=n/mdc(n,d);
denumerador=d/mdc(n,d);
};

racional racional::operator + (racional b)
{
inteiro num=numerdor*b.denumerador + denumerador*b.numerador;
inteiro denum=denumerador*b.denumerador;
racional output(num,denum);
return output;
};
```

O teorema chinês do resto

Solução de sistemas de congruências de números relativamente primos $p_1, \ldots, p_k$

$$\begin{cases} x & \equiv & a_1 & \mod p_1 \\ x & \equiv & a_2 & \mod p_2 \\ \vdots \\ x & \equiv & a_k & \mod p_k \end{cases}$$

Seja $Q_j = \prod_{i \neq j} p_i$ para todo $1 \leq j \leq k$. Então

$$1 = \mathrm{mdc}(Q_j, p_j) = u_j Q_j + v_j p_j \qquad \Rightarrow \qquad a_j \equiv a_j u_j Q_j \mod p_j.$$

A solução é portanto

$$x = a_1 u_1 Q_1 + a_2 u_2 Q_2 + \ldots + a_k u_k Q_k \mod p_1 \cdots p_k.$$

2.3 A classes dos inteiros modulares

Ideias

1. Um *ideal* de um anel R é um subgrupo aditivo I de R tal que $ab \in I$ para todo $a \in R$ e $b \in I$.
2. Dado um subconjunto $X \subseteq R$ o menor ideal I de R que contém X chama-se o *ideal gerado por* X e é denotamos por $I = \langle X \rangle$.

2.3 A classes dos inteiros modulares

Ideias

1. Um *ideal* de um anel R é um subgrupo aditivo I de R tal que $ab \in I$ para todo $a \in R$ e $b \in I$.
2. Dado um subconjunto $X \subseteq R$ o menor ideal I de R que contém X chama-se o *ideal gerado por* X e é denotamos por $I = \langle X \rangle$.
3. Dado um elmento $a \in R$ os múltiplos de a formam um ideal de R que é igual ao ideal gerado por $\{x\}$.

$$\langle a \rangle = Ra = \{ba \mid b \in R\}.$$

2.3 A classes dos inteiros modulares

Ideias

1. Um *ideal* de um anel R é um subgrupo aditivo I de R tal que $ab \in I$ para todo $a \in R$ e $b \in I$.
2. Dado um subconjunto $X \subseteq R$ o menor ideal I de R que contém X chama-se o *ideal gerado por X* e é denotamos por $I = \langle X \rangle$.
3. Dado um elmento $a \in R$ os múltiplos de a formam um ideal de R que é igual ao ideal gerado por $\{x\}$.

$$\langle a \rangle = Ra = \{ba \mid b \in R\}.$$

4. O ideal $I = \langle a_1, \ldots, a_n \rangle = \{\sum_{i=1}^{n} b_i a_i \mid b_1, \ldots, b_n \in R\}$.

Exemplos

1. Ideais de $\mathbb{Z}$ são da forma $n\mathbb{Z} = \{an \mid a \in \mathbb{Z}\}$.

Exemplos

1. Ideais de $\mathbb{Z}$ são da forma $n\mathbb{Z} = \{an \mid a \in \mathbb{Z}\}$.
2. Ideais de $\mathbb{R}[x]$ são da forma $\langle f(x) \rangle = \{g(x)f(x) \mid g(x) \in \mathbb{R}[x]\}$.

Exemplos

1. Ideais de $\mathbb{Z}$ são da forma $n\mathbb{Z} = \{an \mid a \in \mathbb{Z}\}$.
2. Ideais de $\mathbb{R}[x]$ são da forma $\langle f(x) \rangle = \{g(x)f(x) \mid g(x) \in \mathbb{R}[x]\}$.
3. O subconjunto $\{2f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$ é um ideal de $\mathbb{Z}[x]$ que não é gerado por só um elemento.

2.3 A classes dos inteiros modulares

Classes laterais

1. A classe lateral à esquerda $a + I$ de um elemento $a \in R$ módulo um ideal I é o subconjunto

$$\overline{a} = a + I := \{a + b | b \in I\} \subseteq R$$

2.3 A classes dos inteiros modulares

Classes laterais

1. A classe lateral à esquerda $a + I$ de um elemento $a \in R$ módulo um ideal I é o subconjunto

$$\overline{a} = a + I := \{a + b | b \in I\} \subseteq R$$

2. Para $a, b \in R$ tem-se que

$$a + I = b + I \Leftrightarrow a - b \in I.$$

Exemplos

1. Para $m \in \mathbb{Z}$ a classe lateral de a módulo $\mathbb{Z}m$ é

$$\overline{a} = a + m\mathbb{Z} = \{ \text{ os números cujo resto da divisão por } m \text{ é } a\%m\}.$$

Exemplos

1. Para $m \in \mathbb{Z}$ a classe lateral de a módulo $\mathbb{Z}m$ é

$$\overline{a} = a + m\mathbb{Z} = \{ \text{ os números cujo resto da divisão por } m \text{ é } a\%m\}.$$

Para $m = 2$ só temos duas classes.

$$\overline{0} = 0 + 2\mathbb{Z} = \{ \text{ os números pares } \},$$

$$\overline{1} = 1 + 2\mathbb{Z} = \{ \text{ os números ímpares } \}.$$

Exemplos

1. Para $m \in \mathbb{Z}$ a classe lateral de a módulo $\mathbb{Z}m$ é

   $$\overline{a} = a + m\mathbb{Z} = \{ \text{ os números cujo resto da divisão por } m \text{ é } a\%m\}.$$

   Para $m = 2$ só temos duas classes.

   $$\overline{0} = 0 + 2\mathbb{Z} = \{ \text{ os números pares } \},$$

   $$\overline{1} = 1 + 2\mathbb{Z} = \{ \text{ os números ímpares } \}.$$

2. Em geral existem exactamente m classes laterais módulo m.

Exemplos

1. Para $f(x) \in \mathbb{R}[x]$

$$g(x)+\langle f(x)\rangle = \left\{ \begin{array}{l} \text{os polinómios cujo resto da divisão por } f(x) \\ \text{é } g(x)\% f(x) \end{array} \right\}.$$

Exemplos

1. Para $f(x) \in \mathbb{R}[x]$

$$g(x)+\langle f(x)\rangle = \left\{ \begin{array}{l} \text{os polinómios cujo resto da divisão por } f(x) \\ \text{é } g(x)\% f(x) \end{array} \right\}.$$

2. Para $f(x) = x^2 + 1 \in \mathbb{R}[x]$ temos que qualquer classe lateral tem a forma

$$a + bx + \langle x^2 + 1\rangle$$

onde $a, b \in \mathbb{R}$.

2.3 A classes dos inteiros modulares

Anel quociente

1. O anel quociente R/I de R módulo o ideal I é o conjunto das classes laterais:
$$R/I = \{a + I | a \in R\}.$$

2.3 A classes dos inteiros modulares

Anel quociente

1. O anel quociente R/I de R módulo o ideal I é o conjunto das classes laterais:
$$R/I = \{a + I | a \in R\}.$$

2. As operações em R/I são:
$$(a + I) + (b + I) = (a + b) + I$$
$$(a + I) \cdot (b + I) = (ab) + I,$$
para $a, b \in I$.

Exemplos

1. Para $m \in \mathbb{Z}$, tem-se que

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}.$$

Exemplos

1. Para $m \in \mathbb{Z}$, tem-se que

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}.$$

2. Para $f(x) \in \mathbb{R}[x]$ não-nulo, o anel quociente $\mathbb{R}[x]/\langle f(x)\rangle$ tem dimensão $n = \mathrm{grau}(f(x))$ e base $\{\overline{1}, \overline{x}, \dots, \overline{x^{n-1}}\}$ como espaço vectorial sobre $\mathbb{R}$.

Exemplos

1. Para $m \in \mathbb{Z}$, tem-se que

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}.$$

2. Para $f(x) \in \mathbb{R}[x]$ não-nulo, o anel quociente $\mathbb{R}[x]/\langle f(x)\rangle$ tem dimensão $n = \mathrm{grau}(f(x))$ e base $\{\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}\}$ como espaço vectorial sobre $\mathbb{R}$.
3. Para $f(x) = x^2 + 1$ tem-se que

$$\mathbb{R}[x]/\langle x^2+1\rangle \simeq \mathbb{C} \qquad \overline{a+bx} \mapsto a + \imath b.$$

Exemplos

1. Para $m \in \mathbb{Z}$, tem-se que

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}.$$

2. Para $f(x) \in \mathbb{R}[x]$ não-nulo, o anel quociente $\mathbb{R}[x]/\langle f(x) \rangle$ tem dimensão $n = \mathrm{grau}(f(x))$ e base $\{\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}\}$ como espaço vectorial sobre $\mathbb{R}$.
3. Para $f(x) = x^2 + 1$ tem-se que

$$\mathbb{R}[x]/\langle x^2+1 \rangle \simeq \mathbb{C} \qquad \overline{a+bx} \mapsto a + \imath b.$$

4. Para $f(x) = x^2 + 1 \in \mathbb{Z}[x]$ tem-se que

$$\mathbb{Z}[x]/\langle x^2+1 \rangle \simeq \mathbb{Z}[\imath].$$

2.3 A classes dos inteiros modulares

Teorema

Seja R um domínio Euclideano e $I = \langle m \rangle$ o ideal gerado por um elemento $m \in R$. Para qualquer elemento $a \in R$ tem-se que $a + \langle m \rangle$ é invertível em $R/\langle m \rangle$ se e só se $\mathrm{mdc}(a, m) \sim 1$

Definição

Um elemento não invertível $p \in R$ diz-se irredutível (ou primo) se $a \mid p$ então $a \sim 1$ ou $a \sim p$.

Definição

Um elemento não invertível $p \in R$ diz-se irredutível (ou primo) se $a \mid p$ então $a \sim 1$ ou $a \sim p$.

Corolário

Seja R um domínio Euclideano. Então $\overline{R} = R/\langle m \rangle$ é um corpo se e só se m é irredutível.

Definição

Um elemento não invertível $p \in R$ diz-se irredutível (ou primo) se $a \mid p$ então $a \sim 1$ ou $a \sim p$.

Corolário

Seja R um domínio Euclideano. Então $\overline{R} = R/\langle m \rangle$ é um corpo se e só se m é irredutível.

Prova: Se m for irredutível e $a \in R$ então $\mathrm{mdc}(a, m) \sim 1$ ou $\mathrm{mdc}(a, m) \sim p$. Se $\mathrm{mdc}(a, m) \sim m$, então $m|a$ e $\overline{a} = \overline{0}$.

1. $\mathbb{Z}_m$ corpo se e só se m é primo.

1. $\mathbb{Z}_m$ corpo se e só se m é primo.
2. $K[x]/\langle f(x) \rangle$ é corpo se e só se $f(x)$ é um polinómio irredutível.

1. $\mathbb{Z}_m$ corpo se e só se m é primo.
2. $K[x]/\langle f(x)\rangle$ é corpo se e só se $f(x)$ é um polinómio irredutível.
3. $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ é corpo com 4 elementos!

1. $\mathbb{Z}_m$ corpo se e só se m é primo.
2. $K[x]/\langle f(x)\rangle$ é corpo se e só se $f(x)$ é um polinómio irredutível.
3. $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ é corpo com 4 elementos!
4. **Galois:** para qualquer $n \geq 1$ e número primo p existe um polinómio irredutível $f(x) \in \mathbb{Z}_p[x]$ de grau n. Logo existe um corpo com p^n elementos.

Como calcular os inversos em $R/\langle m \rangle$?

Como calcular os inversos em $R/\langle m\rangle$?

Inversos

Sejam $a, m \in R$ com $\mathrm{mdc}(a, m) \sim 1$.
Pelo Algoritmo estendido de Euclides existem $x, y \in R$ tais que

$$1 = xa + ym \qquad \text{ou seja} \qquad 1 - xa \in \langle m\rangle \Leftrightarrow \overline{1} = \overline{xa}.$$

Logo $\overline{x}$ é o inverso de $\overline{a}$ em $R/\langle m\rangle$.

Equações Diofantinas Lineares

A equação diofantinas lineares:

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c,$$

com $a_1, \ldots, a_n, c \in \mathbb{Z}$ tem soluções $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ se e só se $\mathrm{mdc}(a_1, \ldots, a_n)|c$.

Equações Diofantinas Lineares

$$ax + by = c \qquad \Leftrightarrow \qquad a'x + b'y = c'$$

onde $a' = \frac{a}{\mathrm{mdc}(a,b)}, b' = \frac{b}{\mathrm{mdc}(a,b)}, c' = \frac{c}{\mathrm{mdc}(a,b)}$.
Existem $s, t \in \mathbb{Z}$ tais que $1 = sa' + tb'$ e $c' = c'sa' + c'tb'$.

$$\begin{aligned}
&\Rightarrow \quad a'(x - c's) + b'(y - c't) = c' - c' = 0 \\
&\Leftrightarrow \quad a'(x - c's) = b'(c't - y) \\
&\Rightarrow \quad a' | (c't - y) \qquad \text{porque } \mathrm{mdc}(a', b') = 1 \\
&\Rightarrow \quad c't - y = a'n, \qquad n \in \mathbb{Z} \\
&\Rightarrow \quad y = c't - a'n, \qquad n \in \mathbb{Z} \\
&\Rightarrow \quad x = c't + b'n, \qquad n \in \mathbb{Z}
\end{aligned}$$

A classe dos inteiros módulares

```
class modular
{
unsigned int modulo;
int numero;

int mdc(int ,int );

public:
modular(unsigned int ,int );
modular operator + (modular);
modular operator - (modular);
modular operator * (modular);
bool invertivel();
modulear inverso ();
}
```

A classe dos inteiros módulares

```
modular(unsigned int n, int a)
{
base=n;
numero=a%n;
};

modular modular::operator + (modular b)
{
if (b.base == base)
return modular(base,b.numero+numero)
};

bool invertivel()
{
return (mdc(numero,base)==1);
};
```

Algoritmo de Euclid em C++

```
int mdc(int a, int b, int* x, int* y)
{
int r0,s0,t0,r1,s1,t1;
r0=a; s0=1; t0=0;
r1=b; s1=0; t1=1;

while(r1!=0)
{
  int q = r0/r1;
  int h = r0%r1; r0=r1; r1=h;
  h=s0-q*s1; s0=s1; s1=h;
  h=t0-q*t1; t0=t1; t1=h;
};
(*x)=s0;
(*y)=t0;
return r0;
};

int main()
{
int a,b,x,y;
x=0;
y=0;
cin >> a >> b;
cout << "mdc=" << mdc(a,b,&x,&y);
cout << "␣=␣" << x << "*" << a << "␣+␣"<<  y << "*" << b << endl;
}
```