M342 Álgebra Computacional

Christian Lomp

FCUP

19 de setembro de 2011

2. Estruturas de dados

A classe inteiro

```
#include <vector>
#include <inteiro>

class inteiro {

  bool sinal;
  unsigned int base;
  vector<unsigned int> coeficientes;

public:
  inteiro();
  void operator = (inteiro); // copiar
  bool operator < (inteiro); // comparar
  bool operator == (inteiro); // comparar
  inteiro operator + (inteiro); // somar
  inteiro operator - (inteiro); // subtrair
  inteiro operator * (inteiro); // multiplicar
  inteiro operator / (inteiro); // quociente
  inteiro operator % (inteiro);  // resto
}
```

2.

Aritmética dos polinómios

O anel dos polinómios

Um polinómio não nulo $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ com coeficientes num anel comutativo R é únicamente determinado pelos seus coeficientes $(a_0, a_1, \ldots, a_n)$ onde $a_n \neq 0$.

2.

Aritmética dos polinómios

O anel dos polinómios

Um polinómio não nulo $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ com coeficientes num anel comutativo R é únicamente determinado pelos seus coeficientes $(a_0, a_1, \ldots, a_n)$ onde $a_n \neq 0$. Neste caso chama-se n o *grau* do polinómio. $\mathrm{grau}(f) = n$. No caso do polinómio nulo 0 escrevemos $\mathrm{grau}(0) = -\infty$.

2.

Aritmética dos polinómios

O anel dos polinómios

Um polinómio não nulo $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ com coeficientes num anel comutativo R é únicamente determinado pelos seus coeficientes $(a_0, a_1, \ldots, a_n)$ onde $a_n \neq 0$. Neste caso chama-se n o *grau* do polinómio. $\mathrm{grau}(f) = n$. No caso do polinómio nulo 0 escrevemos $\mathrm{grau}(0) = -\infty$. O coeficiente a_n chama-se o **coeficiente guia** (*leading coefficient*) denotado por $a_n = \mathrm{lc}(f)$.

2.

Representamos polinómios pela sucesão dos seus coeficientes.

2.

Representamos polinómios pela sucesão dos seus coeficientes.
Dois polinómios não-nulos $f = (a_0, \ldots, a_n)$ e $g = (b_0, \ldots, b_m))$ são iguais se

$$n = m \qquad a_i = b_i \ \forall 0 \leq i \leq n.$$

2.

Representação de polinómios com C++

```
#include <vector>
#include <inteiro>

class polinomio {

  bool nulo;
  vector<inteiro> coeficientes;

public:
  polinomio();
  unsigned int grau();
  inteiro leadingCoeficient();
  polinomio operator + (polinomio);
  polinomio operator - (polinomio);
  polinomio operator * (polinomio);
  ...
}
```

2.

Adição de Polinómios

Sejam $f = \sum_{i=0}^{n} a_i x^i$ e $g = \sum_{j=0}^{m} b_j x^j$ com $n \leq m$. então

$$f + g = \sum_{i=0}^{n} (a_i + b_i) x^i + \sum_{i=n+1}^{m} b_i x^i.$$

2.

Adição/Subtração de Polinómios

Input: polinómios $f = (a_0, \ldots, a_n)$, $g = (b_0, \ldots, b_m)$ com $n \leq m$
Output: polinómio $h = (c_0, \ldots, c_m)$ tal que $h = f \pm g$.

for $i = 0, \ldots, n$ **do**
  $c_i \leftarrow a_i \pm b_i$
end for
for $i = n+1, \ldots, m$ **do**
  $c_i \leftarrow b_i$
end for

2.

Multiplicação de polinómios

Sejam $f = (a_0, \ldots, a_n)$ e $g = (b_0, \ldots, b_m))$ dois polinómios não-nulos. Então

$$fg = (c_0, \ldots, c_{nm}) \qquad \text{com } c_k = \sum_{i+j=k} a_i b_j.$$

2.

Multiplicação de polinómios

Sejam $f = (a_0, \ldots, a_n)$ e $g = (b_0, \ldots, b_m))$ dois polinómios não-nulos. Então

$$fg = (c_0, \ldots, c_{nm}) \qquad \text{com } c_k = \sum_{i+j=k} a_i b_j.$$

Alternativamente

$$fg = \sum_{i=0}^{n} a_i x^i g.$$

onde $a_i x^i$ é optido por uma translação e multiplicação escalar:

$$(b_0, \ldots, b_m) \mapsto (\underbrace{0, \ldots, 0}_{i-\text{posições}}, a_i b_0, \ldots, a_i b_m).$$

2.

Multiplicação de polinómios

Input: polinómios $f = (a_0, \dots, a_n)$, $g = (b_0, \dots, b_m)$.
Output: polinómio $h = (c_0, \dots, c_{nm})$ tal que $h = fg$.

$h \leftarrow (0)$
for $i = 0, \dots, n$ **do**
  $z \leftarrow shift(i, g)$
  $h \leftarrow h + a_i * z;$
end for
return h

2.

Multiplicação por um monómio

Input: polinómio $g = (b_0, \dots, b_m)$ e exponente i
Output: polinómio $h = shift(i, g) = x^i g$

$h \leftarrow (\underbrace{0, \dots, 0}_{i-\text{posições}})$

for $j = 0, \dots, m$ **do**

$h_{i+j} \leftarrow b_j$

end for

return h

2.

Multiplicação por um escalar

Input: polinómio $g = (b_0, \ldots, b_m)$ e escalar a
Output: polinómio $h = a * g$

for $j = 0, \ldots, m$ **do**
  $h_j \leftarrow a * b_j$
end for
return h

2.

Divisão com resto

Dados inteiros a e b existem inteiros q e r tais que

$$a = qb + r, \qquad \text{com } |r| < |b|.$$

2.

Divisão com resto

Dados inteiros a e b existem inteiros q e r tais que

$$a = qb + r, \qquad \text{com } |r| < |b|.$$

Dado um anel comutativo R e polinómios $f, g \in R[x]$ com $g \neq 0$ queremos encontrar polinómios q e r tais que

$$f = qg + r \qquad \text{com } \mathrm{grau}(r) < \mathrm{grau}(g).$$

2.

Divisão com resto

Dados inteiros a e b existem inteiros q e r tais que

$$a = qb + r, \qquad \text{com } |r| < |b|.$$

Dado um anel comutativo R e polinómios $f, g \in R[x]$ com $g \neq 0$ queremos encontrar polinómios q e r tais que

$$f = qg + r \qquad \text{com } \mathrm{grau}(r) < \mathrm{grau}(g).$$

Nem sempre isto é possível: $R = \mathbb{Z}$, $f = x^2$ e $g = 2x + 1$.

$$
\begin{array}{r|l}
 & 3x^2 \quad - 4x - 1 \\
\hline
x^2 + 2x + 3 & 3x^4 + 2x^3 \qquad\qquad + x + 5 \\
 & \underline{-3x^4 - 6x^3 - 9x^2} \\
 & \qquad -4x^3 - 9x^2 \quad + x \\
 & \qquad \underline{4x^3 + 8x^2 + 12x} \\
 & \qquad\qquad -x^2 + 13x + 5 \\
 & \qquad\qquad \underline{x^2 \quad + 2x + 3} \\
 & \qquad\qquad\qquad 15x + 8
\end{array}
$$

2.

Divisão de polinómios

Input: polinómios $f = (a_0, \ldots, a_n)$, $g = (b_0, \ldots, b_m)$ com $m \leq n$ e b_m invertível.

Output: polinómios $q = (c_0, \ldots, c_k)$ e $r = (d_0, \ldots, d_l)$ tal que $g = qg + r$ e $\mathrm{grau}(r) < \mathrm{grau}(g)$.

$r \leftarrow g$
$q \leftarrow (0)$
for $i = n - m, n - m - 1, \ldots, 0$ **do**
  if $\mathrm{grau}(r) = m + i$ **then**
    $q \leftarrow q + \mathrm{lc}(r) b_m^{-1} x^i$
    $r \leftarrow r - \mathrm{lc}(r) b_m^{-1} x^i g$
  end if
end for
return (q, r)