NO. 17
DATE 5 17 2015

2.2 多項式の表現

2.2.1 多項式の表現と加算.

- R : 可換環.
- $R[x, y, \dots, z]$ 変数 $x, y, \dots, z$ をもつ R 上の多項式全体.

  ($R[x, y, \dots, z]$ 上の自然な加減乗算が定義でき, $R[x, y, \dots, z]$ は可換環となる).

- 当面は 変数を x : 1変数.
  係数を $\mathbb{Z}$: $\mathbb{Z}[x]$.

Def (主項, 主係数, 次数, モニック)

$$a(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x], \quad a_n \neq 0$$

$a_n x^n$: $a(x)$ の 主項 (the leading term), $lt(a(x))$.
a_n : —— の主係数 (the leading coefficient), $lc(a(x))$.
n : —— の次数 (degree), $\deg(a(x))$.
$a(x)$ がモニック (monic) $\Leftrightarrow$ $lc(a(x)) = 1$.

□

Def (1変数多項式の表現)

$$a(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x], \quad a_n \neq 0$$

を

$$(a_0, \dots, a_n) \in \mathbb{Z}^{n+1}$$ で表す.

□ 5/25

6/1

◎ 1変数多項式の加算.

$$a(x) = \sum_{i=0}^{k} a_i x^i = (a_0, a_1, \dots, a_k),$$
$$b(x) = \sum_{i=0}^{k} b_i x^i = (b_0, b_1, \dots, b_k)$$

に対し,

$$c(x) = a(x) + b(x) = \sum_{i=0}^{k} c_i x^i = (c_0, c_1, \dots, c_k)$$

を求める.

Algorithm (1変数多項式の加算)

入力: $a(x) = \sum_{i=0}^{k} a_i x^i$, $b(x) = \sum_{i=0}^{k} b_i x^i$. $\in \mathbb{Z}[x]$

出力: $c(x) = \sum_{i=0}^{k} c_i x^i \in \mathbb{Z}[x]$ s.t. $c(x) = a(x) + b(x)$.

(1) for $i \in [0..k]$ do $c_i \leftarrow a_i + b_i$;
(2) return $(c_0, c_1, \ldots, c_k)$; ■

■ 注意

- $\deg(a) \neq \deg(b)$ の場合は、しかるべき対応(拡張)が必要.
- a_i も b_i として多倍長整数が用いられることもある.

■ 計算量

$$
\begin{array}{rcl}
a(x) & = & (a_0,\ a_1,\ \cdots,\ a_k) \\
 & & \ \ +\ \ \ +\ \ \ \ \ \ \ \ \ \ + \quad \leftarrow \text{加算 } k+1 \text{ 回} = \Theta(k) \\
b(x) & = & (b_0,\ b_1,\ \cdots,\ b_k) \\
c(x) & = & (c_0,\ c_1,\ \cdots,\ c_k)
\end{array}
$$

$\Theta(\mathrm{len}(a_0))$ $\Theta(\mathrm{len}(a_1))$ $\cdots$ $\Theta(\mathrm{len}(a_k))$ の和.

各桁の多倍長数の長さに比例.

- 全体では $\Theta\left(\sum_{i=0}^{k} \mathrm{len}(a_i)\right)$.
- 係数がすべて単精度ならば $\Theta(k)$
- 係数がすべて m ワードならば $\Theta(mk)$.

2.2.2 ホーナー (Horner) 法.

◎多項式の評価

$a(x) \in R[x]$, $x_0 \in R$. $a(x) = a_n x^n + \cdots + a_1 x + a_0$.

$a(x_0)$ の値を求める : $x = x_0$ で $a(x)$ の値を評価する

◎素朴な方法

例 $a(x) = 5x^4 + 3x^3 - 2x^2 + 8x - 10$, $x = 10$

$$a(10) = 5\cdot 10^4 + 3\cdot 10^3 - 2\cdot 10^2 + 8\cdot 10 - 10$$

乗算 4 3 2 1

↑

$\deg a = n$ のとき、$\displaystyle\sum_{j=1}^{n} j = \frac{n(n+1)}{2} = O(n^2)$ . ... (*)

◎剰余定理と組立除法 = Horner法.

剰余定理 $a(x) \in R[x]$, $x_0 \in R$

$a(x)$ を $x - x_0$ で割った剰余は $a(x_0)$ に等しい. $\boxed{\text{言}}$

組立除法

$a(x)$ の係数を並べる.

$$\begin{array}{r|rrrrr}
\overset{x_0}{10} & 5 & 3 & -2 & 8 & -10 \\
1\text{倍} & & 50 & 530 & 5280 & 52880 \\
\hline
 & 5 & 53 & 528 & 5288 & \boxed{52870} = a(10) \\
 & & 10\text{倍} & 10\text{倍} & 10\text{倍} & 10\text{倍}
\end{array}$$

組立除法は

$a(10) = (((5\cdot 10+3)\cdot 10-2)\cdot 10+8)\cdot 10 - 10$ と求めている.

より一般に. $a(x) = a_n x^n + \cdots + a_1 + a_0$ に対し. $a(x_0)$ を求める場合は

$$a(x_0) = ((\cdots((a_n x_0 + a_{n-1})x_0 + a_{n-2})x_0 + \cdots)\cdot x_0 + a_1)x_0 + a_0$$

と計算をする. → $\boxed{\text{ホーナー法 (Horner)}}$ と呼ばれる. ≡ $\boxed{\text{組立除法}}$

(Horner (英) が 19世紀前期に発表. しかし、東洋ではより古くから組立除法として知られていたとのこと.)

◎ Horner 法のアルゴリズムと計算量.

__アルゴリズム__ (Horner 法)

__入力__ $a(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $x_0 \in \mathbb{Z}$.
__出力__ $y = a(x_0) \in \mathbb{Z}$.

ループ n 回

(1) $y \leftarrow a_n$;
(2) for $i \in [n-1..0]$ do $y \leftarrow y \cdot x_0 + a_i$;
(3) return y; ◎

乗算1回 加算1回

全体の演算回数は $\Theta(n)$ … (☆)の $\Theta(k(n^2)n)$ に比べ、大分小さくなっている!
(現時点で多倍長整数の乗算の計算量を評価していないことに注意.)

6/1

2.2.3 非負整数の2進・10進変換.

6/8

※ Horner 法のアイデアで効率化できる.

◎ 2進表記 → 10進表記. (整数)

__例__ $m = 1\,0\,1\,1\,0\,1\,1$

$$2^6 + 2^4 + 2^3 + 2^1 + 2^0$$
$$= 64 + 16 + 8 + 2 + 1 = 91.$$

これは、

$$M(x) = 1 \cdot x^6 + \underbrace{}_{0 \cdot x^5 +} 1 \cdot x^4 + 1 \cdot x^3 + \underbrace{}_{0 \cdot x^2 +} 1 \cdot x + 1$$

において、$M(2)$ を求める計算と同値.
そこで、$M(2)$ の計算に Horner 法を用いると、次のように計算される.

$$\begin{aligned}
M(2) &= ((((((\underset{a_6}{1} \cdot 2 + \underset{a_5}{0})2 + \underset{a_4}{1})2 + \underset{a_3}{1})2 + \underset{a_2}{0})2 + \underset{a_1}{1})2 + \underset{a_0}{1} \\
&= ((((2 \cdot 2 + 1)2 + 1)2 + 0)2 + 1)2 + 1 \\
&= ((((5 \cdot 2 + 1)2 + 0)2 + 1)2 + 1 \\
&= (((11 \cdot 2 + 0)2 + 1)2 + 1 \\
&= ((22 \cdot 2 + 1)2 + 1 \\
&= 45 \cdot 2 + 1 = 91.
\end{aligned}$$