6/13

2.4 剰余つき除算.

▨ 整数の剰余つき除算.

Thm. 1 (整数の剰余つき除算の性質.)

$a, b \in \mathbb{Z}$, $b > 0$ のとき, $\exists q, r \in \mathbb{Z}$ s.t. $a = bq + r$ かつ $0 \leq r < b$.

(Proof) ⟶ 問題 2.13. ▨

Def. 2 (整数の剰余つき除算)

a, b, q, r as in Thm. 1.

- a, b に対し, 上の q, r を求める計算を a の b による除算といい, $a \div b$ で表す.
- a : 被除数 (dividend)
- b : 除数 (divisor)
- q : 商 (quotient) $= \mathrm{quo}(a, b)$
- r : 剰余 (remainder) $= a \bmod b$.
- $a \div b$ に対し, q と r の組を同時に求めることを $(q, r) \longleftarrow a \div b$ で表す. ▨

2.4.1 多項式の剰余つき除算.

$a(x), b(x) \in \mathbb{Z}[x]$, $b(x)$: monic
$\deg(a) = k \geq m = \deg(b)$.

に対し. 多項式の剰余つき除算を Def. 2 と同様に定義する.

例) $a(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$, $b(x) = 1 \cdot x + b_0$.

$$
\begin{array}{rr|llll}
 & & a_3 & a_2 - a_3 b_0 & a_1 - a_2 b_0 + a_3 b_0^2 & \\
\hline
1 & b_0 & a_3 & a_2 & a_1 & a_0 \\
 & & a_3 & a_3 b_0 & & \\
\hline
 & & & a_2 - a_3 b_0 & a_1 & \\
 & & & a_2 - a_3 b_0 & a_2 b_0 - a_3 b_0^2 & \\
\hline
 & & & & a_1 - a_2 b_0 + a_3 b_0^2 & a_0 \\
 & & & & a_1 - a_2 b_0 + a_3 b_0^2 & a_1 b_0 - a_2 b_0^2 + a_3 b_0^3 \\
\hline
 & & & & & a_0 - a_1 b_0 + a_2 b_0^2 - a_3 b_0^3
\end{array}
$$

Algorithm (多項式の剰余つき除算)

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

$b(x) = x^m + \sum_{i=0}^{m-1} b_i x^i \in \mathbb{Z}[x]$ with $m \leq k$;

出力: $q(x) = \sum_{i=0}^{k-m} q_i x^i \in \mathbb{Z}[x]$ (quotient),

$r(x) = \sum_{i=0}^{m-1} r_i x^i \in \mathbb{Z}[x]$ (remainder).

s.t. $a(x) = q(x)\, b(x) + r(x)$;

(1) for $i \in [k..0]$ do $r_i \leftarrow a_i$;
($r(x) \leftarrow a(x)$)

(2) for $i \in [k-m..0]$ do　　ループ $(k-m+1)$回

$q_i \leftarrow r_{i+m}$; $r_{i+m} \leftarrow 0$;
for $j \in [m-1..0]$ do　　ループ m 回
$r_{i+j} \leftarrow r_{i+j} - q_i b_j$;

乗算 1回
加算 1回

(3) return $[(q_{k-m}, \ldots, q_0), (r_{m-1}, \ldots, r_0)]$;

・係数の演算回数 : $O((k-m+1)m) = O(km)$.

2.4.2 多倍長整数÷単精度整数の剰余つき除算.

$[a_0\ a_1]$: 倍精度整数 (長さ2) : $a_1 \cdot 2^n + a_0$.

b : 単精度整数 : $0 \leq a_1 < b$.

このとき、計算機は $(q, r) \leftarrow [a_0\ a_1] \div b$
(ただし、q, r はそれぞれ単精度変数) なる除算の機構をもつ(とする).

4. ユークリッド互除法 (The Euclidean Algorithm)

◎ 復習 (主に2年次の「代数入門」から)

- R : 可換環 (commutative ring)
- R のイデアル (ideal)
  - 生成元 (generator(s))
  - 有限生成 (finitely generated)
  - 単項イデアル (principal ideal)
- 剰余類 (residue class), 剰余環 (residue class ring)

Def 4.3 (p. 49)

- 約元 (divisor), 倍元 (multiple),
- 最大公約元 (the greatest common divisor, GCD)
- 最小公倍元 (the least common multiple)

一般に一意には定まらないが、$R=\mathbb{Z}$ の場合、正数にとれば一意に定まる。

4.2 Euclid 整域と互除法

Def 4.11 (Euclid 整域)

R : 整域, $d : R \longrightarrow \mathbb{N} \cup \{-\infty\}$.
このとき、(R, d) が Euclid 整域 (Euclidean Domain)

$\overset{\text{def}}{\iff} \forall a, b \in R \ (b \neq 0 \Rightarrow \exists q, r \in R \text{ s.t. } a = bq + r, \ d(r) < d(b))$

- d : Euclid 関数 (Euclidean function)
- q : (a を b で割ったときの) 商 (quotient)
- r : 剰余 (remainder) ☒

※ a と b に対し、q と r が一意に定まるとは限らない。

Def. 4.14 (互いに素)

$a_1, \ldots, a_n \in R$ が互いに素 (mutually prime)
$\overset{\text{def}}{\iff}$ $a_1, \ldots, a_n$ の GCD が単元。
特に $a, b \in R$ が互いに素のとき、$a \perp b$ で表す。 ☒