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 $0 \le r < b$.

Proof ⟶ 問題 2.13. (6/23) ↓ □

Def. 2 (整数の剰余つき除算) (6/29)

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

- a, b に対し, 上の q, r を定める対応を 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) $= quo(a, b)$
- 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

$$(q, r) \leftarrow a \div b$$

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

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) $a(x) = a_3x^3 + a_2x^2 + a_1x + a_0$, $b(x) = 1x + b_0$ の場合.

$$\begin{array}{r|l} & a_3 \\ \hline 1 \quad b_0 & a_3 \quad a_2 \quad a_1 \quad a_0 \\ & a_3 \quad a_3b_0 \\ \hline & a_2 - a_3b_0 \quad \cdots \end{array}$$

□

6-21-2015

Algorithm (多項式の剰余つき除算)

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

$b(x) = x^m + \sum_{i=0}^{m-1} b_i x^i \in \mathbb{Z}[x]$ (monic).

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

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

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.

$q_i \leftarrow r_{i+m}$;

for $j \in [m-1 \,..\, 0]$ do ← ループ m回.

$r_{i+j} \leftarrow r_{i+j} - q_i b_j$;

(3) return ($(q_{k-m}, \ldots, q_0)$, ← 等式1回
$(r_{m-1}, \ldots, r_0)$); ← 加算1回

・係数の演算回数: $O((k-m+1)m) = O(km)$.

($k \geq m$ を仮定する. $k < m$ のときは (2) は実行されないので, 実質的な計算は行われない.)

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. $a_1 2^n + a_0$.
(底 2^n)

b : 単精度整数. $0 \leq a_1 < b$.

このとき, 計算機で $(q, r) \leftarrow [a_0\ a_1] \div b$
(ただし, q, r はそれぞれ単精度整数) なる「除算の操作」をもつ(とする).

NO. 35

DATE 6 25 2015

4. ユークリッドの互除法 (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) (Generator(s))
  - 生成元, 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 (greatest common divisor) GCD)
- 最小公倍元 (least common multiple) LCM) □

一般に一意的に定まらないが, $R=\mathbb{Z}$ の場合, 正数でそれが一意的に定まる.

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)

$\overset{\text{def}}{\Longleftrightarrow}$ $\forall a, b \in R$,

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

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

□

★ a と b に対し, q, r が一意的に定まるとは限らない.

Def. 4.14 (互いに素)

$a_1, \dots, a_n \in \mathbb{R}$ が互いに素 (mutually prime)

def $\Leftrightarrow$ $a_1, \dots, a_n$ の GCD が単元.

特に $a, b \in R$ が互いに素のとき, $a \perp b$ とかく.

□

◎ Euclid の互除法.

Theorem (EA) $a, b \in \mathbb{Z}$. with $a \geq b \geq 0$.
剰余つき除算により, $\lambda \geq 0$ が好しく
$r_0, r_1, \dots, r_{\lambda+1}$ および $q_1, \dots, q_\lambda$ を以下により定める:

$$
\begin{aligned}
a &= r_0, \\
b &= r_1, \\
r_0 &= r_1 q_1 + r_2 \qquad (0 < r_2 < r_1), \\
&\vdots \\
r_{i-1} &= r_i q_i + r_{i+1} \qquad (0 < r_{i+1} < r_i), \\
&\vdots \\
r_{\lambda-2} &= r_{\lambda-1} q_{\lambda-1} + r_\lambda \qquad (0 < r_\lambda < r_{\lambda-1}), \\
r_{\lambda-1} &= r_\lambda q_\lambda \qquad (r_{\lambda+1} = 0).
\end{aligned}
$$

(このとき, $\lambda \begin{cases} = 0 & (b = 0) \\ > 0 & (\text{その他}). \end{cases}$)

このとき. ① $r_\lambda = \gcd(a, b)$.

② $b > 0 \Rightarrow \lambda \leq \dfrac{\log b}{\log \varphi} + 1$.

ただし $\varphi = \dfrac{1+\sqrt{5}}{2} \simeq 1.62$ (黄金比).

(φ は $\varphi^2 - \varphi - 1 = 0$ をみたす.)

Proof ① (テキスト p.51.) Thm 4.15 を参照.

② $b>0$ と仮定. $\therefore \lambda > 0$.
$\lambda = 1$ のとき自明.
$\lambda > 1$ とおく. このとき, $i = 0, \dots, \lambda - 1$ において,

(※) $\boxed{r_{\lambda - i} \geq \varphi^i}$ $\Rightarrow$ $i = \lambda - 1$ とおいて log をとると

$$r_1 = b \geq \varphi^{\lambda - 1}.$$

$$\therefore \log b \geq (\lambda - 1)\log\varphi.$$

$$\therefore \lambda - 1 \leq \frac{\log b}{\log \varphi} \qquad \therefore \lambda \leq \frac{\log b}{\log \varphi} + 1.$$

そこで, (※) を示す. (帰納法)

$i = 0$ のとき $r_\lambda \geq 1 = \varphi^0$.
$i = 1$ 〃 $r_{\lambda-1} \geq r_\lambda + 1 \geq 2 \geq \varphi^1$.

$i = 2, \dots, \lambda - 1$ のとき. $\varphi^2 = \varphi + 1$ を用いると

$$r_{\lambda - i} \geq r_{\lambda-(i-1)} + r_{\lambda-(i-2)}$$
$$\geq \varphi^{i-1} + \varphi^{i-2} = \varphi^{i-2}\underbrace{(1+\varphi)}_{\varphi^2} = \varphi^i$$

により成り立つ. ☒ 6/29

Note 上の証明は, $r_{\lambda - i}$ を構成するのに, b がどんな値をとると, 最も λ が大きくなるか (= 剰余をとる計算の回数が大きくなるか) という考察である. すると, $r_i = 1$, すなわち $r_{\lambda - i}$ がフィボナッチの数列になることがわかる. 7/6

Note K を体とするとき, $K[x]$ は, Euclid 整域である. Euclid 関数 d を $d(f) = \deg f$ で定義すれば Euclid 整域であり, Euclid の互除法が $\mathbb{Z}$ と同様に成り立つ.