NO. 35

DATE 5 · 31 · 2016

7/6

⑪ 法逆元計算 (Computing modular inverse) (§4.7, p.59)

R：可換環，I⊂R：イデアル，R/I：剰余環．
a ∈ R/I が単元のとき (⇔ 乗法の逆元をもつ)，
その逆元を計算する！
(Iを法とするaの逆元「法逆元」)

この計算も，EEAが有効である．
← Euclid関数．

Theorem 4.50 (R, d)：Euclid整域．
a, m ∈ R
このとき，a mod m ∈ R/mR が単元 ⇔ gcd(a, m) = 1.
∪
{a + bm | b ∈ R}

よって，このとき，EEAを用いて，R/mRにおける a mod m の逆元 b を計算可能．(s.t. a·b ≡ 1 mod m.)

(Proof)

a mod m が R/mR の単元
⇔ ∃ s ∈ R s.t. s·a ≡ 1 mod m
⇔ ∃ -t ∈ R s.t. s·a - 1 = -t·m
⇔ s·a + t·m = 1 ← s,tはEEAにより計算可能．
⇐ gcd(a, m) = 1.

(⇐) gcd(a,m) = 1
⇒ EEAより ∃ s,t ∈ R s.t. sa + tm = 1
⇔ sa = 1 - tm
⇔ sa ≡ 1 mod m
⇔ s は a の R/mR における乗法の逆元.
(s mod m) (a mod m)

□

☆ <r, s, t> ← EEA(a, m) において

- r = 1 ⇒ s mod m が R/mR における a mod m の逆元．
- r ≠ 1 ⇒ a mod m は R/mR において単元ではなく，逆元は存在しない．

NO. 36

DATE 5 · 31 · 2016

例 4.51　　$R=\mathbb{Z}$, $m=29$, $a=12$.

$m=29$ を法として $a=12$ の逆元が存在するかを求める.

$\langle r, s, t\rangle \leftarrow EEA(29, 12)$ を計算する.

$i=0$　$r_0=29$, $s_0=1$, $t_0=0$;

$i=1$　$r_1=12$, $s_1=0$, $t_1=1$;

$i=2$　$r_2=29-2\cdot 12$, $q_1=2$, $s_2=1$, $t_2=-2$;
$=29-24$
$=5$.

$i=3$　$r_3=12-2\cdot 5$, $q_2=2$, $s_3=0-2$, $t_3=1-2(-2)$
$=12-10$　　$=-2$, $=5$;
$=2$

$i=4$　$r_4=5-2\cdot 2$, $q_3=2$, $s_4=1-2(-2)$, $t_4=-2-2\cdot 5$
$=5-4$　　$=5$　　$=-12$;
$=1$.

$i=5$　$r_5=2-2\cdot 1$, $q_4=2$, $s_5=-2-2\cdot 5$, $t_5=5-2(-12)$
$=0$.　　$=-12$, $=29$.

よって $i=4$ のとき, $\underbrace{5}_{=m}\cdot\underbrace{29}+\underbrace{(-12)}_{=a}\cdot 12=1$.

$\therefore \underbrace{(-12)}_{=11}\, a \equiv 1 \mod 29$

$17 \mod 29$.

より, 17 が 29 を法とする 12 の逆元. □

問題 4.53　　$f(x)=$ α: 方程式 $x^3-x^2-x-1=0$ の根の一つ.

$R=\mathbb{Q}(\alpha)$ で $\alpha^2+\alpha$ の逆元を $A\alpha^2+B\alpha+C$ $(A, B, C\in\mathbb{Q})$ の形で表せ.

$\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/\langle f(x)\rangle$

$A\alpha^2+B\alpha+C \leftrightarrow Ax^2+Bx+C$　$(A, B, C\in\mathbb{Q})$

$f(x)$ は $\mathbb{Q}$ 上既約より. $\mathbb{Q}[x]/\langle f(x)\rangle$ は体をなす. そこで,

$g(x)=x^2+x \in \mathbb{Q}[x]/\langle f(x)\rangle$ の逆元を EEA で求める.
$(x^2+x$ と $f(x)$ を法とする逆元$)$

$i=0$ $r_0 = f(x)$, $s_0 = 1$, $t_0 = 0$

$i=1$ $r_1 = g(x)$ $s_1 = 0$, $t_1 = 1$.

$i=2$ $r_2 = f(x) - \underbrace{(x-2)}_{q_1} g(x)$, $s_2 = 1$, $t_2 = -x+2$.

$= x-1$.

$$\begin{array}{r} 1\quad -2 \\ \hline 1\ 1\ 0 \;)\; 1\quad -1\quad -1\quad -1 \\ \quad 1\quad 1\quad 0 \\ \hline \quad -2\quad -1\quad -1 \\ \quad -2\quad -2\quad 0 \\ \hline \qquad 1\quad -1 \end{array}$$

$i=3$ $r_3 = g(x) - \underbrace{(x+2)}_{q_2} \cdot r_2$, $s_3 = 0 - (x+2)$

$= 2$. $= -x-2$.

$t_3 = 1 - (x+2)(-x+2)$

$= 1 + (x^2-4)$

$= x^2 - 3$

$$\begin{array}{r} 1\quad 2 \\ \hline 1\ -1 \;)\; 1\quad 1\quad 0 \\ \quad 1\quad -1 \\ \hline \quad 2\quad 0 \\ \quad 2\quad -2 \\ \hline \qquad 2 \end{array}$$

中辺 $(-x-2) f(x) + (x^2-3) g(x) = 2$

両辺を2で割って $\frac{-x-2}{2} f(x) + \frac{x^2-3}{2} g(x) = 1$.

$\therefore \frac{\alpha^2-3}{2} g(\alpha) \equiv 1 \pmod{f(\alpha)}$.

$\therefore \frac{1}{g(\alpha)} = \frac{\alpha^2-3}{2} \in \mathbb{Q}[\alpha] / \langle f(\alpha) \rangle$.

(検算) $(\alpha^2-3)(\alpha^2+\alpha) = \alpha^4 + \alpha^3 - 3\alpha^2 - 3\alpha$

$\alpha^4+\alpha^3-3\alpha^2-3\alpha \div f(\alpha) \longrightarrow (\alpha+2,\ 2)$.

$$\begin{array}{r} 1\quad 2 \\ \hline 1\ -1\ -1\ -1 \;)\; 1\quad 1\quad -3\quad -3\quad 0 \\ \quad 1\quad -1\quad -1\quad -1 \\ \hline \quad 2\quad -2\quad -2 \\ \quad 2\quad -2\quad -2\quad -2 \\ \hline \qquad 2 \end{array}$$