

⑧ 法逆元計算 (Computing modular inverse) (§ 4.7, p. 59)

R : 可換環, ICR : イデアル.

R/I : 剰余環.

$a \in R/I$ が単元 (def 乗法の逆元をもつ) とき, その逆元を計算する こと.

(I を法とする a の逆元: 「法逆元」)

すなわち, 242 EEA が有効である.

Thm. 450

(R, d) : Euclid 整環.

$a, m \in R$

ならば,

$$\underbrace{a \bmod m}_{\in \{a + bm \mid b \in R\}} \in R/mR \text{ の単元} \Leftrightarrow \gcd(a, m) = 1.$$

さらに, この時, EEA を用いて R/mR における $a \bmod m$ の逆元 b を計算可能.
(s.t. $a \cdot b \equiv 1 \pmod{m}$)

Proof ($\Rightarrow$) $a \bmod m$ が R/mR の単元

$$\Leftrightarrow \exists s \in R \text{ s.t. } s \cdot a \equiv 1 \pmod{m}$$

$$\Leftrightarrow \exists -t \in R \text{ s.t. } s \cdot a - 1 = -t \cdot m$$

$$\Leftrightarrow s \cdot a + t \cdot m = 1$$

$$\Rightarrow \gcd(a, m) = 1.$$

$$(\Leftarrow) \gcd(a, m) = 1$$

$$\Rightarrow \text{EEA より } \exists s, t \in R \text{ s.t. } sa + tm = 1.$$

$$\Leftrightarrow sa = 1 - tm$$

$$\Leftrightarrow sa \equiv 1 \pmod{m}$$

$$\Leftrightarrow s \text{ は } a \text{ の } R/mR \text{ における乗法の逆元.}$$

$$(s \bmod m) (a \bmod m)$$



$$\langle r, s, t \rangle \leftarrow \text{EEA}(a, m) \quad \text{11.3.1.1.7}$$

$$\begin{cases} r = 1 \Rightarrow & s \bmod m \text{ が } \mathbb{R}/m\mathbb{R} \text{ における } a \bmod m \text{ の逆元.} \\ r \neq 1 \Rightarrow & a \bmod m \text{ が } \mathbb{R}/m\mathbb{R} \text{ における単位元でない. 逆元が存在しない.} \end{cases}$$

例 4.51

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

$$\langle r, s, t \rangle \leftarrow \text{EEA}(29, 12) \quad \text{を計算.}$$

$$i=0: \quad r_0 = 29, \quad s_0 = 1, \quad t_0 = 0.$$

$$i=1: \quad r_1 = 12, \quad s_1 = 0, \quad t_1 = 1.$$

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

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

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

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

$$\text{よって } \underline{i=4} \text{ となる.} \quad 1 = \underbrace{5 \cdot 29}_{\equiv 1 \pmod{m}} + \underbrace{(-12) \cdot 12}_{\equiv 1 \pmod{a}} = 1.$$

$$\therefore \underbrace{(-12)a}_{\equiv 1 \pmod{m}} \equiv 1 \pmod{29}.$$

$$\text{すなわち } 17 \bmod 29$$

すなわち 17 が 29 における 12 の逆元.



問題 4.53

 $\mathbb{Q}[x]$

方程式 $f(x) = x^3 - x^2 - x - 1 = 0$ の根の 1 つ $\rightarrow \alpha$.

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

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

このとき、 $\alpha^2 + \alpha$ の逆元を $A\alpha^2 + B\alpha + C\alpha$ の形で求めよ.

$$\mathbb{Q}[x] / \langle f(x) \rangle \quad \text{ここで } g(x) = x^2 + x \in \mathbb{Q}[x] / \langle f(x) \rangle$$

の逆元 ($x^2 + x$ の $f(x)$ と法とる逆元) を EEA で求めよ.

$$i=0: r_0 = f(x),$$

$$s_0 = 1, \quad t_0 = 0$$

$$i=1: r_1 = g(x)$$

$$s_1 = 0, \quad t_1 = 1$$

$$i=2: r_2 = f(x) - (x-2)g(x) = x-1.$$

$$s_2 = 1, \quad t_2 = -x+2.$$

$$\begin{array}{r|rrrr} & 1 & -2 & & \\ \hline 1 & 1 & 0 & 1 & -1 & -1 & -1 \\ & 1 & & & 0 & & \\ \hline & & -2 & -1 & -1 & & \\ & & -2 & -2 & 0 & & \\ \hline & & & 1 & -1 & & \end{array}$$

$$i=3: r_3 = g(x) - (x+2)(x-1) = 2.$$

$$s_3 = 0 - (x+2) = -x-2.$$

$$\begin{array}{r|rrrr} & 1 & 2 & & \\ \hline 1 & 1 & 0 & 1 & -1 & 0 \\ & 1 & -1 & & & \\ \hline & & 2 & 0 & & \\ & & 2 & -2 & & \\ \hline & & & 2 & & \end{array}$$

$$\begin{aligned} t_3 &= 1 - (x+2)(-x+2) \\ &= 1 + (x^2 - 4) \\ &= x^2 - 3 \end{aligned}$$

$$\text{ゆえに } (-x-2)f(x) + (x^2-3)g(x) = 2.$$

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

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

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