14. 有限体と初等整数論

p : 素数、$\boldsymbol{F}_p = \boldsymbol{Z}/p\boldsymbol{Z}$、しばしば $a \in \boldsymbol{Z}$ と $\overline{a} = a \bmod p \in \boldsymbol{F}_p$ とを区別せずに表記する。

14–1. **逆元の計算.** $a \in \boldsymbol{F}_p^\times$ $(p \nmid a)$ に対し、その逆元 $x \in \boldsymbol{F}_p^\times$ は、$ax + py = 1$ の解として、**Euclid の互除法拡張版 (Extended Euclidean Algorithm)** で求められる。

14–2. **乗法群・原始根と Fermat の小定理.**

- 有限体 $\boldsymbol{F}_p$ の乗法群 $\boldsymbol{F}_p^\times$ は位数 $(p-1)$ の巡回群
- $\boldsymbol{F}_p^\times$ の生成元 (の代表元) を**原始根**と呼ぶ。言い替えると、$a \in \boldsymbol{Z}$ に対し、
  $a : p$ **を法とする (法 p に関する) 原始根 (primitive root modulo p)**
  $\overset{\leftarrow}{\iff} 0 < \forall k < p-1 : a^k \not\equiv 1 \pmod p \iff \langle a \bmod p \rangle = \boldsymbol{F}_p^\times$
- $(a,p) = 1$ のとき、$a^{p-1} \equiv 1 \pmod p$ (**Fermat の小定理**)
- より一般に $(a,n) = 1$ のとき、$a^{\varphi(n)} \equiv 1 \pmod n$ (**Fermat-Euler の定理**)

14–3. **平方剰余.** $p \nmid a$ $(a \in \boldsymbol{F}_p^\times)$ に対し、

- a が p を法とする (法 p に関する) **平方剰余 (quadratic residue)**
  $\overset{\leftarrow}{\iff} \exists x \in \boldsymbol{Z} : x^2 \equiv a \pmod p \iff a \in \boldsymbol{F}_p^{\times 2}$
- a が p を法とする (法 p に関する) **平方非剰余 (quadratic non-residue)**
  $\overset{\leftarrow}{\iff} \nexists x \in \boldsymbol{Z} : x^2 \equiv a \pmod p \iff a \notin \boldsymbol{F}_p^{\times 2}$
- $\left(\dfrac{a}{p}\right) := \begin{cases} +1 & (a\text{: mod } p \text{ で平方剰余}) \\ -1 & (a\text{: mod } p \text{ で平方非剰余}) \\ 0 & (p \mid a) \end{cases}$: **平方剰余記号・Legendre 記号**
- $\left(\dfrac{\cdot}{p}\right) : \boldsymbol{F}_p^\times = (\boldsymbol{Z}/p\boldsymbol{Z})^\times \longrightarrow \{\pm 1\}$: 全射群準同型
- $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ (Euler の規準)

14–4. **平方剰余の相互律.** p, l: 奇素数 $(p \neq l)$ に対し、

- $\left(\dfrac{l}{p}\right)\left(\dfrac{p}{l}\right) = (-1)^{\frac{p-1}{2}\frac{l-1}{2}}$: **平方剰余の相互律 (quadratic reciprocity law)**
- **平方剰余の第 1 補充法則**: $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & (p \equiv 1 \mod 4) \\ -1 & (p \equiv 3 \mod 4) \end{cases}$
- **平方剰余の第 2 補充法則** $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & (p \equiv \pm 1 \mod 8) \\ -1 & (p \equiv \pm 5 \mod 8) \end{cases}$

15. 演習 (5)

問 15–1. 色々な素数に対し、原始根を求めてみよ。

問 15–2. Fermat の小定理 $a^p \equiv a \pmod p$ の、Fermat による原証明は、次のようなものだったと言われている: 二項係数の性質から $(a+b)^p \equiv a^p + b^p \pmod p$ を導き、a に関する帰納法を用いる。この証明を完成せよ。

問 15–3. p を奇素数、ζ_p を 1 の原始 p 乗根 (1 つ取って固定) とする。$G(p) := \displaystyle\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a$ を **Gauß 和 (Gaussian sum)** と言う。

(1) $(k,p) = 1$ のとき、$\displaystyle\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) (\zeta_p^k)^a = \left(\frac{k}{p}\right) G(p)$

(2) $G(p)^2 = \left(\dfrac{-1}{p}\right) p \ (=: p^*)$

(3) l : 奇素数に対し、平方剰余の相互律 $\left(\dfrac{l}{p}\right) = \left(\dfrac{p^*}{l}\right)$ を示せ。

(4) $\zeta_p = \exp(\dfrac{2\pi i}{p}) \in \boldsymbol{C}$ に取るとき、$G(p)$ の符号 (偏角) を決定せよ。