

楕円曲線の合同と類数の合同について

大阪大理 山本芳彦 (Yoshihiko Yamamoto)

0. 序 判別式 D をもつ 2 次体 $\mathbb{Q}(\sqrt{D})$ のイデアル類群を $H(D)$, 類数を $h(D)$ とかく. p, f は素数で,

$p \equiv 3 \pmod{4}$, $f \equiv 1 \pmod{4}$ をみたすものとする.

Gauss の genus theory により, $2 \mid h(-pf)$ かつ $H(-pf)$ の 2-Sylow 群は巡回群である. さらに, 次のことが知られている:

$$(1) \quad 4 \mid h(-pf) \Leftrightarrow \left(\frac{-p}{f}\right) = 1 \quad (\text{Rédei-Reichardt})$$

$$(2) \quad 8 \mid h(-pf) \Leftrightarrow \left(\frac{-p}{f}\right)_4 = 1 \quad (\text{Buchner, Hasse, Kaplan 他}).$$

いま $I_f = \left(\frac{f-1}{2}\right)!$ とおくと, Wilson の定理より, $I_f^2 \equiv -1 \pmod{f}$, よって I_f は $\mathbb{F}_f = \mathbb{Z}/f\mathbb{Z}$ の元と考えるとき 1 の原始 4 乗根の 1 つである. 一方, 実 2 次体 $\mathbb{Q}(\sqrt{f})$ の基本単数 $\varepsilon_f = (T + U\sqrt{f})/2$ (T, U は正整数) とすると, $T/2$ も $\mathbb{F}_f$ の原始 4 乗根で, 両者の間には次の関係がある:

$$(3) \quad (T/2)^{h(f)} \equiv -I_f \pmod{f} \quad (\text{S. Chowla}).$$

上の関係は $\varepsilon_f^{h(f)} \equiv -I_f \pmod{f}$ ともかける.

Dirichlet の類数公式より次を得る:

定理 1. (Yamamoto)

$$\left(\frac{-p}{f}\right)_4 \equiv (-I_f)^{h^*(-p)h(-pf)/2} \pmod{f}, \text{ 即ち}$$

$$\left(\frac{-p}{f}\right)_4 \equiv \varepsilon_f^{h(f)h^*(-p)h(-pf)/2} \pmod{\sqrt{f}},$$

$$\text{すなわち } \left(\frac{-p}{f}\right)_4 \equiv (-p)^{\frac{f-1}{4}} \pmod{f}, \quad h^*(-p) = \begin{cases} 3 & \text{if } p=3 \\ h(-p) & \text{if } p>3. \end{cases}$$

系 $\left(\frac{-p}{f}\right)_4 \equiv I_f^a \pmod{f}$ のとき ($a=0,1,2,3$),

$$h(-pf) \equiv -2a h^*(-p) \pmod{8}.$$

1. $4|h(-pf)$ のとき. 以後 $4|h(-pf)$ 即ち $\left(\frac{-p}{f}\right)$

$=1$ と仮定する. また簡単のため $p>3$ とする. このとき
虚二次体 $K=\mathbb{Q}(\sqrt{-p})$ において f は完全分解するので,

$$(f) = \mathfrak{q} \overline{\mathfrak{q}} \quad (\mathfrak{q} \text{ は } K \text{ の素イデアル, } \mathfrak{q} \neq \overline{\mathfrak{q}}, N\mathfrak{q} = f)$$

とおく. $\mathfrak{q}^{h(-p)}$ は単位イデアルだから, $\mathfrak{q}^{h(-p)} = (\alpha)$

$$\alpha = (x + y\sqrt{-p})/2 \quad (x, y \in \mathbb{Z}) \text{ とおける. } \alpha \text{ は条件}$$

$$(4) \quad \alpha^3 \equiv 1 \pmod{4}$$

により一意に定まる. このとき, 次の成り立つ:

$$(5) \quad 8|h(-pf) \Leftrightarrow \left(\frac{x}{f}\right) = 1$$

$$(6) \quad 16|h(-pf) \Leftrightarrow \left(\frac{x}{f}\right)_4 = 1 \quad (\text{Yamamoto}).$$

さらに, 定理 1 に対応して

定理 2.

$$\left(\frac{x}{f}\right)_4 \equiv (-I_f)^{h(-pf)/4} \pmod{f}, \text{ 即ち}$$

$$\left(\frac{x}{f}\right)_4 \equiv \varepsilon_f^{h(f)h(-p)/4} \pmod{\sqrt{f}}.$$

系 $\left(\frac{x}{f}\right)_4 \equiv I_f^a \pmod{f}$ かつ $a \equiv 0, 1, 2, 3$,
 $h(-pf) \equiv 4a \pmod{16}$.

以後では定理2の証明の方針を述べる.

2. Kroneckerの極限定理の応用 虚2次体 $K = \mathbb{Q}(\sqrt{f})$

において, 法 $f\mathcal{O}$ ($\mathcal{O}$ は K の整数環) の Hecke 指標で位数が高々2であるものは丁度4つ存在する. それらを χ_i ($i = 0, 1, 2, 3$) とする. $h(-p)$ は奇数だから, χ_1 は $\mathcal{O}/f\mathcal{O}$ の類指標により一意に定まるので, 両者を同一視して,

$$\chi_0(\beta) = 1, \quad \chi_1(\beta) = \left(\frac{\beta}{f}\right), \quad \chi_2(\beta) = \chi_1(\bar{\beta}),$$

$$\chi_3(\beta) = \chi_1(\beta)\chi_2(\beta) \quad (\beta \in \mathcal{O})$$

とする. $H(-p)$ の各イデアル類の完全代表系 $\{\mathfrak{o}_i\}$ として

$\mathfrak{o}_i$ は $2f\mathcal{O}$ と素な整イデアルとなるものをとり, その

$\mathbb{Z}$ -基底を ω_1, ω_2 ($\text{Im } \omega_2/\omega_1 > 0$) とする. ここで,

$$S_i = \sum_{\mathfrak{o}} \chi_i(\mathfrak{o}) \sum_{\lambda \in \mathfrak{o}/f\mathfrak{o}} \chi_i(\lambda) \log \left| F\left(\frac{\lambda}{f\omega_1}, \frac{\omega_2}{\omega_1}\right) \right|^2$$

とおく ($i = 0, 1, 2, 3$). 上で, $F(w, z)$ は Siegel 関数

で, 次により与えられる: ($w \in \mathbb{C}$, $z \in \mathfrak{h}_2$ (上半平面))

$$F(w, z) = \exp\left[\pi i w \left(\frac{w - \bar{w}}{z - \bar{z}}\right)\right] \frac{i \vartheta_1(w, z)}{\eta(z)},$$

$$\vartheta_1(w, z) = -i e^{\pi i z/4} (e^{\pi i w} - e^{-\pi i w}) \times \\ \times \prod_{n=1}^{\infty} (1 - e^{2\pi i n z + 2\pi i w}) (1 - e^{2\pi i n z - 2\pi i w}) (1 - e^{2\pi i n z})$$

$$\eta(z) = e^{\pi i z/12} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z}) \quad (\text{Dedekind の } \eta).$$

$F(w, z)$ の変換公式より, S_i は (i) $\sigma/g\sigma$ の代表系 $\{\sigma\}$,
(ii) σ の base w_1, w_2 (iii) $H(-p)$ の素類の代表系 $\{\sigma\}$, の
選ぶ方によらないことがわかる. Kronecker の無限公式より.

Prop. 1 $S_0 = 0,$

$$S_1 = -2(1 - \chi_1(\bar{q})) L'(0, \chi_1, k),$$

$$S_2 = -2(1 - \chi_2(\bar{q})) L'(0, \chi_2, k) = S_1,$$

$$S_3 = -2 L'(0, \chi_3, k) = -2h(-p) h(g) \log \varepsilon_g.$$

これと

$$S_0 - S_1 + S_2 - S_3 = 4 \sum_{\sigma} \sum_{\substack{\chi_1(\lambda\sigma) = -1 \\ \chi_2(\lambda\sigma) = 1}} \log \left| F\left(\frac{\lambda}{g\omega_1}, \frac{\omega_2}{\omega_1}\right) \right|^2 \quad \text{より,}$$

Prop. 2

$$\prod_{\sigma} \prod_{\substack{\lambda: \chi_1(\lambda\sigma) = -1 \\ \chi_2(\lambda\sigma) = 1}} \left| F\left(\frac{\lambda}{g\omega_1}, \frac{\omega_2}{\omega_1}\right) \right| = \varepsilon_g^{h(g)h(-p)/4}.$$

3. 虚数乗法論の応用, 単数の合同式 $J(\sigma) = j(\omega/\omega_1)$

と構作 modular 関数, $\tau(w, \sigma) \in \text{Weber の } \tau\text{-関数}$ とす

るとす:

Prop. 3 (Ramachandra) $\lambda \in \mathcal{O}$, $\lambda \notin 2\mathcal{O}$, $\lambda \notin g\mathcal{O}$ のとき,

$$F\left(\frac{\lambda}{g\omega_1}, \frac{\omega_2}{\omega_1}\right)^{3g} = R\left(\tau\left(\frac{\lambda}{g}, \mathcal{O}\right), J(\mathcal{O})\right) \quad (R \text{ は } \lambda \text{ に } g$$

らなる $\mathbb{Q}$ -係数の 2 変数有理関数).

虚数乗法論より, $F\left(\frac{\lambda}{g\omega_1}, \frac{\omega_2}{\omega_1}\right)$ は k の法 π に関する ray class field $k^{(qg)}$ の整数である. 一方, τ は本體域に ρ -関数であることより, 加法公式から

Prop. 4 $\mathcal{Q} \in \mathcal{O}$ の上にある $k^{(qg)}$ の素イデアルとする. $\lambda, \lambda' \in \mathcal{O} - 2\mathcal{O} - g\mathcal{O}$ かつ $\lambda \equiv \lambda' \pmod{\pi \mathcal{Q}}$ ならば

$$F\left(\frac{\lambda}{g\omega_1}, \frac{\omega_2}{\omega_1}\right)^{3g} \equiv F\left(\frac{\lambda'}{g\omega_1}, \frac{\omega_2}{\omega_1}\right)^{3g} \pmod{\mathcal{Q}}.$$

4. 定理 2 の証明

Lem. 1 $\mathcal{O}$ の基底 ω_1, ω_2 と $\mathcal{O}$ の (i) (ii) を満たすものがとれる: $((\mathcal{O}, g) = 1, \omega_2/\omega_1 \in k_g)$

$$(i) \quad g\mathcal{O} = [\omega_1, g\omega_2], \quad \overline{g}\mathcal{O} = [g\omega_1, \omega_2]$$

$$(ii) \quad \omega_1 \in \mathcal{O}^{h(p)} = (\alpha), \quad \omega_2 \in \overline{\mathcal{O}}^{h(p)} = (\overline{\alpha}).$$

以後, $\mathcal{O}$ の base ω_1, ω_2 は Lem. 1. (i) (ii) を満たすとする.

$\mathcal{O}/g\mathcal{O}$ の代表系として, $\{\lambda = (g+qa)\omega_1 + (g+qb)\omega_2 \mid 0 \leq a, b \leq g-1, a, b \in \mathbb{Z}\}$ をとり,

$$P_{\mathcal{O}} = \prod_{\substack{\lambda \in \mathcal{O}/g\mathcal{O} \\ \chi_1(\lambda\mathcal{O}) = -1 \\ \chi_2(\lambda\mathcal{O}) = 1}} \left| F\left(\frac{\lambda}{g\omega_1}, \frac{\omega_2}{\omega_1}\right) \right|$$

とすると, $P_{\mathcal{O}}$ は $k^{(qg)}$ の整数である. Prop. 4 より

$$F\left(\frac{\lambda}{f\omega_1}, \frac{\omega_2}{\omega_1}\right)^{3f} \equiv F\left(\frac{f+4g}{f}, \frac{\omega_2}{\omega_1}\right)^{3f} \pmod{Q}.$$

ここで、左辺は $k^{(4f)}$ の単数であるが、右辺は $k^{(4f)}$ の整数で $\overline{q}$ 上のある素イデアルで割られる。

Prop. 5

$$P_\alpha P_{\overline{\alpha}} \equiv \rho \prod_{a=1}^{f-1} F\left(\frac{4a}{f}, \frac{\omega_2}{\omega_1}\right)^{\frac{f-1}{4}} \prod_{b=1}^{f-1} F\left(\frac{4b}{f}, \frac{\overline{\omega_1}}{\omega_2}\right)^{\frac{f-1}{4}} \pmod{Q}$$

($\rho \in \mathbb{C}$, $\rho^{3f} = 1$).

また、 $F(w, z)$ の定義より

$$\text{Lem 2} \quad \prod_{a=1}^{f-1} F\left(\frac{4a}{f}, \frac{\omega_2}{\omega_1}\right) = f \cdot \frac{f^2 \left(\frac{f\omega_2}{\omega_1}\right)}{f^2 \left(\frac{\omega_2}{\omega_1}\right)}.$$

イデアル類群 $H(-p)$ において、 q の属する類の位数 e とすると、 $q^e = (\alpha_0)$, $\alpha_0^3 \equiv 1 \pmod{4}$ ($\alpha_0 \in \mathcal{O}$) とかける。 $\alpha_0^{\frac{f}{e}} = \alpha$ である。 $q^e = [w_1, f^e w_2] = (\alpha_0)$ より次を得る。

Lem 3. (単項化定理)

$$f^e \cdot \frac{f^2 \left(\frac{f^e \omega_2}{\omega_1}\right)}{f^2 \left(\frac{\omega_2}{\omega_1}\right)} = \mu \overline{\alpha_0} \quad (\mu^3 = 1).$$

$H(-p)$ において、 q -orbit 毎に P_α の積を計算するとにより:

$$\text{Prop. 6} \quad \prod_{\alpha} P_\alpha \equiv \rho' \overline{\alpha}^{\frac{f-1}{2}} \pmod{Q} \quad (\rho'^{3f} = 1).$$

Prop. 2 と Prop. 6 より

$$\rho' \bar{\alpha}^{\frac{p-1}{4}} \equiv \varepsilon_f^{h(f)h(-p\delta)/4} \pmod{Q}.$$

$\equiv 1$,

$$\bar{\alpha}^{\frac{p-1}{4}} = \left(\frac{\bar{\alpha}}{f}\right)_4 \equiv \left(\frac{x}{f}\right)_4 \pmod{Q}$$

$$\text{したがって, } \left(\frac{x}{f}\right)_4 = \varepsilon_f^4 \equiv 1 \pmod{Q} \text{ より } \rho' = 1 \text{ となる}$$

り, 定理 2 を得る.