数理解析研究所講究録
第658巻 1988年 1-7

楕円単数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, q は素数で, $p \equiv 3 \pmod 4$, $q \equiv 1 \pmod 4$ をみたすものとする. Gauss の genus theory により, $2 \mid h(-pq)$ かつ $H(-pq)$ の 2-Sylow 群は巡回群である. さらに, 次が知られている:

(1) $4 \mid h(-pq) \Leftrightarrow \left(\frac{-p}{q}\right) = 1$ (Rédei - Reichardt)

(2) $8 \mid h(-pq) \Leftrightarrow \left(\frac{-p}{q}\right)_4 = 1$ (Bucher, Hasse, Kaplan etc).

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

(3) $(T/2)^{h(q)} \equiv -I_q \pmod q$ (S. Chowla).

上の関係は $\varepsilon_q^{h(q)} \equiv -I_q \pmod{\sqrt{q}}$ ともかける.

Dirichlet の類数公式より次を得る:

定理1. (Yamamoto)

$$\left(\frac{-p}{q}\right)_4 \equiv (-I_q)^{h^*(-p)h(-pq)/2} \pmod{q}, \text{ 即ち}$$

$$\left(\frac{-p}{q}\right)_4 \equiv \varepsilon_q^{h(q)h^*(-p)h(-pq)/2} \pmod{\sqrt{q}},$$

ここで $\left(\frac{-p}{q}\right)^4 \equiv (-p)^{\frac{q-1}{4}} \pmod{q}$, $h^*(-p) = \begin{cases} 3 & \text{if } p=3 \\ h(-p) & \text{if } p>3. \end{cases}$

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

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

1. $4 \mid h(-pq)$ のとき. 以後 $4 \mid h(-pq)$ 即ち $\left(\frac{-p}{q}\right) = 1$ と仮定する. また簡単のため $p>3$ とする. このとき虚2次体 $k = \mathbb{Q}(\sqrt{-p})$ において q は完全分解するので,

$(q) = \mathfrak{q}\overline{\mathfrak{q}}$ ($\mathfrak{q}$ は k の素イデアル, $\mathfrak{q} \neq \overline{\mathfrak{q}}$, $N\mathfrak{q} = q$)

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

$\alpha = (x+y\sqrt{-p})/2$ $(x, y \in \mathbb{Z})$ とかける. α は条件

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

により一意的に定まる. このとき, 次が成り立つ:

(5) $8 \mid h(-pq) \Leftrightarrow \left(\frac{x}{q}\right) = 1$

(6) $16 \mid h(-pq) \Leftrightarrow \left(\frac{x}{q}\right)_4 = 1$ (Yamamoto).

さらに, 定理1に対応して

定理2.

$$\left(\frac{x}{q}\right)_4 \equiv (-I_q)^{h(-pq)/4} \pmod{q}, \text{ 即ち}$$

$$\left(\frac{2}{f}\right)_4 \equiv \varepsilon_f^{h(f)h(-pf)/4} \pmod{\sqrt{f}}.$$

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

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　虚二次体 $k=\mathbb{Q}(\sqrt{-p})$ 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_i 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,

$$\chi_0(\beta)=1,\quad \chi_1(\beta)=\left(\frac{\beta}{f}\right),\quad \chi_2(\beta)=\chi_1(\bar{\beta}),$$
$$\chi_3(\beta)=\chi_1(\beta)\chi_2(\beta) \qquad (\beta\in\mathcal{O})$$

とする. $H(-p)$ の各イデアル類の完全代表系 $\{\mathfrak{a}\}$ として $\mathfrak{a}$ 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 ($\mathrm{Im}\,\omega_2/\omega_1>0$) とする. ここで,

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

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: ($w\in\mathbb{C}$, $z\in\mathfrak{h}$ (上半平面))

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

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

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

$F(w,z)$ の変換公式より，S_i は (i) $\mathfrak{o}/g\mathfrak{o}$ の代表系以上，(ii) $\mathfrak{o}$ の base ω_1,ω_2 (iii) $H(-p)$ の各類の代表系 $\{\mathfrak{o}\}$，の選び方によらないことがわかる．Kronecker の極限公式より．

<u>Prop. 1</u>　$S_0=0$,

$$S_1=-2(1-\chi_1(\bar{q}))L'(0,\chi_1,k),$$
$$S_2=-2(1-\chi_2(q))L'(0,\chi_2,k)=S_1,$$
$$S_3=-2L'(0,\chi_3,k)=-2h(-pq)h(q)\log\varepsilon_q.$$

これと

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

<u>Prop. 2</u>

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

3. 虚数乗法論の応用，単数の合同式　$J(\mathfrak{o})=j(\omega_2/\omega_1)$ を構成 modular 関数，$\tau(w,\mathfrak{o})$ を Weber の τ-関数とすると：

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

$$F\left(\frac{\lambda}{g\omega_1}, \frac{\omega_2}{\omega_1}\right)^{24} = R\left(\tau\left(\frac{\lambda}{g}, \mathfrak{o}\right), J(\mathfrak{o})\right)$$ (R は λ によらない $\mathbb{Q}$-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 $\mathfrak{g}$ に関する ray class field $k^{(\mathfrak{g})}$ の整数である. 一方, τ は本質的に p-関数であることより, 加法公式から

Prop. 4 $\mathfrak{Q}$ を $\mathfrak{q}$ の上にある $k^{(\mathfrak{g})}$ の素イデアルとする. $\lambda, \lambda' \in \mathfrak{o} - 2\mathfrak{o} - g\mathfrak{o}$ かつ $\lambda \equiv \lambda' \pmod{\mathfrak{q}\bar{\mathfrak{q}}}$ なら

$$F\left(\frac{\lambda}{g\omega_1}, \frac{\omega_2}{\omega_1}\right)^{24} \equiv F\left(\frac{\lambda'}{g\omega_1}, \frac{\omega_2}{\omega_1}\right)^{24} \pmod{\mathfrak{Q}}.$$

4. 定理2の証明

Lem. 1 $\mathfrak{o}$ の基底 ω_1, ω_2 として次の (i) (ii) をみたすものがとれる: ($(\mathfrak{o}, 2g) = 1$, $\omega_2/\omega_1 \in \mathfrak{h}$)

(i) $\mathfrak{q}\mathfrak{o} = [\omega_1, g\omega_2]$, $\bar{\mathfrak{q}}\mathfrak{o} = [g\omega_1, \omega_2]$

(ii) $\omega_1 \in \mathfrak{q}^{h(-p)} = (\alpha)$, $\omega_2 \in \bar{\mathfrak{q}}^{h(-p)} = (\bar{\alpha})$.

以後, $\mathfrak{o}$ の base ω_1, ω_2 は Lem 1. (i)(ii) をみたすとする. $\mathfrak{o}/g\mathfrak{o}$ の代表系として, $\{\lambda = (g+\alpha a)\omega_1 + (g+\alpha b)\omega_2 \mid 0 \leq a, b \leq g-1, a, b \in \mathbb{Z}\}$ をとり,

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

とおくと, $P_{\mathfrak{o}}$ は $k^{(\mathfrak{g})}$ の整数である. Prop. 4 より

$$F\left(\frac{\wedge}{f\omega_1}, \frac{\omega_2}{\omega_1}\right)^{3f} \equiv F\left(\frac{\beta+q\alpha}{f}, \frac{\omega_2}{\omega_1}\right)^{3f} \pmod{\Omega}.$$

ここで，左辺は $k^{(4f)}$ の単数であるが，右辺は $k^{(4f)}$ の整数で $\mathfrak{q}$ 上のある素イデアルで割れる．

Prop. 5

$$P_\sigma P_{\bar\sigma} \equiv \rho \prod_{a=1}^{f-1} F\left(\frac{qa}{f}, \frac{\omega_2}{\omega_1}\right)^{\frac{f-1}{4}} \prod_{b=1}^{f-1} F\left(\frac{qb}{f}, \frac{\bar\omega_1}{\bar\omega_2}\right)^{\frac{f-1}{4}} \pmod{\Omega}$$

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

また，$F(w,z)$ の定義より

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

イデアル類群 $H(-p)$ において，$\mathfrak{q}$ の属する類の位数を e とすると，$\mathfrak{q}^e = (\alpha_0)$，$\alpha_0^3 \equiv 1 \pmod 4$ $(\alpha_0 \in \mathcal{O})$ とかける．$\alpha_0^{h/e} = \alpha$ である．$\mathfrak{q}^e = [\omega_1, f^e\omega_2] = (\alpha_0)$ より次を得る．

Lem 3. (単項化定理)

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

$H(-p)$ において，$\mathfrak{q}$-orbit 毎に P_σ の積を計算することにより：

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

Prop. 2 と Prop. 6 より

$$\rho' \overline{\alpha}^{\frac{q-1}{4}} \equiv \varepsilon_q^{h(q)h(-pq)/4} \pmod{\mathfrak{Q}}.$$

ここで,

$$\overline{\alpha}^{\frac{q-1}{4}} \equiv \left(\frac{\overline{\alpha}}{\sigma_q}\right)_4 \equiv \left(\frac{\chi}{q}\right)_4 \pmod{\mathfrak{Q}}$$

であり, $\left(\frac{\chi}{q}\right)_4^4 = \varepsilon_q^4 \equiv 1 \pmod{\mathfrak{Q}}$ より $\rho' = 1$ となり, 定理2を得る.