数理解析研究所講究録
第 603 巻 1987 年 43-50

Congruence relations between class numbers of quadratic fields

山本芳彦 (阪大 理)
Yoshihiko YAMAMOTO (Osaka University)

0. Introduction.

Let $K = \mathbf{Q}(\sqrt{D})$ be the quadratic field with discriminant $D = D_K$. We denote by $C_K = C(D)$ and $h_K = h(D)$ the ideal class group of K and its class number respectively. We also denote by $\varepsilon_D > 1$ the fundamental unit of K when $D > 0$ and by $w(D)$ the number of roots of unity contained in K. Put $\zeta_n = e^{2\pi i/n}$ for a positive integer n.

Assume $D = -pq$, where p and q are prime numbers such that $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$, so that $2 \mid h(D)$ and the 2-part (i.e. the 2-Sylow subgroup) of C_K is cyclic. Then we have

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

$$8 \mid h(-pq) \iff \left(\frac{-p}{q}\right)_4 = 1 \qquad \text{(Bucher, Kaplan)}.$$

Hence we have

$$4 \parallel h(-pq) \iff \left(\frac{-p}{q}\right)_4 = -1 \quad \text{and}$$

$$2 \parallel h(-pq) \iff \left(\frac{-p}{q}\right) = -1 \iff \left(\frac{-p}{q}\right)_4 = \pm i,$$

where $\pm$ depends on the defnition of the biquadratic residue symbol $\left(\frac{\ }{q}\right)_4$.

One might ask the naive question: Is it possible to have

$$\left(\frac{-p}{q}\right)_4 = i^{h(-pq)/2}$$

by a suitable definition of $\left(\frac{\ }{q}\right)_4$?

In fact we have

<u>THEOREM 1.</u> Let p and q be primes such that $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$. Then we have

$$\text{(1-1)} \qquad \left(\frac{-p}{q}\right)_4 \equiv (-I_q)^{h^*(-p)h(-pq)/2} \pmod q,$$

where $\left(\frac{-p}{q}\right)_4 \equiv (-p)^{(q-1)/4} \pmod q$, $I_q \equiv [\frac{q-1}{2}]! \pmod q$ $h^*(-p) = h(-p)$ if $p > 3$ and $h^*(-3) = 3$.

Since $I_q^2 \equiv -1 \pmod q$, we see that theorem 1 determines the congruence class $h(-pq)$ modulo 8. Congrence relation (1-1) can be rewritten into

$$\text{(1-1')} \qquad \left(\frac{-p}{q}\right)_4 \equiv \varepsilon_q^{h^*(-p)h(q)h(-pq)/2} \pmod q$$

by Chowla's formula

$$\text{(1-2)} \qquad I_q \equiv \varepsilon_q^{-h(q)} \pmod q,$$

where we understand that $\varepsilon_q \equiv \frac{T}{2} \pmod q$ if $\varepsilon_q = \frac{T + Q\sqrt{q}}{2}$.

Now we further assume $\left(\frac{-p}{q}\right) = 1$, hence $4 \mid h(-pq)$ and q splits in $A = \mathbf{Q}(\sqrt{-p})$: $(q) = \mathfrak{q}_A \bar{\mathfrak{q}}_A$. Put $\mathfrak{q}_A^{h(-p)} = (\alpha)$, $\alpha = \frac{x + y\sqrt{-p}}{2} \in O_A$, the integer ring of A ($x, y \in \mathbf{Z}$). α is uniquely determined by the condition

$$\alpha^3 \equiv 1 \pmod{4\, O_A} \qquad \text{(cf. [2]).}$$

Then we have

$$8 \mid h(-pq) \iff \left(\frac{x}{q}\right) = 1 \quad \text{and}$$

$$16 \mid h(-pq) \iff \left(\frac{x}{q}\right)_4 = 1 \quad \text{(cf.[2], th. 5.6).}$$

Hence

$$8 \parallel h(-pq) \iff \left(\frac{x}{q}\right)_4 = -1 \quad \text{and}$$

$$4 \parallel h(-pq) \iff \left(\frac{x}{q}\right)_4 = \pm i \,.$$

Again we can ask whether $\left(\frac{x}{q}\right)_4$ determines the class $h(-pq)$ modulo 16. Numerical experiments lead us to the following

CONJECTURE. Let p and q be primes such that $p \equiv 3 \pmod 4$, $q \equiv 1 \pmod 4$ and $\left(\frac{-p}{q}\right) = 1$. Then it holds

$$\text{(1-3)} \qquad \left(\frac{x}{q}\right)_4 \equiv (-I_q)^{h(-pq)/4} \pmod q$$

or equivalently

$$\text{(1-3')} \qquad \left(\frac{x}{q}\right)_4 \equiv \varepsilon_q^{\,h(q)h(-pq)/4} \pmod q.$$

We have

THEOREM 2. If $h(-p) = 1$ and $p \neq 3$ then above conjecture is true.

1. Proof of theorem 1.

It is easy to see (1-1) when $\left(\frac{-p}{q}\right) = 1$. So we assume

$(\frac{-p}{q}) = -1$ in this section. From Dirichlet's class number formu la we have

$$S_1 = \sum{}' \log(1 - \zeta_{pq}{}^a) = 0,$$

$$S_{-p} = \sum{}' (\frac{a}{p})\log(1 - \zeta_{pq}{}^a) = -4\pi i\ h(-p)/w(-p),$$

$$S_q = \sum{}' (\frac{a}{q})\log(1 - \zeta_{pq}{}^a) = -4\ h(q)\log \varepsilon_q,$$

$$S_{-pq} = \sum{}' (\frac{a}{p})(\frac{a}{q})\log(1 - \zeta_{pq}{}^a) = -\pi i\ h(-pq),$$

where the summations are taken on a's such that $0 < a < pq$ and $(a, pq) = 1$. Add S_1, S_{-p}, S_q and S_{-pq}, and we have

$$(1\text{-}4) \qquad 4 \sum{}'' \log(1 - \zeta_{pq}{}^a) = -4\pi i\ h(-p)/w(-p) - 4\ h(q)\log \varepsilon_q - \pi i\ h(-pq),$$

the summation being taken on a's such that $0 < a < pq$ and $(\frac{a}{p}) = (\frac{a}{q}) = 1$. Taking expnentials,

$$(1\text{-}5) \qquad \prod{}'' (1 - \zeta_{pq}{}^a) = (-i)^{h^*(-p)+h(-pq)/2}\ \varepsilon_q{}^{-h(q)},$$

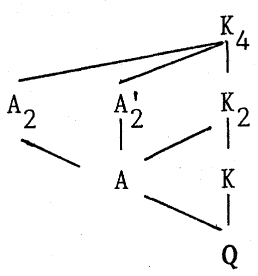
the product being taken on the same range of a's as in $\sum''$. Let $\underline{Q}$ be a prime ideal in $\mathbf{Q}(\zeta_{pq})$ such that $\underline{Q} \mid q$ and $i \equiv -I_q \pmod{\underline{Q}}$. Since $\zeta_q \equiv 1 \pmod{\underline{Q}}$, it follows from (1-2) that

$$I_q{}^{-h^*(-p)+1-h(-pq)/2} \equiv \prod_{0<y<p,\ (\frac{y}{p})=-1} (1 - \zeta_p{}^y) \equiv (-p)^{(q-1)/4} \pmod{\underline{Q}}.$$

This imples the theorem.

2. Proof of theorem 2.

In case $8 \mid h(-pq)$ theorem 2 being reduced to the known results, we may assume $4 \,\|\, h(-pq)$. There exists unique unramified cyclic extension K_4/K of degree 4. K_4 is normal over $\mathbf{Q}$ and $\mathrm{Gal}(K_4/\mathbf{Q})$ is isomorphic to D_4, the dihedral group of order 8. We have the following diagram of subfields:



$K_4 = \mathbf{Q}(\sqrt{\alpha})$

$K_2 = \mathbf{Q}(\sqrt{-p}, \sqrt{q})$, $\quad A_2 = A(\sqrt{\alpha})$, $\mathrm{cond}(A_2/A) = \mathfrak{q}$,

$K = \mathbf{Q}(\sqrt{-pq})$ $\quad A_2' = A(\sqrt{\bar{\alpha}})$, $\mathrm{cond}(A_2'/A) = \bar{\mathfrak{q}}$,

$\mathbf{Q}$ $\quad (\ \mathfrak{q} = \mathfrak{q}_A)$.

We see that K_4/A has conductor $(q) = \mathfrak{q}\bar{\mathfrak{q}}$. Let χ_0, χ_1, χ_2 and χ_3 be the Hecke charactor modulo (q) of A corresponding to abelian extensions A, A_2, A_2' and K_4 over A, respectivly:

$$\chi_0(\gamma) = 1, \quad \chi_1(\gamma) = \left(\frac{\gamma}{\mathfrak{q}}\right), \quad \chi_2(\gamma) = \left(\frac{\gamma}{\bar{\mathfrak{q}}}\right) = \left(\frac{\bar{\gamma}}{\mathfrak{q}}\right),$$

and $$\chi_3(\gamma) = \left(\frac{\gamma}{\mathfrak{q}}\right)\left(\frac{\bar{\gamma}}{\mathfrak{q}}\right) = \left(\frac{\gamma\bar{\gamma}}{q}\right).$$

Define $S(\chi_i)$ $(i = 0, 1, 2, 3)$ by

$$(2\text{-}1) \qquad S(\chi_i) = \sum \chi_i(\gamma) \log\left|F\left(\frac{\gamma}{q}, z_0\right)\right|^2 \qquad (\ \gamma \in O_A/(q)\ ),$$

where F is the Siegel function,

$$F(\gamma, z) = \exp\left[\ \pi i \gamma \left(\frac{\gamma - \bar{\gamma}}{z - \bar{z}}\right)\right] \frac{i\,\theta_1(\gamma, z)}{\eta(z)^2},$$

and $$z_0 = \frac{1 + \sqrt{-p}}{2}.$$

From Krocker's limit formula for imaginary quadratic fields, we have

$$S(\chi_0) = 0,$$

$$S(\chi_1) = -2(1 - \chi_1(\overline{\alpha}))\, h_{A_2} \log|U|^2,$$

where h_{A_2} is the class number of A_2 and U is a fundamental unit of A_2 such that $|U| > 1$ and $O_{A_2} = \langle -1, U \rangle$,

$$S(\chi_2) = -2(1 - \chi_2(\alpha))\, h_{A_2'} \log|\overline{U}|^2 = S(\chi_1), \text{ since } A_2' = \overline{A}_2,$$

and $S(\chi_3) = -2\, h(q)\, h(-pq) \log \varepsilon_q$.

Since $\chi_1(\alpha) = \chi_2(\alpha) = (\frac{x}{q}) = -1$, we have

(2-2) $$S(\chi_0) + S(\chi_1) - S(\chi_2) - S(\chi_3)$$

$$= 4 \sum_{\substack{\lambda \in O_A/(q) \\ \chi_1(\lambda)=-1, \chi_2(\lambda)=1}} \log|F(\frac{\lambda}{q}, z_0)|^2 = 2\, h(q)h(-pq)\log \varepsilon_q .$$

Hence we get

<u>PROPOSITION 1</u>. $$\prod_{\chi_1(\lambda)=-1, \chi_2(\lambda)=1} |F(\frac{\lambda}{q}, z_0)|^2 = \varepsilon_q^{h(q)h(-pq)/2}.$$

On the other hand, it follows from Ramachandra [1] that

<u>PROPOSITION 2.</u> Assume $\lambda \in O_A = [1, z_0]$, $\lambda \notin 2\, O_A$, and $\lambda \notin q\, O_A$. Then it holds that

$$F(\frac{\lambda}{q}, z_0)^{3q} = R(\, \tau(\frac{\lambda}{4q}, O_A), \quad j(z_0))$$

for a rational function $R \in \mathbf{Q}[X, Y]$ not depending on λ, where $\tau(w, L)$ is the Weber's τ-function.

Let

$$E: \quad Y^2 = 4X^3 - 12J(J-1728)X - 8J(J-1728)^2$$

be the elliptic curve defined by $(X, Y) = (\tau(w,L), c^{3/2}\wp'(w,L))$, where $L = [1, z_0] = \mathbf{Z} + \mathbf{Z} z_0$, $c = -2^7 3^5 g_2(z_0)g_3(z_0)/\Delta(z_0)$ and $J = 1728\, j(z_0)$. (Note $\tau(w, L) = c\,\wp(w, L)$.) E is defined over A and End(E) is isomorphic to O_A. For an ideal $\mathfrak{a}$ in A we denote by $E(\mathfrak{a})$ the group of $\mathfrak{a}$-torsion points of E. Since E has good ordianly reduction molulo $\mathfrak{q}$, we have the following diagram

$$\begin{array}{lccccccc} & E(4q) & = & E(4) & + & E(\mathfrak{q}) & + & E(\bar{\mathfrak{q}}) \\ \text{red. mod } \mathfrak{q} & \downarrow & & \downarrow \text{inj.} & & \downarrow & & \downarrow \text{inj.} \\ & \tilde{E}(4q) & = & \tilde{E}(4) & + & 0 & + & \tilde{E}(\bar{\mathfrak{q}}). \end{array}$$

Hence we have

PROPOSITION 3. Let $\lambda = q + 4a\alpha + 4b\bar{\alpha}$ and $\lambda' = q + 4a\alpha$ $(a, b \in \mathbf{Z})$. If $a \not\equiv 0 \pmod q$, then λ and λ' satisfy the assumptions in proposition 2 and we have

$$F(\frac{\lambda}{q}, z_0)^{3q} \equiv F(\frac{\lambda'}{q}, z_0)^{3q} \pmod{\underline{Q}},$$

where $\underline{Q}$ is a prime ideal in $A(E(4q))$ such that $\underline{Q} \mid \mathfrak{q}$.

By the transformation formulas of Siegel function we have

PROPOSITION 4.

$$\prod_{\chi_1(\lambda)=-1,\ \chi_2(\lambda)=1} \left| F(\frac{\lambda}{q}, z_0)\right| \equiv \rho \prod_{a=1}^{q-1} F(\frac{4a\alpha}{q}, z_0)^{(q-1)/4} \pmod{\underline{Q}},$$

where ρ is a 3q-th root of 1.

By the product formula of Siegel function and the transformation formula of η-function we get

PROPOSITION 5. Let $\mathfrak{q} = (\alpha) = [q, z_0 - r]$ $(r \in Z)$ be the Z-basis of $\mathfrak{q}$. Then

$$\prod_{a=1}^{q-1} F\left(\frac{4a\alpha}{q}, z_0\right) = \zeta_{12}^{qr}\ \eta\left(\frac{z_0 - r}{q}\right)^2/\eta(z_0)^2 = \bar{\alpha}.$$

Now we get

$$\varepsilon_q^{h(q)h(-pq)/4} = \Pi \left|F\left(\frac{\lambda}{q}, z_0\right)\right| \qquad \text{(Prop. 1)}$$

$$\equiv \rho \left(\frac{\bar{\alpha}}{q}\right)_4 \pmod{\underline{Q}} \qquad \text{(Prop. 4 and Prop. 5).}$$

Since $\varepsilon_q^{\ 4} \equiv \left(\frac{\bar{\alpha}}{q}\right)_4^{\ 4} \equiv 1 \pmod{\underline{Q}}$. we have $\rho = 1$. This implies Theorem 2.

References

[1] Ramachandra, K.: Some applications of Kronecker's limit formulas. Ann. of Math. (2) 80(1964), 104-148.

[2] Yamamoto, Y.: Divisibility by 16 of class number of quadratic fields whose 2-class groups are cyclic. Osaka J. of Math. 21(1984), 1-22.