On Simultaneous Divisibility of the Class Numbers of Imaginary Quadratic Fields

Toru Komatsu

1 Introduction

In this article, we explain some results in the papers [7, 8] on simultaneous divisibility of the class numbers of quadratic fields and present an evolved problem of the inverse Galois problem.

Let k be an algebraic number field with $[k : \mathbb{Q}] < \infty$. Let $Cl(k)$ denote the ideal class group of k, and $h(k)$ the class number of k.

Theorem 1.1 (Komatsu [7] 2002, Acta Arith.) *Let $m \neq 0$ be a rational integer. Then there exist infinitely many real (imaginary) quadratic fields $\mathbb{Q}(\sqrt{D})$ such that $3 \mid h(\mathbb{Q}(\sqrt{D}))$ and $3 \mid h(\mathbb{Q}(\sqrt{mD}))$.*

Theorem 1.2 (Komatsu [8] 2017, IJNT) *Let n and m be rational integers greater than 1. Then, there exist infinitely many imaginary quadratic fields $\mathbb{Q}(\sqrt{D})$ such that $n \mid h(\mathbb{Q}(\sqrt{D}))$ and $n \mid h(\mathbb{Q}(\sqrt{mD}))$.*

2 Old Motivation for the Results

Let $d > 1$ be a squarefree rational integer. Let r denote the 3-rank of $Cl(\mathbb{Q}(\sqrt{d}))$ of the real quadratic field $\mathbb{Q}(\sqrt{d})$, and s that of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3d})$.

Theorem 2.1 (Scholz, reflection theorem) *The inequality $r \leq s \leq r + 1$ holds. For a rational integer $d > 1$, if $3 \mid h(\mathbb{Q}(\sqrt{d}))$, then $3 \mid h(\mathbb{Q}(\sqrt{-3d}))$.*

The conference ICCGNFRT at Harish-Chandra Research Institute on September 2017.

T. Komatsu (✉)
Tokyo University of Science,Tokyo, Japan
e-mail: komatsu_toru@ma.noda.tus.ac.jp

K. Chakraborty et al. (eds.), *Class Groups of Number Fields and Related Topics*,
https://doi.org/10.1007/978-981-15-1514-9_2

Remark 2.2 By some experiments with calculators, I wondered if the 3-divisibilities of $h(\mathbb{Q}(\sqrt{d}))$ and $h(\mathbb{Q}(\sqrt{-d}))$ are independent of one another. The problem is whether there are infinitely many quadratic fields $\mathbb{Q}(\sqrt{D})$ such that $3 \mid h(\mathbb{Q}(\sqrt{D}))$ and $3 \mid h(\mathbb{Q}(\sqrt{-D}))$ or not. It was solved affirmatively in a paper at 2001. Its general cases are done in [7] at 2002.

3 Comparison of Methods

Let $H(k)$ denote the Hilbert class field of k, that is, the maximal unramified abelian extension of k. Class field theory yields an isomorphism $Cl(k) \simeq \mathrm{Gal}(H(k)/k)$ where $\mathrm{Gal}(H(k)/k)$ is the Galois group of the extension $H(k)/k$.

Remark 3.1 In the paper [7] (2002), we construct unramified cyclic cubic extensions of k due to Honda's method [4] (1968) and also to Kishi-Miyake (2000). It is not necessary for the method to consider influence of units. In the paper [8] (2017), we construct ideals of k with order n in $Cl(k)$ due to Yamamoto's method [12] (1970), which needs consideration for the influence of units.

4 Construction of Fields and Extensions

Let us recall the result in the paper [7]. Let $m \neq 1$ be a squarefree rational integer. Let l be a prime number which splits in the extension $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ and is inert in the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. We take a rational integer ν such that

$$\nu \equiv \begin{cases} \pm(4m-3) \pmod{27} & \text{if } m \equiv 1 \pmod{3}, \\ \pm(4m+12) \pmod{27} & \text{if } m \equiv 2 \pmod{3}, \\ \pm 4m \pmod{27} & \text{if } m \equiv 3 \pmod{9}, \\ \pm 1 \pmod{3} & \text{otherwise}, \end{cases}$$

and $m\nu^2 \equiv 1 \pmod{l}$. Now put $r = m\nu^2$. Let T be the set of all of the rational integers t such that

$$t \equiv \begin{cases} 4 \text{ or } 7 \pmod{9} & \text{if } m \equiv 1 \pmod{3}, \\ 3 \pmod{9} & \text{if } m \equiv 2 \pmod{3}, \\ -3 \pmod{27} & \text{if } m \equiv 3 \pmod{9}, \\ \pm(r/3)^2 \pmod{9} & \text{otherwise}, \end{cases}$$

$t \equiv -1 \pmod{l}$ and $t \not\equiv r \pmod{p}$ for every prime divisor $p \neq 3$ of $r(r-1)$. We define

$$D_r(X) := (3X^2 + r)(2X^3 - 3(r+1)X^2 + 6rX - r(r+1))/27.$$

Theorem 4.1 (Komatsu [7]) *For each $t \in T$, we have that $3 \mid h(\mathbb{Q}(\sqrt{D_r(t)}))$ and $3 \mid h(\mathbb{Q}(\sqrt{mD_r(t)}))$. When $m > 0$, if $t \geq 3r/2$ (resp. $t < 3r/2$), then $\mathbb{Q}(\sqrt{D_r(t)})$ and $\mathbb{Q}(\sqrt{mD_r(t)})$ are both real (resp. both imaginary).*

For $t \in T$, put

$$u := t^3 + 3tr, \quad w := 3t^2 + r, \quad a := u - w, \quad b := u - rw, \quad c := t^2 - r.$$

We define

$$f_1(Z) := Z^3 - 3cZ - 2a, \quad f_2(Z) := Z^3 - 3cZ - 2b.$$

For $j = 1$ and 2, let K_j denote the minimal splitting field of $f_j(Z)$ over $\mathbb{Q}$, and $d(f_j)$ the discriminant of the polynomial $f_j(Z)$. Put $k_j := \mathbb{Q}(\sqrt{d(f_j)})$.

Proposition 4.2 *For every $j = 1$ and 2, the extension K_j/k_j is cyclic cubic and unramified. We have that $k_1 = \mathbb{Q}(\sqrt{D_r(t)})$ and $k_2 = \mathbb{Q}(\sqrt{mD_r(t)})$.*

Proof By the definition one has that $r \equiv 1 \pmod{l}$, $t \equiv -1 \pmod{l}$, $a \equiv b \equiv -2^3 \pmod{l}$ and $c \equiv 0 \pmod{l}$. Note that $2 \notin \mathbb{F}_l^3$. Thus $f_j \equiv Z^3 + 2^4 \pmod{l}$ are irreducible over $\mathbb{F}_l$, and so are over $\mathbb{Q}$. Thus K_j/k_j are cyclic cubic.

By using Llorente–Nart's criterion for the decompositions of primes in cubic fields $\mathbb{Q}(\theta)$ where $f_j(\theta) = 0$, we see that $\mathbb{Q}(\theta)/\mathbb{Q}$ are not totally ramified at any finite primes. Hence K_j/k_j are unramified. □

Remark 4.3 The construction yields infinite families, not only of pairs of imaginary and imaginary, but also of those of real and real.

Remark 4.4 Without considering any influence of units, we focus on only the sign of the discriminant. In general, for the n-divisibilities of the class numbers of quadratic fields, we may try to construct $\mathcal{D}_n$-extensions of $\mathbb{Q}$ as the minimal splitting fields of polynomial with degree n. It is difficult to make such polynomials of large degree n with parameters yielding infinite family.

5 Construction of Fields and Ideals

Let us explain the result in the paper [8]. Let $n > 1$ be a rational integer with the prime decomposition $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$. Let $m > 1$ be a squarefree rational integer.
Step 1. We take distinct prime numbers l_i such that $l_i \equiv 1 \pmod{12p_i}$ and $m \in \mathbb{F}_{l_i}^{\times 2}$ for $i = 1, 2, \dots, s$.
Step 2. For each i, we take a rational integer g_i with $g_i, g_i + 1 \notin \mathbb{F}_{l_i}^{p_i}$.
Step 3. We take a positive even number a such that $a^2 m \equiv g_i^2/(g_i + 1)^2 \pmod{l_i}$ for all i.
Step 4. We take a rational integer t satisfying all of the following conditions:

$$\begin{cases} t \equiv g_i/(g_i+1) \pmod{l_i} \text{ for all } i, \\ \gcd(t, am) = 1, \\ \gcd(t-1, b) = 1, \\ t > a^2mn/2, \end{cases}$$

where b is the maximal divisor of $a^2m - 1$ relatively prime to $l_1 l_2 \cdots l_s$.
Step 5. We put $M := \mathbb{Q}(\sqrt{m})$, and

$$\beta := t - a\sqrt{m}, \quad \gamma_1 := 1 + \frac{1}{a\sqrt{m}}, \quad \gamma_2 := 1 + a\sqrt{m},$$
$$x_1 := \mathrm{Tr}(\beta^n \gamma_1), \quad x_2 := \mathrm{Tr}(\beta^n \gamma_2), \quad z_1 := z_2 := N(\beta),$$

where $\mathrm{Tr} = \mathrm{Tr}_{M/\mathbb{Q}}$ and $N = N_{M/\mathbb{Q}}$. For each $j = 1$ and 2, let F_j denote the quadratic field $\mathbb{Q}(\sqrt{x_j^2 - 4z_j^n})$ with discriminant D_j.

Theorem 5.1 (Komatsu [8]) *For each $j = 1$ and 2, F_j is an imaginary quadratic field with an ideal of order n. The ratio $D_2/(mD_1)$ is square.*

Remark 5.2 For each $j = 1$ and 2, there exists a rational integer y_j such that $x_j^2 - 4z_j^n = y_j^2 D_j$. We put $\alpha_j := (x_j + y_j\sqrt{D_j})/2$. Let $\mathfrak{a}_j$ be an ideal of F_j satisfying $\mathfrak{a}_j^n = (\alpha_j)$. This implies that $\mathfrak{a}_j$ is the ideal generated by z_j and α_j. Then the order of $\mathfrak{a}_j$ in $Cl(F_j)$ is equal to n.

For the existence of l_i, we have the following lemma.

Lemma 5.3 *Let p be a prime number. If l is a prime number with $l \equiv 1 \pmod{12mp}$, then $l \equiv 1 \pmod{12p}$ and $m \in \mathbb{F}_l^{\times 2}$.*

Proof Let m_0 be the maximal odd divisor of m. Then one has $\left(\frac{m}{l}\right) = \left(\frac{m_0}{l}\right) = \left(\frac{l}{m_0}\right) = \left(\frac{1}{m_0}\right) = 1$. □

For the existence of g_i, we have the following lemma.

Lemma 5.4 *Let p and l be prime numbers with $l \equiv 1 \pmod{2p}$. Then there exists a rational integer g such that both g and $g+1$ are pth power non-residue modulo l.*

Proof Note that 1 and $l-1$ are pth power residues modulo l. Let g be a pth power non-residue modulo l with $2 \le g \le l-2$. Assume that $g+1$ is a pth power residue modulo l. Then g^{-1} is a suitable one, that is, g^{-1} and $g^{-1} + 1 = (g+1)/g$ are pth power non-residue modulo l. □

Remark 5.5 We can show the existence of a and t due to Chinese remainder theorem (CRT). Since l_i are odd, distinct and $\left(\frac{m}{l_i}\right) = 1$, the integer a proves to exist by CRT. Since $l_1, \ldots, l_s, am, b$ are relatively prime to each other, the integer t proves to exist by CRT.

Remark 5.6 Using Yamamoto's method [12], one can see that $\mathfrak{a}_j$ is of order n in $Cl(F_j)$. In fact, by $\mathfrak{a}_j^n = (\alpha_j)$, the order of $\mathfrak{a}_j$ is a divisor of n. Since α_j is a p_ith power non-residue modulo $\mathfrak{l}_i$ above l_i and units are power residues, the order does not decrease.

Remark 5.7 With l_i, g_i, and a fixed, the family of fields constructed in the run of t is infinite. Indeed, for every large number C, the family contains a quadratic field ramified at a prime number greater than C.

6 New Motivation, Application to a Problem

Let k be a number field with $[k:\mathbb{Q}] < \infty$, and K a Galois extension of k with $[K:k] < \infty$. Let G denote the Galois group of K/k, and $\mathcal{H}$ the family of all of the subgroups of G, that is,

$$\mathcal{H} := \{H : \text{ subgroups of } G\} := \{H_1, H_2, \ldots, H_s\},$$

where s is the number of the subgroups of G. Let K_j denote the fixed field by H_j in K/k. Let $\mathfrak{q}$ be an integral ideal of K, and $\mathfrak{q}_j$ the ideal of K_j below $\mathfrak{q}$, that is, $\mathfrak{q} \cap K_j$. Let n_j denote the order of $\mathfrak{q}_j$ in $Cl(K_j)$, respectively.

Definition 6.1 *We say that $(n_1, n_2, \ldots, n_s)$ is the tuple of the orders in the extension K/k of $\mathfrak{q}$, and shorten it to toe of $\mathfrak{q}$.*

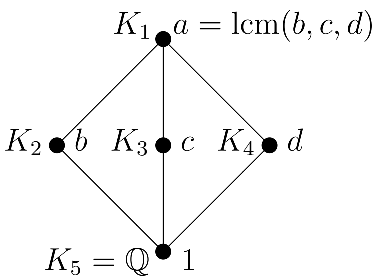
Definition 6.2 *(Inverse Galois problem with toe condition) Let k be a number field with $[k:\mathbb{Q}] < \infty$. Let G be a finite group and $\mathcal{H}$ the family of all of the subgroups of G, $\mathcal{H} := \{H : \text{ subgroups of } G\} := \{H_1, H_2, \ldots, H_s\}$. For given positive integers $n_1, n_2, \ldots, n_s$, does there exist a Galois G-extension K of k with an ideal of toe $(n_1, n_2, \ldots, n_s)$?*

Remark 6.1 It seems to need some conditions on n_j's according to the relations between H_j's.

Let $k = \mathbb{Q}$ and $G = \{e, \sigma, \tau, \sigma\tau\} \simeq V_4 \simeq C_2 \times C_2$ with

$$\mathcal{H} = \{H_1 = \{e\}, H_2 = \langle\sigma\rangle, H_3 = \langle\tau\rangle, H_4 = \langle\sigma\tau\rangle, H_5 = G\}.$$

Corollary 6.3 *Let b, c, d be positive, odd numbers and put $a := lcm(b, c, d)$. Then there exist infinitely many Galois V_4-extensions K of $\mathbb{Q}$ with ideals $\mathfrak{a}$ of toe $(a, b, c, d, 1)$.*



Proof By Yamamoto's result, there exists a real quadratic field $\mathbb{Q}(\sqrt{m})$ with an ideal $\mathfrak{b}$ of order b. Due to Theorem 5.1 at Sect. 5, there exist imaginary quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{mD})$ with ideals $\mathfrak{c}$ and $\mathfrak{d}$ of order cd, respectively. Put $K = \mathbb{Q}(\sqrt{m}, \sqrt{D})$ and $G = \text{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle$ where

$$\sigma : \sqrt{m} \mapsto \sqrt{m}, \sqrt{D} \mapsto -\sqrt{D},$$
$$\tau : \sqrt{m} \mapsto -\sqrt{m}, \sqrt{D} \mapsto \sqrt{D}.$$

Then it follows from the Galois correspondence that $K_1 = K$, $K_2 = \mathbb{Q}(\sqrt{m})$, $K_3 = \mathbb{Q}(\sqrt{D})$, $K_4 = \mathbb{Q}(\sqrt{mD})$, and $K_5 = \mathbb{Q}$. Put $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^d\mathfrak{d}^c$ as ideals of K. Let $\mathfrak{q}$ be a prime ideal of K which is equivalent to $\mathfrak{a}$ in $Cl(K)$, and which splits completely in $K/\mathbb{Q}$. Then the toe of $\mathfrak{q}$ is $(a, b, c, d, 1)$. Indeed, the classes $[\mathfrak{q}_j]$ of $\mathfrak{q}_j$ in $Cl(K_j)$ are as follows:

$$[\mathfrak{q}_1] = [\mathfrak{q}] = [\mathfrak{a}], \quad [\mathfrak{q}_2] = [N_{K/K_2}(\mathfrak{q})] = [\mathfrak{b}^2],$$
$$[\mathfrak{q}_3] = [N_{K/K_3}(\mathfrak{q})] = [\mathfrak{c}^{2d}], \quad [\mathfrak{q}_4] = [N_{K/K_4}(\mathfrak{q})] = [\mathfrak{d}^{2c}], \quad [\mathfrak{q}_5] = [(q)].$$

This completes the proof. □

7 Real Quadratic Cases

Let us recall Yamamoto's method in [12] not only for the imaginary but also for the real. Let F be a quadratic field with discriminant $D \neq -3, -4$. Let x, y, z be rational integers such that $x^2 - y^2 D = 4z^n$ and $\gcd(x, z) = 1$. Put $\alpha_\pm := (x \pm y\sqrt{D})/2$. Then there exists an ideal $\mathfrak{a}$ of F such that $\mathfrak{a}^n = (\alpha_+)$. Put

$$\varepsilon := \begin{cases} \text{the fundamental unit of } F & \text{if } D > 0, \\ 1 & \text{if } D < -4. \end{cases}$$

Let p be a prime factor of n, and l a prime number with $l \equiv 1 \pmod{2p}$. Assume that $x \notin \mathbb{F}_l^p$ and $l \mid z$. Then there exists a prime ideal $\mathfrak{l}$ of F above l dividing α_-.

Lemma 7.1 (Yamamoto [12]) *If ε is a pth power residue modulo $\mathfrak{l}$, then (α_+) is the pth power of no principal ideal in F.*

Let n be a rational integer greater than 1 with the prime decomposition $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$. Let l_i, l_i' be distinct prime numbers with $l_i \equiv l_i' \equiv 1 \pmod{2p_i}$. Let x, z, x', z' be rational integers such that

$$\begin{cases} x^2 - 4z^n = x'^2 - 4z'^n, \\ \gcd(x, z) = \gcd(x', z') = 1, \\ x \notin \mathbb{F}_{l_i}^{p_i}, \quad x' \notin \mathbb{F}_{l_i'}^{p_i}, \quad \dfrac{x + x'}{2} \in \mathbb{F}_{l_i}^{p_i}, \\ l_i \mid z, \quad l_i' \mid z'. \end{cases}$$

Let F denote the quadratic field $\mathbb{Q}(\sqrt{x^2 - 4z^n})$ with discriminant D.

Theorem 7.2 (Yamamoto [12], Prop. 2) *The ideal class group $Cl(F)$ has a subgroup $\mathcal{N}$ isomorphic to $C_n \times C_n$ if $D < -4$, and C_n if $D > 0$.*

Proof There exists a rational integer y such that $x^2 - 4z^n = x'^2 - 4z'^n = y^2 D$. Then there exist ideals $\mathfrak{a}, \mathfrak{a}'$ of F such that $\mathfrak{a}^n = ((x + y\sqrt{D})/2)$ and $\mathfrak{a}'^n = ((x' + y\sqrt{D})/2)$. When $D < -4$, the ideals $\mathfrak{a}$ and $\mathfrak{a}'$ generate $\mathcal{N} \simeq C_n \times C_n$. When $D > 0$, the ideals $\mathfrak{a}$ and $\mathfrak{a}'$ may have orders less than n because of units in F; however, $\mathfrak{a}$ and $\mathfrak{a}'$ generate an ideal of order n in $Cl(F)$. □

Remark 7.3 Diophantine equation $X^2 - Y^2 D = 4Z^n$ does not become complicated as n increases. We need to consider the influence of units. The number of using integers $x, \dots$ for real quadratic cases is more than that for imaginary quadratic cases.

Acknowledgements The author would like to express his deepest gratitude to the organizers Prof. Kalyan Chakraborty, Dr. Azizul Hoque, and Dr. Prem Prakash Pandey for giving an opportunity to talk and inviting to the conference ICCGNFRT held at Harish-Chandra Research Institute on September 2017.

References

1. N.C. Ankeny, S. Chowla, On the divisibility of the class number of quadratic fields. Pac. J. Math. **5**, 321–324 (1955)
2. P. Hartung, Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3. J. Number Theory **6**, 276–278 (1974)
3. P. Hartung, Explicit construction of a class of infinitely many imaginary quadratic fields whose class number is divisible by 3. J. Number Theory **6**, 279–281 (1974)
4. T. Honda, On real quadratic fields whose class numbers are multiples of 3. J. Reine Angew. Math. **233**, 101–102 (1968)
5. P. Humbert, Sur les nombres de classes de certains corps quadratiques. Comment. Math. Helv. **12**, 233–245 (1940)

6. A. Ito, Existence of an infinite family of pairs of quadratic fields $\mathbb{Q}(\sqrt{m_1 D})$ and $\mathbb{Q}(\sqrt{m_2 D})$ whose class numbers are both divisible by 3 or both indivisible by 3. Funct. Approx. Comment. Math. **49**(1), 111–135 (2013)
7. T. Komatsu, An infinite family of pairs of quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{mD})$ whose class numbers are both divisible by 3. Acta Arith. **104**(2), 129–136 (2002)
8. T. Komatsu, An infinite family of pairs of imaginary quadratic fields with ideal classes of a given order. Int. J. Number Theory **13**, 253–260 (2017)
9. S. Kuroda, On the class number of imaginary quadratic number fields. Proc. Jpn. Acad. **40**, 365–367 (1964)
10. T. Nagel, Über die Klassenzahl imaginär-quadratischer Zahlkörper. Abh. Math. Sem. Univ. Hambg. **1**, 140–150 (1922)
11. P.J. Weinberger, Real quadratic fields with class numbers divisible by n. J. Number Theory **5**, 237–241 (1973)
12. Y. Yamamoto, On unramified Galois extensions of quadratic number fields. Osaka J. Math. **7**, 57–76 (1970)