Journal of Number Theory **79**, 249–257 (1999)
Article ID jnth.1999.2433, available online at http://www.idealibrary.com on IDEAL®

Class Numbers and Iwasawa Invariants of Certain Totally Real Number Fields

Dongho Byeon

School of Mathematics, Korea Institute for Advanced Study, 207-43 Cheongryangri-dong, Dongdaemun-gu, Seoul 130-012, Korea

Communicated by Alan C. Woods

Received July 19, 1998

Let p be an odd regular prime number. We prove that there exist infinitely many totally real number fields k of degree $p-1$ whose class numbers are not divisible by p. Moreover, for certain regular prime number p, we prove that there exist infinitely many totally real number fields k of degree $p-1$ whose Iwasawa λ_p-, μ_p-invariants vanish. © 1999 Academic Press

1. INTRODUCTION

For a number field k and a prime number p, we denote by $h(k)$ the class number of k and by $\lambda_p(k), \mu_p(k)$ the Iwasawa λ-, μ-invariants of the cyclotomic $\mathbb{Z}_p$-extension of k, where $\mathbb{Z}_p$ is the ring of p-adic integers.

Let p be an odd prime number. Hartung [5] proved that there exist infinitely many imaginary quadratic fields k whose class numbers are not divisible by p. Later, Horie [7] proved that there exist infinitely many imaginary quadratic fields k such that p does not divide $h(k)$ and p does not split in k. Thus from a theorem of Iwasawa [8], their exist infinitely many imaginary quadratic fields k with $\lambda_p(k) = \mu_p(k) = 0$. Recently, Naito [11] generalized the results of Hartung or Horie to the case of CM-fields, that is, totally imaginary quadratic extensions over a totally real number field.

However, for the case of real number fields, very little is known. Indivisibility of class numbers of real number fields is closely related to Greenberg's conjecture which says that both $\lambda_p(k)$ and $\mu_p(k)$ always vanish for any totally real number field k and any prime number p. It is well-known that $\mu_p(k)$ always vanishes for any abelian number field k and any prime number p by Ferrero and Washington [4], but for $\lambda_p(k)$, very little is known. Nakagawa, and Horie [13] proved that there exist infinitely many real quadratic fields k such that 3 does not divide $h(k)$ and 3 does

0022-314X/99 $30.00

not split in k. Thus, similarly, there exist infinitely many real quadratic fields k with $\lambda_3(k)=\mu_3(k)=0$. Recently, Kraft [10] also showed that the existence of such an infinite family of real quadratic fields by using a result of Jochonowitz.

In this paper, we generalize the results of Nakagawa and Horie or Kraft and prove the following theorem.

THEOREM 1.1. *Let p be an odd regular prime number. Then there exist infinitely many totally real number fields k of degree $p-1$ whose class numbers are not divisible by p.*

Moreover, we show the following theorem.

THEOREM 1.2. *Let p be an odd regular prime number such that $p\equiv 3 \pmod 4$ and satisfies the conditions* (1), (2), (3), *and* (4) *which are stated in Section* 5. *Then there exist infinitely many totally real number fields k of degree $p-1$ such that p does not divide $h(k)$ and p totally ramifies in k. Thus there exist infinitely many totally real number fields of degree $p-1$ with $\lambda_p(k)=\mu_p(k)=0$.*

If $p=3$, since it is easy to see that 3 satisfies the conditions in Theorem 1.2, this is the results of Nakagawa and Horie or Kraft.

In order to get these theorems, we use Parry's work [16] on class number relations between certain pairs of number fields and Naito's work [11, 12] on indivisibility of the class numbers of CM-fields. In Section 2 and Section 3, we briefly introduce their works and in Section 4 and Section 5, using them we prove Theorem 1.1 and Theorem 1.2.

2. CLASS NUMBER RELATION

Let F be a totally real number field. Let p be an odd prime number and ζ_p a primitive pth root of unity. Let $K_3=F(\zeta_p)$ be the totally imaginary quadratic extension over F which contains ζ_p, K_2 a totally imaginary quadratic extension over F such that $K_2\neq K_3$, $K=K_2(\zeta_p)$ a bicyclic biquadratic extension over F, and finally K_1 the maximal real subfield of K. Then using class field theory and Kuroda's class number relation, Parry [16] obtained the following class number relation between $h(K_1)$ and $h(K_2)$.

THEOREM 2.1. *Suppose that p does not divide $h(K_3)$. Then the prime number p divides $h(K_2)$ if and only if p divides $h(K_1)$ or*

$$X^p\equiv e \qquad \bmod (1-\zeta_p)^p$$

is solvable in K for some unit e of K_1 which is not a pth power.

If $p=3$, $K_3=\mathbb{Q}(\zeta_3)$, then this is the result of Herz [6]. For the case $p=5$, $K_3=\mathbb{Q}(\zeta_5)$ and $p=7$, $K_3=\mathbb{Q}(\zeta_7)$, the above class number relations are studied in great detail by Parry [15, 16] and Endô [2, 3].

3. INDIVISIBILITY OF CLASS NUMBERS OF CM-FIELDS

Let F be a totally real number field. For a prime number p, we denote by $n(p)$ the maximum value of n such that primitive p^nth roots ζ_{p^n} of unity are at most of degree 2 over F. If F is fixed, we have $n(p)=0$ for all but finitely many p. Thus we can put $\omega_F=2^{n(2)+1}\prod_{p\neq 2}p^{n(p)}$. Let $\zeta_F(s)$ be the Dedekind zeta function of F. Serre [18] proved that $\omega_F\zeta_F(-1)$ is a rational integer. Using trace formula of Hecke operators and p-adic representations related to automorphic forms obtained from division quaternion algebras over F, Naito [11] proved the following theorem.

THEOREM 3.1. *Let F be a totally real number field. Let p be an odd prime number which does not divide $\omega_F\zeta_F(-1)$. Then there exist infinitely many totally imaginary quadratic extensions k over F such that the relative class number of k is not divisible by p and each prime ideal of F over p does not split in k.*

If $F=\mathbb{Q}$, then this is the result of Hartung [5] or Horie [7].

On the other hand, Naito mentioned that he did not know whether the condition on $\omega_F\zeta_F(-1)$ in Theorem 3.1 is indispensable or not. Thus he studied the case without the condition (see [12]).

4. PROOF OF THEOREM 1.1

Let p be an odd regular prime number and ζ_p a primitive pth root of unity. Let $F=\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ be the maximal real subfield of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$. To use the class number relation in Section 2, we set $K_3=\mathbb{Q}(\zeta_p)$, $K_2=F(\sqrt{-\delta})$ a totally imaginary quadratic extension over F, where δ is a totally positive element in F, $K=F(\sqrt{-\delta},\zeta_p)$ a bicyclic biquadratic extension over F, and finally K_1 the maximal real subfield of K. We note that the degrees of K_1, K_2, and K_3 are all $p-1$. Since p is a regular prime number, p does not divide $h(K_3)$. Thus we can apply the class number relation in Section 2 to our case and have the following relation between $h(K_1)$ and $h(K_2)$.

If p does not divide $h(K_2)$ then p does not divide $h(K_1)$.

Thus we know that if there exist infinitely many totally imaginary quadratic extensions K_2 over F such that p does not divide $h(K_2)$, then

there exist infinitely many totally real number fields of K_1 of degree $p-1$ such that p does not divide $h(K_1)$.

From Theorem 3.1, we conclude that to prove Theorem 1.1, it is enough to show the following lemma.

LEMMA 4.1. *Let p be an odd regular prime number and ζ_p a primitive pth root of unity. Let $F=\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ be the maximal real subfield of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$. Then p does not divide $\omega_g\zeta_F(-1)$.*

Proof. First we note that $\omega_F=2^3\cdot 3\cdot p$. Using the method of Serre in [18], Brown [1] computed the exact fractional part of $\zeta_k(-1)$ for arbitrary totally real number fields k. One of his results is the following: Let p be an odd prime number and ζ_p a primitive pth root of unity. Let k be a totally real number field. If k is the maximal real subfield of $k(\zeta_p)$ and no prime of k lying over p splits in $k(\zeta_p)$, then the power of p dividing the denominator of $\zeta_k(-1)$ is the same as the power of p dividing the denominator of h^-/ω, where h^- is the relative class number of $k(\zeta_p)$ and ω is the number of roots of unity in $k(\zeta_p)$.

If we set $k=F$, then F satisfies the conditions in the above. Since p is a regular prime, p does not divide the relative class number h^-. We know that $\omega=2p$. Thus we have that the exact power of p dividing the denominator of $\zeta_F(-1)$ is 1. Hence we have that p does not divide $\omega_F(-1)$ and this proves the lemma. ∎

This completes the proof of Theorem 1.1.

5. PROOF OF THEOREM 1.2

Let p be an odd regular prime number such that $p\equiv 3 \pmod 4$ and ζ_p be a primitive pth root of unity. Let $F=\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ be the maximal real subfield of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$. Suppose that there exist a prime number $q\neq p$ with the following properties:

(1) $q\equiv 1 \bmod 4$,

(2) q is a non-quadratic residue modulo p,

(3) q remains prime in $F/\mathbb{Q}$,

(4) the class number of $k_0=F(\sqrt{-q})$ is prime to p.

First we claim that there are only finitely many totally imaginary quadratic extensions over F which contain algebraic integers whose norm to F are equal to q. Suppose that a totally imaginary quadratic extension k over F has an algebraic integer $x+y\sqrt{-\delta}$ with $x, y, \delta\in F$ such that

$x^2+\delta y^2=q$ and δ is totally positive. Note that y should not be zero. Since $x-y\sqrt{-\delta}$ is also an algebraic integer in k, $X=2x$ is an algebraic integer in F. Now we can write $\delta=(q-(X^2/4))/y^2$ and

$$k=F(\sqrt{-\delta})=F(\sqrt{-(4q-X^2)},$$

where X is an algebraic integer in F and $4q-X^2$ is totally positive. Then we easily see that there exist only finitely many algebraic integers X such that $4q-X^2$ is totally positive and the claim follows.

Let $k_0=F(\sqrt{-q})$, k_1, ..., k_t be all totally imaginary quadratic extensions over F which contain algebraic integers whose norm to F are equal to q. Let $\mathfrak{p}_i'$ $(i\neq 0)$ be a prime ideal of F which splits completely in k_i/F $(i\neq 0)$ and remains prime in k_0/F.

Since a division quaternion algebra B over F can be determined by giving an even number of archimedean or non-archimedean primes of F which are ramified in B/F, we can take a division quaternion algebra B/F as follows:

(i) only one real prime is unramified in B/F and other real primes are ramified in B/F

(ii) $\mathfrak{p}_1'$, ..., $\mathfrak{p}_t'$ are ramified in B/F,

(iii) q is unramified in B/F,

(iv) the other prime ideals $\mathfrak{r}$ which are ramified in B/F remain prime in k_0/F.

Let $\mathfrak{S}(s,\rho)$ be the space of automorphic forms associated with B/F in [11] and $\mathfrak{T}(\mathfrak{r})$ the Hecke operators acting on $\mathfrak{S}(s,\rho)$ for a prime ideal $\mathfrak{r}$ of F. Let $\phi_{S,\rho}\colon \mathrm{Gal}(\bar{F}/F)\to \mathrm{GL}_{2\dim_{\mathbb{C}}\mathfrak{S}(S,\rho)}(\mathbb{Q}_p)$ be the p-adic representation which Ohta got in [14]. Let Ω_0 be the set of isomorphism classes of orders $\mathfrak{o}$ of totally imaginary quadratic extensions over F in B satisfying the following properties:

(i) no prime factor of the discriminant $D(B/F)$ of B/F splits in $F(\mathfrak{o})$,

(ii) the conductor of $\mathfrak{o}$ is prime to $D(B/F)$.

Let E and E^+ be the group of units and the group of totally positive units of the ring of integers of F respectively. Let $h(\mathfrak{o})$ be the class number of $\mathfrak{o}$ and $E(\mathfrak{o})$ the group of units in $\mathfrak{o}$. For a prime ideal $\mathfrak{p}$ in F, we define $(\mathfrak{o}/\mathfrak{p})$ by $(\mathfrak{o}/\mathfrak{p})=1$, -1, and 0 when $\mathfrak{p}$ splits completely, remains prime, and ramifies in $F(\mathfrak{o})/F$ respectively. We denote by $v=v_{B/F}$ the reduced norm of B/F. We put $n=2$ if $p\geqslant 5$ and $n=4$ if $p=3$. Now we can state trace formula of Hecke operator $\mathfrak{T}(\mathfrak{r})$ for a prime ideal $\mathfrak{r}$ of F,

$$\operatorname{tr}.\mathfrak{T}(\mathfrak{r}) = -\frac{[E:E^+]}{2} \sum_{\mathfrak{o}\in\Omega_0} h(\mathfrak{o}) \frac{\prod_{\mathfrak{p}\mid D(B/F)}(1-(\mathfrak{o}/\mathfrak{p}))}{[E(\mathfrak{o}:E)]}$$
$$\times \sum_{\substack{\alpha\in J(\mathfrak{o}) \\ \alpha \pmod E}} \operatorname{tr}.\Psi(\alpha) \frac{\zeta_\alpha^{n+1}-\eta_\alpha^{n+1}}{\zeta_\alpha-\eta_\alpha} (\det\alpha)^{-n/2},$$

where $J(\mathfrak{o}) = \{\alpha\in\mathfrak{o}: \alpha\notin F, (v(\alpha))=\mathfrak{r}\}$, ζ_α, η_α are eigenvalues of α and Ψ is a representation introduced in [11, Sect. 1].

From the choice of B/F and q, by the similar argument in [12], we see that to compute the trace of Hecke operator $\mathfrak{T}((q))$, it is enough to consider only the ring of integers $\mathfrak{o}_{k_0}$ of k_0. Put $\alpha=\sqrt{-q}$. Then we get

$$\operatorname{tr}.\mathfrak{T}((q)) = -\frac{[E:E^+]}{2} h(k_0) \prod_{\mathfrak{p}\mid D(D/F)} \left(1-\left(\frac{\mathfrak{o}}{\mathfrak{p}}\right)\right)$$
$$\times \operatorname{tr}.\Psi(\alpha) \frac{\zeta_\alpha^{n+1}-\eta_\alpha^{n+1}}{\zeta_\alpha-\eta_\alpha} q^{-n/2}.$$

Moreover, since α satisfies (2), (3), (4), and (5) in [12] and p does not divide $h(k_0)$, we can also prove that

$$\operatorname{tr}.\mathfrak{T}((q)) \not\equiv 0 \pmod p.$$

We put $H_p = \{g\in \mathrm{GL}_{2\dim_{\mathbb{C}}\mathfrak{S}(S,\rho)}(\mathbb{Q}_p): g\equiv 1 \bmod p\}$. Let M_p be the fixed field by $\phi_{s,\rho}^{-1}(H_p)$. From (iii), q does not divide $pD(B/F)$. So from the properties of $\phi_{s,\rho}$, (q) does not ramify in M_p/F. But (q) ramifies in k_0/F. Thus we have $M_p\cap k_0 = F$. From Tchebotarev density theorem [9] and class field theory, we know that there exist infinitely many prime numbers s such that $s\equiv q \pmod p$ and (s) decomposes in $M_p/\mathbb{Q}$ in the same manner as (q) and remains prime in $k_0/\mathbb{Q}$. Let s be one of these prime numbers. Then, from $s\equiv q \pmod p$, we see that (s) remains prime in $F/\mathbb{Q}$ and the prime ideal (s) of F decomposes in M_p/F in the same manner as (q) and remains prime in k_0/F. Thus there is no element β of k_0 such that $(N_{k_0/F}(\beta))=(s)$. So no order of k_0 appears in the formula of $\operatorname{tr}.\mathfrak{T}((s))$. Because $\operatorname{tr}.\mathfrak{T}((s)) = \operatorname{tr}.\mathfrak{T}((q)) \not\equiv 0 \pmod p$, we see that F has another totally imaginary quadratic extension k' whose class number is not divisible by p. Let $k'=F(\sqrt{-\delta'})$ be another such totally imaginary quadratic extension over F, where δ' is a totally positive algebraic integer in F. Then there exist x, y in F satisfying $x^2+\delta' y^2 = s$. We claim that δ' is prime to p. Otherwise, we have $x^2\equiv s \pmod p$. But since $s\equiv q \pmod p$ and q is a non-quadratic residue modulo p, we have a contradiction and get the claim.

Finally, from the above argument and from the same argument in [12], we get the following conclusion: Let p be an odd regular prime number such that $p \equiv 3 \pmod 4$ and ζ_p be a primitive pth root of unity. Let $F = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ be the maximal real subfield of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$. If there exist a prime number $q \neq p$ satisfying (1), (2), (3), and (4), then there exist infinitely many totally imaginary quadratic extensions $k' = F(\sqrt{-\delta'})$ over F such that p does not divide $h(k')$ and p is prime to the totally positive algebraic integer δ' in F.

Now, we set $K_3 = \mathbb{Q}(\zeta_p)$, $K_2 = k' = F(\sqrt{-\delta'})$ the totally imaginary quadratic extension over F in the above, $K = k'(\zeta_p) = F(\sqrt{-\delta'}, \zeta_p)$ a bicyclic biquadratic extension over F, and finally $K_1 = F(\sqrt{p\delta'})$ the maximal real subfield of K. Then from the class number relation in Section 2 and the above conclusion, we have there exist infinitely many totally real number fields $k = F(\sqrt{p\delta'})$ of degree $p-1$ such that p does not divide $h(k)$ and p totally ramifies in k.

From a theorem of Iwasawa in [8], we get that for these totally real number fields k, $\lambda_p(k) = \mu_p(k) = 0$. This completes the proof of Theorem 1.2.

Now, we give some examples.

EXAMPLE 1. Let $p = 3$ then $F = \mathbb{Q}$. Let $q = 5$ then q satisfies (1), (2), and (3). Since the class number of $k_0 = \mathbb{Q}(\sqrt{-5})$ is 2, q satisfies also (4). Thus we have that there exist infinitely many real quadratic fields k such that 3 does not divide $h(k)$ and 3 totally ramifies in k. This is the result of Nakagawa and Horie [13] or Kraft [10].

EXAMPLE 2. Let $p = 7$ then $F = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ is a totally real cyclic cubic field. Let $q = 5$ then q satisfies (1),(2), and (3). Since the class number of $k_0 = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \sqrt{-5})$ is 2 (cf. [17]), q satisfies also (4). Thus we have that there exist infinitely many totally real number fields k of degree 6 such that 7 does not divide $h(k)$ and 7 totally ramifies in k.

Finally, we suggest some problems which naturally arise from this work.

Problem 1. Let p be an odd regular prime number. We note that the assumption that $p \equiv 3 \pmod 4$ is indispensable for our proof of Theorem 1.2. For example, if $p = 5$ then there is no prime number s such that (s) remains prime in a bicyclic biquadratic field $k_0 = \mathbb{Q}(\zeta_5 + \zeta_5^{-1}, \sqrt{-q})/\mathbb{Q}$. Thus we can not show that p is prime to δ' in the proof of Theorem 1.2. Can we remove the assumption that $p \equiv 3 \pmod 4$ in Theorem 1.2?

Problem 2. Let p be an odd regular prime number and ζ_p a primitive pth root of unity. Let $F = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ be the maximal real subfield of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$. From the class number relation in Section 2

and class field theory (cf. [16, Corollary 2 and Corollary 3]), we know that if $p \equiv 3 \pmod 4$ (resp. $p \equiv 1 \pmod 4$) and F has infinitely many totally imaginary quadratic extensions $F(\sqrt{-pm})$ (resp. $F((\zeta_p - \zeta_p^{-1})\sqrt{m})$) whose ideal class numbers are not divisible by p, where m is a positive square free integer, then there exist infinitely many real quadratic fields $\mathbb{Q}(\sqrt{m})$ whose ideal class numbers are not divisible by p. Indivisibility of class numbers of real quadratic fields by an odd prime number $p \neq 3$ is a well known open problem. Can we construct infinitely many the such totally imaginary quadratic extensions over F?

Problem 3. To use the class number relation in Section 2, p should be a regular prime. Thus the assumption that p is a regular prime is essential to our proofs of Theorem 1.1 and Theorem 1.2. Can we generalize these theorems to an irregular prime p?

ACKNOWLEDGMENT

The author thanks the referee for many helpful suggestions.

REFERENCES

1. K. S. Brown, Euler characteristics of discrete groups and G-spaces, *Invent. Math.* **27** (1974), 229–264.
2. A. Endô, Remark on the divisibility of class numbers of certain quartic number fields by 5, *Proc. Amer. Math. Soc.* **91**, No. 4 (1984), 513–517.
3. A. Endô, Class number relation between certain sextic number fields, *Proc. Amer. Math. Soc.* **95**, No. 2 (1985), 199–204.
4. B. Ferrero and L. C. Washington, The Iwasawa invariants μ_p vanishes for abelian number fields, *Ann. of Math.* **109** (1979), 377–395.
5. P. Hartung, Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3, *J. Number Theory* **6** (1974), 276–278.
6. C. S. Herz, "Construction of Class Fields," Lecture Notes in Math., Vol. 21, Springer-Verlag, Berlin/New York, 1966.
7. K. Horie, A note on basic Iwasawa λ-invariants of imaginary quadratic fields, *Invent. Math.* **88** (1987), 31–38.
8. K. Iwasawa, A note on class numbers of algebraic number fields, *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 257–258.
9. G. J. Janusz, "Algebraic Number Fields," Academic Press, San Diego, 1973.
10. J. S. Kraft, Class numbers and Iwasawa invariants of quadratic fields, *Proc. Amer. Math. Soc.* **124** (1996), 31–34.
11. H. Naito, Indivisibility of class numbers of totally imaginary quadratic extensions and their Iwasawa invariants, *J. Math. Soc. Japan* **43**, No. 1 (1991), 185–194.
12. H. Naito, Erratum to "Indivisibility of class numbers of totally imaginary quadratic extensions and their Iwasawa invariants," *J. Math. Soc. Japan* **46**, No. 4 (1994), 725–726.
13. J. Nakagawa and K. Horie, Elliptic curves with no rational points, *Proc. Amer. Math. Soc.* **104** (1988), 20–24.

14. M. Ohta, On *l*-adic representations attached to automorphic forms, *Japan J. Math.* **8** (1982), 1–47.
15. C. J. Parry, Real quadratic fields with class numbers divisible by five, *Math. Comp.* **31**, No. 140 (1977), 1019–1029.
16. C. J. Parry, On the class numbers of relative quadratic fields, *Math. Comp.* **32**, No. 144 (1978), 1261–1270.
17. Y. H. Park and S. H. Kwon, Determination of all imaginary abelian sextic number fields with class number $\leqslant 11$, *Acta Arith.* **82**, No. 1 (1997), 27–43.
18. J. P. Serre, Cohomologie des groupes discretes, *in* "Prospects in Mathematics," Ann. of Math. Stud., Vol. 70, pp. 77–170, Princeton Univ. Press, Princeton, NJ, 1971.