Divisibility of class numbers of non-normal totally real cubic number fields

By Jungyun Lee

ASARC Department of Mathematical Sciences KAIST 335 Gwahangno, Yuseong-gu,
Daejeon 350-701, Republic of Korea

(Communicated by Shigefumi Mori, M.J.A., Jan. 12, 2010)

Abstract: In this paper, we consider a family of cubic fields $\{K_m\}_{m\geq 4}$ associated to the irreducible cubic polynomials $P_m(x) = x^3 - mx^2 - (m+1)x - 1$, $(m \geq 4)$. We prove that there are infinitely many $\{K_m\}_{m\geq 4}$'s whose class numbers are divisible by a given integer n. From this, we find that there are infinitely many non-normal totally real cubic fields with class number divisible by any given integer n.

Key words: Class number; totally real cubic fields.

1. Introduction. Let K_m be a field associated with the irreducible polynomials

$$P_m = x^3 - mx^2 - (m+1)x - 1,$$

for $(m \geq 4)$. It is well known that K_m $(m \geq 4)$ are non-normal totally real cubic number fields with discriminants (See [4])

$$D_m = (m^2 + m - 3)^2 - 32. \tag{1}$$

Louboutin in [1] studied the class groups of $\{K_m\}_{m\geq 4}$ and determined K_m of small class number or of class group with small exponent.

In this paper, we are interested in the divisibility of the class numbers of a family $\{K_m\}_{m\geq 4}$ by a given integer n. The following is a result:

Theorem 1.1. *There are infinitely many m for which the ideal class group of K_m has a subgroup isomorphic to $\mathbf{Z}/n\mathbf{Z}$.*

To prove above theorem, we use Nakano's Lemma in [3]:

Lemma 1.2 (Nakano)**.** *Let n, m be integers greater than 1 and n_0 be the product of all prime divisors of n,*

$$m_0 := \mathrm{lcm}\{|w_K| \mid K \text{ is a field of degree } m\},$$

where w_K is the number of roots of unity in K, and $L(n)$ be the set of all prime divisors l of n. Let $f(x) \in \mathbf{Z}[x]$ be a monic irreducible polynomial of degree m, θ be a root of $f(x)$, $K = \mathbf{Q}(\theta)$, and r be the free rank of the unit group of K. Suppose there exist primes $p_1, \cdots, p_s$ which are 1 modulo $m_0 n_0$ and rational integers t, $A_1, \cdots, A_s$ and $C_1, \cdots, C_s$ such that

(1) $f(A_i) = \pm C_i^n$, $(1 \leq i \leq s)$,
(2) $(f'(A_i), C_i) = 1$, $(1 \leq i \leq s)$,
(3) $f(t) \equiv 0, f'(t) \not\equiv 0 \pmod{p_i}$, $(1 \leq i \leq s)$
(4) $\left(\frac{t-A_j}{p_i}\right)_l = 1, \left(\frac{t-A_i}{p_i}\right)_l \neq 1, (1 \leq j < i \leq s, l \in L(n))$,

where $f'(x)$ is the derivative of $f(x)$. Then the ideal class group of K contains a subgroup isomorphic to $(\mathbf{Z}/n\mathbf{Z})^{s-r}$.

Since K_m is totally real cubic field, the free rank r of the unit group is 2 and w_{K_m} is 2. We find p_i, A_i and C_i $(1 \leq i \leq 3)$ and t satisfying all the conditions of Nakano's Lemma for infinitely many $f(x) = P_m(x)$ to prove the main theorem.

According to Nakano (cf. [3]), for each extension degree, there are infinitely many totally real number fields of class number divisible by a given integer n. *A priori* we know for each n, there are infinitely many totally real cubic number fields whose class number is divisible by n. Since K_m are non-normal totally real cubic number fields, from Theorem 1.1, we conclude:

Corollary 2.2. *There are infinitely many non-normal totally real cubic number fields whose class numbers are divisible by any given integer n.*

2. Proof of Main Theorem. Firstly, to use Lemma 1.2, we need the following lemma.

Lemma 2.1. *Let n be an integer and n_1 be n or $2n$ according as $n \not\equiv 2 \pmod 4$ or $n \equiv 2 \pmod 4$ and $A_1 = -1, A_2 = 0$ and $A_3 = 1$. Then there exists a rational integer t for which there are infinitely many triple of primes (p_1, p_2, p_3) such that $p_i \equiv 1 \pmod{n_1}$ for $i = 1, 2, 3$ and*

2000 Mathematics Subject Classification. Primary 11R29, 11R80.

doi: 10.3792/pjaa.86.38

$$\left(\frac{t-A_j}{p_i}\right)_l = 1 \ and \ \left(\frac{t-A_i}{p_i}\right)_l \neq 1$$

for $l \in L(n)$, $i \neq j$ *in* $\{1,2,3\}$ *and*

$$\left(\frac{\frac{(1-t)(2t^2+3t+2)}{t(t+1)}}{p_i}\right)_n = 1.$$

Proof. Let $F = \mathbf{Q}(\zeta_{n_1})$, where ζ_{n_1} is an n_1-th root of unity. Since there are infinitely many rational integers a such that $2a^2+3a+2$ is square free, we can take an integer B and a rational prime q such that $2B^2+3B+2$ is square free and

$$q | 2B^2+3B+2,$$

$$q \not| 14n_1.$$

Since only primes dividing n_1 are ramified in F over $\mathbf{Q}$, for a prime ideal $\mathbf{q} \in F$ lying over q, we have

$$(2) \qquad ord_{\mathbf{q}}(2B^2+3B+2) = 1.$$

Next, we take three distinct prime ideals $\mathbf{q}_i (\neq \mathbf{q}) \in F$ $(i=1,2,3)$ which are relatively prime to $14n_1$ and rational integers B_i $(i=1,2,3)$ for which

$$(3) \qquad ord_{\mathbf{q}_i}(B_i) = 1 \quad \text{for } 1 \leq i \leq 3.$$

Then we can find a nonzero element $T \in O_F$ such that

$$(4) \qquad \begin{aligned} T &\equiv B \pmod{\mathbf{q}^2}, \\ T - A_i &\equiv B_i \pmod{\mathbf{q}_i^2} \quad \text{for } i=1,2,3. \end{aligned}$$

Then

(5)

$$\begin{aligned} &ord_{\mathbf{q}}(2T^2+3T+2) = ord_{\mathbf{q}}(2B^2+3B+2) = 1, \\ &2T^2+3T+2 \equiv 2A_i^2+3A_i+2 \pmod{\mathbf{q}_i}. \\ &\qquad\qquad\qquad \text{for } i=1,2,3. \end{aligned}$$

Since $\mathbf{q}$ and $\mathbf{q}_i$ $(i=1,2,3)$ are relatively prime to 14, form (5) we have

$$(6) \qquad \begin{aligned} &ord_{\mathbf{q}_i}(2T^2+3T+2) = 0, \\ &ord_{\mathbf{q}}(T-A_i) = 0. \end{aligned}$$

And

$$(7) \quad ord_{\mathbf{q}_i}(T-A_i) = ord_{\mathbf{q}_i}(B_i) = 1 \quad \text{for } 1 \leq i \leq 3.$$

Since $\mathbf{q}_i$ $(i=1,2,3)$ are relatively prime to 2,

$$ord_{\mathbf{q}_i}(T-A_j) = 0 \quad \text{for } 1 \leq i \neq j \leq 3.$$

Let $\beta := (2T^2+3T+2)^a \quad (T-A_1)^{a_1} \quad (T-A_2)^{a_2}$ $(T-A_3)^{a_3}$. Then

$$\begin{aligned} &ord_{\mathbf{q}}(\beta) = a, \\ &ord_{\mathbf{q}_i}(\beta) = a_i \quad \text{for } i=1,2,3. \end{aligned}$$

Thus if $\beta \in F^{*l}$, then we have

$$\begin{aligned} &a \equiv 0 \pmod{l}, \\ &a_i \equiv 0 \pmod{l} \quad \text{for } i=1,2,3. \end{aligned}$$

It implies that $2T^2+3T+2$, $T-A_1$, $T-A_2$ and $T-A_3$ are independent in F^*/F^{*l}. So for $n_0 = \prod_{l \in L(n)} l$,

$$F(\sqrt[n_0]{T-A_i}) \cap E_i = F \quad (i=1,2,3),$$

where

$$E_i = \prod_{j \neq i} F(\sqrt[n_0]{T-A_j}) F\left(\sqrt[n]{\frac{(1-T)(2T^2+3T+2)}{T(T+1)}}\right) \qquad (i=1,2,3).$$

By Frobenious density theorem, we know that there exist infinitely many primes $\mathbf{p}_i$ in F which have inertia degree 1 over $\mathbf{Q}$ and inert in $F(\sqrt[n_0]{T-A_i})$ and completely split in E_i for $i=1,2,3$. Let p_i be a rational prime such that $(p_i) = \mathbf{Z} \cap \mathbf{p}_i$ for $i=1,2,3$. Since

$$O_F/\mathbf{p}_i \simeq \mathbf{Z}/(p_i),$$

we can take a rational integer t in $T + \mathbf{p}_i$ and we have

$$\left(\frac{T-A_j}{\mathbf{p}_i}\right)_l = \left(\frac{t-A_j}{p_i}\right)_l \quad \text{for } i,j=1,2,3,$$

and

$$\left(\frac{\frac{(1-T)(2T^2+3T+2)}{T(T+1)}}{\mathbf{p}_i}\right)_n = \left(\frac{\frac{(1-t)(2t^2+3t+2)}{t(t+1)}}{p_i}\right)_n.$$

Since the prime ideals $\mathbf{p}_i$ inert in $F(\sqrt[n_0]{T-A_i})$ and completely split in E_i for $i=1,2,3$, we have

$$\left(\frac{T-A_j}{\mathbf{p}_i}\right)_l = 1,$$

if and only if $i \neq j$ and

$$\left(\frac{\frac{(1-T)(2T^2+3T+2)}{T(T+1)}}{\mathbf{p}_i}\right)_n = 1.$$

Moreover since $\mathbf{p}_i$ $(i=1,2,3)$ have inertia degree 1 over $\mathbf{Q}$, we have $p_i \equiv 1 \pmod{n_1}$. This completes the proof. □

Now, we come to prove Theorm 1.1.

Proof of Theorem 1.1. Let a be a rational integer such that

(8) $$(a, 14) = 1.$$

Put

$$m = \frac{-1 - a^n}{2}.$$

Then

(9) $$P_m(-1) = -1.$$

(10) $$P_m(0) = -1.$$

(11) $$P_m(1) = -1 - 2m = a^n.$$

and from (8), we have

(12) $$(P'_m(1), a) = \left(\frac{7 + 3a^n}{2}, a\right) = 1.$$

Let us consider $P_m(x)$ to $f(x)$ and $A_1 = -1$, $A_2 = 0$, $A_3 = 1$ and $C_1 = C_2 = 1$, $C_3 = a$. Then they satisfy the conditions (1) and (2) in Lemma 1.2.

We can take distinct primes p_1, p_2 and p_3 (> 7) and a rational integer t satisfying all conditions of Lemma 2.1 and

(13)

$$p_i \nmid (1 + t - 4t^2 - 9t^3 - 4t^4 + t^5 + t^6)^2 - 32(t(t+1))^4.$$

Since

$$\left(\frac{\frac{(1-t)(2t^2+3t+2)}{t(t+1)}}{p_i}\right)_n = 1,$$

we can find an integer a such that

(14) $$a^n = \frac{(1-t)(2t^2 + 3t + 2)}{t(t+1)} \pmod{p_i} \quad \text{for } i = 1, 2, 3.$$

Then we have

(15) $$P_m(t) \equiv 0 \pmod{p_i} \quad \text{for } i = 1, 2, 3.$$

Suppose that $P'_m(t) \equiv 0 \pmod{p_i}$ then t is a multiple root of $P_m(x) \pmod{p_i}$. Therefore p_i divide the discriminant of $P_m(x)$. So we have

(16)

$$(m^2 + m - 3)^2 - 32 \equiv 0 \pmod{p_i} \quad \text{for } i = 1, 2, 3.$$

Since

(17) $$m \equiv \frac{t^3 - t - 1}{t(t+1)} \pmod{p_i} \quad \text{for } i = 1, 2, 3,$$

the equation (16) implies that for $i = 1, 2, 3$,

$$(1 + t - 4t^2 - 9t^3 - 4t^4 + t^5 + t^6)^2 - 32(t(t+1))^4 \equiv 0 \pmod{p_i}.$$

It contracidts to (13). Hence

$$P'_m(t) \not\equiv 0 \pmod{p_i} \quad \text{for } i = 1, 2, 3.$$

Finally, we find the rational integers A_i, C_i ($i = 1, 2, 3$) and t and primes p_i ($i = 1, 2, 3$) satisfying all conditions of Lemma 1.2. Thus we find that the class group of $K_{\frac{-1-a^n}{2}}$ has the subgroup isomorphic to $\mathbf{Z}/n\mathbf{Z}$, if an integer a satisfy (8), (14). Thus for any n, we can find $m(n)$ (an integer depending on n) such that the class number of $K_{m(n)}$ is divisible by n. Hence for every multiples ns ($s = 1, 2, \cdots$) of n we also find an integer $m(n, s)$ such that the class number of $K_{m(n,s)}$ is divisible by ns. The set $\{K_{m(n,s)} \mid s = 1, 2, \cdots\}$ is infinite since the set of class numbers of $K_{m(n,s)}$ cannot be finite. From this, we complete the proof of theorem. □

Corollary 2.2. *There are infinitely many non-normal totally real cubic number fields whose class numbers are divisible by any given integer n.*

Remark. The method of the proof is from [2]. In [2], this method is used to prove there are infinitely many cubic cyclic fields whose ideal class groups contain a subgroup isomorphic to $(\mathbf{Z}/n\mathbf{Z})^2$.

Acknowledgements. The author thanks referee for helpful suggestions. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (N.R.F) funded by the Ministry of Education, Science and Technology 2009-0063182.

References

[1] S. Louboutin, Class number and class group problems for some non-normal totally real cubic number fields, Manuscripta Math. **106** (2001), no. 4, 411–427.

[2] S. Nakano, Ideal class groups of cubic cyclic fields, Acta Arith. **46** (1986), no. 3, 297–300.

[3] S. Nakano, On ideal class groups of algebraic number fields, J. Reine Angew. Math. **358** (1985), 61–75.

[4] M. Mignotte and N. Tzanakis, On a family of cubics, J. Number Theory **39** (1991), no. 1, 41–49.