Class number 3 problem for the simplest cubic fields

Dongho Byeon

[1] [2]

ABSTRACT. We give some necessary conditions for class numbers of the simplest cubic fields to be 3 and using Lettl's lower bounds of residues at $s = 1$ of Dedekind zeta functions attached to cyclic cubic fields [**?**], determine all the simplest cubic fields of class number 3.

1 Introduction

Let $m \geq -1$ be a rational integer such that $m \not\equiv 3 \bmod 9$ and $m^2 + 3m + 9$ is square-free or 9 times a square-free rational integer. Let K be the cyclic cubic field defined by the irreducible polynomial over the rational number field $\mathbb{Q}$ of the following form

$$f(x) = x^3 + mx^2 - (m+3)x + 1.$$

Let α be the negative root of $f(x)$. Then $\alpha' = 1/(1-\alpha)$ and $\alpha'' = 1-1/\alpha$ are its conjugates. Moreover $\{1, \alpha, \alpha^2\}$ is an integral basis of K and $\{\alpha, \alpha'\}$ is a fundamental system of units of K. The discriminant of K is the discriminant of the polynomial of $f(x)$: $D^2 = (m^2 + 3m + 9)^2$ and the conductor of K is $D = (m^2 + 3m + 9) = ((2m+3)^2 + 27)/4$. We call K be the simplest cubic field ([**?**] [**?**]).

In [**?**], Lettl has obtained a lower bound of residues at s=1 of Dedekind zeta functions attached to cyclic cubic fields and applying his lower bound

[1] *1991 Mathematics Subject Classification 11R16, 11R29*

[2] This research is supported by POSTECH/BSRI special fund.

to the simplest cubic fields with prime conductors, has shown that there are exactly seven simplest cubic fields of class number 1: their conductors D=7, 13, 19, 37, 79, 97, 139.

In this paper, first we derive some necessary conditions for class numbers of the simplest cubic fields to be 3 and finally applying Lettl's lower bound, determine all the simplest cubic fields of class number 3.

2 Some necessary conditions for class numbers of the simplest cubic fields to be 3

First we give the preliminary results. Let h_K be the class number of the simplest cubic field K. Let $N_{K/\mathbb{Q}}$ denote the norm of an element in K and N denote the norm of an ideal in K.

Lemma 2.1 *Let f be a factor of $2m+3$. Then (f) is factorized in K with the following form,*

$$(f) = (f, \alpha+1)(f, \alpha-2)(f, \alpha+m+1),$$

in fact, these three factors are conjugated under Galois action. Moreover, if $f = 2m+3$ then $(f, \alpha+1)$, $(f, \alpha-2)$ and $(f, \alpha+m+1)$ are principal.

Proof: First we note that

$$\begin{aligned}(\alpha+1)(\alpha-2)(\alpha+m+1) &= \alpha^3 + m\alpha^2 - (m+3)\alpha + 1 - (2m+3) \\ &= -(2m+3).\end{aligned}$$

By a direct computation, we have

$$\begin{aligned}& (f, \alpha+1)(f, \alpha-2)(f, \alpha+m+1) \\ = \; & f(f^2, f(\alpha+1), f(\alpha-2), f(\alpha+m+1), (\alpha-2)(\alpha+m+1), \\ & (\alpha+1)(\alpha+m+1), (\alpha+1)(\alpha-2), -g) \\ = \; & f\mathbf{a},\end{aligned}$$

where $2m+3 = fg$.

It is not difficult to see that $\mathbf{a} = (1)$. Note that $\alpha - 2 = -\frac{1}{\alpha'}(\alpha+1)'$ and $\alpha + m + 1 = -\alpha'(\alpha+1)''$. Then we know that the three factors of (f) are

conjugated under Galois action. From the fact $(\alpha+1)(\alpha-2)(\alpha+m+1) = -(2m+3)$, we easily see that $(2m+3, \alpha+1) = (\alpha+1)$, $(2m+3, \alpha-2) = (\alpha-2)$ and $(2m+3, \alpha+m+1) = (\alpha+m+1)$. Thus we have proved the lemma. □

Lemma 2.2 *(Lemmermeyer and Pethö [?]) For all algebraic integers γ in K, either $|N_{K/\mathbb{Q}}(\gamma)| \geq 2m+3$ or γ is associated to a rational integer. Moreover if $|N_{K/\mathbb{Q}}(\gamma)| = 2m+3$ then γ is associated to one of the conjugates of $\alpha+1$.*

As an application of Lemma 2.2, we have the following theorem.

Theorem 2.3 *Let K be a simplest cubic field. If $h_K = 1$ then $2m+3$ is a prime.*

Proof: Suppose that $2m+3$ be a composite integer and p be a prime factor of $2m+3$. Then p can not inert in K by Lemma 2.1. Let $\mathbf{p}$ denote a prime divisor over p in K. Then $N(\mathbf{p}) = p < 2m+3$. So $\mathbf{p}$ can not be principal by Lemma 2.2 and $h_K \neq 1$. Thus we have proved the theorem. □

Remark. Though all the simplest cubic fields of class number 1 was determined, it seems interesting to note that Theorem 2.3 can be a cubic analogue of the following well-known work for quadratic fields [?]

> Let $K = \mathbb{Q}(\sqrt{4m^2+1})$ for some rational integer m. If $h_K = 1$ then m is prime.

Proposition 2.4 *Let K be a simplest cubic field. If $h_K = 3$ then $D = m^2+3m+9 = 9p$ where p is a prime or $D = m^2+3m+9 = pq$ where $p < q$ are both primes and p is not cubic residue modulo q or q is not cubic residue modulo p.*

Proof: See [?] [?] or [?] for a proof of a more general theorem. □

From now on, we only have to consider the simplest cubic fields with conductors $D = 9p$ where p is a prime or $D = pq$ where $p < q$ are both primes. To give more necessary conditions for class numbers of the simplest cubic fields to be 3, we need the following proposition and lemmas. We only give the details of the case $D = pq$. Let $[\mathbf{a}]$ denote the ideal class containing an ideal $\mathbf{a}$ in K.

Proposition 2.5 *Let K be the simplest cubic field with conductor $D = pq$ where $p < q$ are both primes. Let $p = \mathbf{p}^3$ where $\mathbf{p}$ is a prime ideal in K. Then $\mathbf{p}$ is not principal. Specially if $h_K = 3$ then the ideal class group of K is generated by $[\mathbf{p}]$.*

Proof: Since $p < \sqrt{m^2 + 3m + 9} < 2m + 3$, $N(\mathbf{p}) = p < 2m + 3$. From Lemma 2.2, we know that $\mathbf{p}$ is not principal and the order of $[\mathbf{p}]$ is 3. Thus we have proved the proposition. □

Lemma 2.6 *Let K be the simplest cubic field with conductor $D = pq$ where $p < q$ are both primes. If $h_K = 3$ and a prime r splits in K then $r^3 \geq 2m+3$ and $p^2 r \geq 2m + 3$.*

Proof: Let $p = \mathbf{p}^3$ and $r = \mathbf{r}_1\mathbf{r}_2\mathbf{r}_3$, where $\mathbf{p}$, $\mathbf{r}_1$, $\mathbf{r}_2$ and $\mathbf{r}_3$ are prime ideals in K. Suppose that $r^3 < 2m + 3$. Then $N(\mathbf{r}_1) = r < 2m + 3$ and $N(\mathbf{r}_1^3) = r^3 < 2m + 3$. From Lemma 2.2, $\mathbf{r}_1$ and $\mathbf{r}_1^3$ are not principal. Thus $h_K \neq 3$. So r^3 should be greater than or equal to $2m + 3$.

Now we consider the ideal $\mathbf{p}^2\mathbf{r}_1$. If $h_k = 3$ then from Proposition 2.5, $[\mathbf{p}^2\mathbf{r}_1] = I$, $[\mathbf{p}]$ or $[\mathbf{p}^2]$, where I is the principal ideal class. If $[\mathbf{p}^2\mathbf{r}_1] = I$, then $N(\mathbf{p}^2\mathbf{r}_1) = p^2 r \geq 2m + 3$, from Lemma 2.2. If $[\mathbf{p}^2\mathbf{r}_1] = [\mathbf{p}]$, then $[\mathbf{p}\mathbf{r}_1] = I$ and $N(\mathbf{p}\mathbf{r}_1) = pr \geq 2m + 3$, from Lemma 2.2. So $p^2 r > pr \geq 2m + 3$. If $[\mathbf{p}^2\mathbf{r}_1] = [\mathbf{p}^2]$, then $[\mathbf{r}_1] = I$ and $N(\mathbf{r}_1) = r \geq 2m + 3$, from Lemma 2.2. So $p^2 r > r \geq 2m + 3$. Thus we have proved the lemma. □

Lemma 2.7 *Let K be the simplest cubic field with conductor $D = pq$ where $p < q$ are both primes. If $h_K = 3$ then $2m + 3 = s^u$, where s is a prime and $u = 1$ or 3.*

Proof: Let s be the smallest prime factor of $2m + 3$. From Lemma 2.1, s splits and from lemma 2.2, $s^3 \geq 2m + 3$. Thus we have $2m + 3 = s, s^2, st$ or s^3, where $s < t$ are both primes. But if $2m + 3 = s^2$ then h_k is even by Lemma 2.1. So if $h_K = 3$ then $2m + 3$ should not be a square of a prime.

Now we consider the case $2m + 3 = st$, where $s < t$ are both primes. Let $s = \mathbf{s}_1\mathbf{s}_2\mathbf{s}_3$ and $t = \mathbf{t}_1\mathbf{t}_2\mathbf{t}_3$, where $\mathbf{s}_i$, $\mathbf{t}_l$ are prime ideals in K for $1 \leq i, l \leq 3$ such that $\mathbf{s}_1\mathbf{t}_1 = (\alpha+1)$, $\mathbf{s}_2\mathbf{t}_2 = (\alpha-2)$ and $\mathbf{s}_3\mathbf{t}_3 = (\alpha+m+1)$ in Lemma 2.1. From Lemma 2.2, we know that $\mathbf{s}_i$ are not principal, since $N(\mathbf{s}_i) = s < 2m+3$

for $1 \leq i \leq 3$. We claim that $[\mathbf{s}_i] \neq [\mathbf{s}_j]$ if $i \neq j$, for $1 \leq i, j \leq 3$. For example, suppose that $[\mathbf{s}_1] = [\mathbf{s}_2]$. Since $\mathbf{s}_1\mathbf{t}_1$ is principal, $\mathbf{s}_2\mathbf{t}_1$ is also principal. Note that $N(\mathbf{s}_2\mathbf{t}_1) = st = 2m + 3$. From Lemma 2.2, $\mathbf{s}_2\mathbf{t}_1 = (\gamma)$, where γ is one of the conjugates of $\alpha + 1$. This means $\mathbf{s}_2\mathbf{t}_1 = \mathbf{s}_1\mathbf{t}_1$, $\mathbf{s}_2\mathbf{t}_2$ or $\mathbf{s}_3\mathbf{t}_3$. But we easily see that it is impossible. We can also prove the other cases similarly. Thus we have $[\mathbf{s}_i] \neq [\mathbf{s}_j]$ if $i \neq j$, for $1 \leq i, j \leq 3$ and $h_k > 3$. So if $h_K = 3$, then $2m + 3$ should not be a product of two different primes.

Thus we have completely proved the lemma. □

From Lemma 2.6 and Lemma 2.7, we have the following theorem.

Theorem 2.8 *Let K be the simplest cubic fields with conductors $D = m^2 + 3m + 9 = pq$, where $p < q$ are both primes and p is not cubic residue modulo q or q is not cubic residue modulo p. If $h_K = 3$ then we have*

(i) $D = pq = (s^{2u} + 27)/4$, where s is a prime and $u = 1$ or 3.

(ii) if a prime r splits in K, then $r^3 \geq 2m + 3$ and $p^2 r \geq 2m + 3$.

Similarly we have the following theorem.

Theorem 2.8' *Let K be the simplest cubic fields with conductors $D = m^2 + 3m + 9 = 9p$, where p is a prime. If $h_K = 3$ then we have*

(i) $D = 9p = 9(s^2 + 3)/4$, where s is a prime.

(ii) if a prime r splits in K, then $r^3 \geq 2m + 3$ and $9r \geq 2m + 3$.

Remark. Theorem 2.8 (2.8') is very similar to Theorem 1 (1') in [5].

3 Determination of the simplest cubic fields of class number 3

Let k be a cyclic cubic field with conductor D. Set $l(s) = L(s, \chi)L(s, \overline{\chi})$ for $s \in \mathbb{C}$, where χ and $\overline{\chi}$ are the nontrivial cubic Dirichlet characters modulo (D) belonging to k. In [**?**]. Lettl have obtained a lower bound of $l(1)$.

Lemma 3.1 *If k is a cyclic cubic field with conductor D, then $l(1) > c_6 D^{-c_7}$, for some constants c_6, $c_7 > 0$ as notations in [?].*

From this lower bound, we have the following proposition.

Proposition 3.2 *Let K be the simplest cubic fields with conductor $D = m^2 + 3m + 9$. If $h_K = 3$ then $D \leq 25000$.*

Proof: First set $m_0 = 20000$, $\mu = 10$, $\rho = 9.9$ and $\alpha = 0.975$ as notations in [?]. Compute c_6 and c_7. Then we have

$$l(1) > 0.022 D^{-0.054} \text{ if } D > 20000.$$

Note that $4R_K < (logD)^2$, where R_K is the regulator of K ([?]). By Dirichlet's class number formular, we have

$$h_k = \frac{D \cdot l(1)}{4R_K} > \frac{0.022 \cdot D^{0.946}}{(logD)^2} \text{ if } D > 20000.$$

So if $D > 25000$ then $h_K \simeq 3.14 > 3$. Thus we have proved the proposition. □

With the help of a computer, we find that there are exactly 28 positive integers smaller than 25000 which satisfy the necessary conditions in Theorem 2.8 or Theorem 2.8': D= 63, 117, 217, 247, 279, 387, 427, 469, 559, 1899, 2169, 3199, 3789, 4039, 4167, 4699, 4837, 5707, 6169, 6649, 6979, 8197, 10107, 13579, 14527, 15507, 15757, 22959. Then, by checking tables of class numbers of cyclic cubic fields [4, table 1 2 3 4] [8, table 3], we have the following theorem.

Theorem 3.3 *There are exactly nine simplest cubic fields of class number 3: their conductors D=63, 117, 217, 247, 279, 387, 427, 469, 559.*

References

[1] N. C. Ankeny, S. Chowla and H. Hasse, *On the class-number of the maximal real subfield of a cyclotomic field*, J. Reine Angew. Math. 217 (1965), 217–220.

[2] F. Gerth III, *Sylow 3-subgroups of ideal class groups of certain cubic fields*, Thesis Princeton University, 1972.

[3] G. Gras, *Sur les l-Classes d'Idéaux dans les Extensions Cycliques Relative de Degré Premier*, Thesis, Grenoble, 1972.

[4] M.-N. Gras, *Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de* $\mathbb{Q}$, J. Reine Angew. Math., 277 (1975), 89–116.

[5] M.-G. Leu, *On a determination of certain real quadratic fields of class number two*, J. Number Theory 33 (1989) 101–106.

[6] F. Lemmermeyer and A. Pethö, *Simplest cubic fields*, Manuscripta Math. 88 (1995), 53–58.

[7] G. Lettl, *A lower bound for the class number of certain cubic number fields*, Math. Compu. 46, No. 174 (1986), 659–666.

[8] D. Shanks, *The simplest cubic fields*, Math. Compu. 28, No. 128 (1974), 1137–1152.

[9] L. C. Washington, *Class numbers of the simplest cubic fields*, Math. Compu. 48, No. 177 (1987), 371–384.

School of Mathematics, Korea Institute for Advanced Study
207-43 Cheongryangri-dong, Dongdaemoon-ku, Seoul 130-012, KOREA
E-mail address: dhbyeon@kias.re.kr