H. K. Kim and H. J. Hwang
Nagoya Math. J.
Vol. 160 (2000), 161–180

VALUES OF ZETA FUNCTIONS AND CLASS NUMBER 1 CRITERION FOR THE SIMPLEST CUBIC FIELDS

HYUN KWANG KIM[1] AND HYUNG JU HWANG

The first author dedicates this work to Professor Takashi Ono

Abstract. Let K be the simplest cubic field defined by the irreducible polynomial

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

where m is a nonnegative rational integer such that m^2+3m+9 is square-free. We estimate the value of the Dedekind zeta function $\zeta_K(s)$ at $s = -1$ and get class number 1 criterion for the simplest cubic fields.

§1. The simplest cubic fields

In this section, we review basic facts about the simplest cubic fields and give a motivation for our work.

Let m be a nonnegative integer and K_m (or simply K) be the cubic field obtained by adjoining a root of the irreducible polynomial

$$f(x) = x^3 + mx^2 - (m+3)x + 1. \tag{1.1}$$

The discriminant of the polynomial $f(x)$ is D^2, where $D = m^2 + 3m + 9$.

Let ρ be the negative root of $f(x)$. Then

$$\rho' = \frac{1}{1-\rho}, \quad \rho'' = \frac{1}{1-\rho'} = 1 - \frac{1}{\rho} \tag{1.2}$$

are the other two roots of $f(x)$, so $K = \mathbb{Q}(\rho)$ is a cyclic cubic field. The field K is called the simplest cubic field. The terminology "simplest cubic field" was first introduced by Shanks [6]. He studied the arithmetic of this family

Received March 12, 1998.
1991 Mathematics Subject Classification: 11R16, 11R42.
[1]The present studies were supported by the Basic Science Research Institute Program, Ministry of Education and Com^{2}MaC-KOSEF.

of cyclic cubic fields in the case that $D = m^2 + 3m + 9$ is a prime. Later Washington [8] extended these notions to the case that m is an integer such that $m \not\equiv 3 \pmod 9$ and studied the class number problem of these fields.

For the discriminant of the simplest cubic fields, we have:

PROPOSITION 1.1. *Let $m \not\equiv 3 \pmod 9$ and write $D = m^2 + 3m + 9 = bc^3$ with b cube-free. Then the discriminant of K_m is $(\delta \prod_{p|b} p)^2$, where $\delta = 1$ if $3 \nmid b$ and $\delta = 3$ if $3|b$.*

Proof. See [8]. □

In the case that $D = m^2 + 3m + 9$ is square-free, our information is more precise:

PROPOSITION 1.2. *Let $m \geq 0$ be an integer such that $D = m^2+3m+9$ is square-free. Then $\{1, \rho, \rho^2\}$ forms an integral basis for K and $\{-1, \rho, \rho'\}$ generates the full unit group of K.*

Proof. See [2]. □

Let h_m denote the class number of K_m. We borrow the following class number table from Shanks [6] and extend it by computing the term $2m+3$. Note that Shanks only considered the case where D is a prime.

m	h_m	$2m+3$
0	1	3
1	1	5
2	1	7
4	1	11
7	1	17
8	1	19
10	1	23
11	4	25
16	7	35
17	4	37
23	4	49
25	4	53
28	7	59

A glance of this table suggests that

(A) if $h_m = 1$, then $2m + 3$ is a prime,

and

(B) the converse of (A) is not necessarily true.

The purpose of this paper is to prove these two facts by using special values of zeta functions of the simplest cubic fields.

Our basic idea is simple and runs as follows:

> Let $\zeta_K(s)$ denote the Dedekind zeta function of K and $\zeta_K(s, C)$ be the class zeta function of K belonging to the principal ideal class of K. Then we have
>
> $$\zeta_K(2) \geq \zeta_K(2, C) \tag{1.3}$$
>
> or equivalently, by functional equation,
>
> $$\zeta_K(-1) \leq \zeta_K(-1, C), \tag{1.4}$$
>
> and the equality holds if and only if the class number of K is one. We shall compute the values of two sides of (1.4) and compare them.

For the values of class zeta functions, Halbritter and Pohst [3] developed a method of expressing special values of class zeta functions of totally real cubic fields as a finite sum involving norm, trace, and 3-fold Dedekind sums. Their result has been exploited by Byeon [1] to give an explicit formula for the values of class zeta functions of the simplest cubic fields. Using these values, Byeon proved (A).

We summarize Byeon's result as in the following theorem.

THEOREM 1.3. *Let $m \geq 0$ be an integer such that $m^2 + 3m + 9$ is square-free, K the simplest cubic field defined by the equation* (1.1)*, and C the principal ideal class of K. Then*

$$\zeta_K(-1, C) = -\frac{1}{2^3 \cdot 3^3 \cdot 5 \cdot 7} P(m),$$

where $P(m) = m^6 + 9m^5 + 55m^4 + 195m^3 + 544m^2 + 876m + 840$.

Proof. By Theorem 2.3 of [1], we have

$$\zeta_K(2,C)=\frac{\pi^6}{D^3}\left\{\frac{1}{945}m^6+\frac{1}{105}m^5+\frac{11}{189}m^4+\frac{13}{63}m^3+\frac{544}{945}m^2+\frac{292}{315}m+\frac{8}{9}\right\}.$$

We apply the functional equation to get the desired result. □

§2. Values of zeta functions of the simplest cubic fields

Using finite dimensionality of elliptic modular forms of weight h, Siegel [7] developed an ingenious method of computing $\zeta_K(b)$, where K is a totally real algebraic number field and b a negative odd integer. Siegel's formula has been exploited by Zagier [9] to give an explicit formula for the values of zeta fuctions of real quadratic fields. In this section, we apply Siegel's formula to the simplest cubic fields.

2.1. Siegel's formula and Siegel lattice

In this subsection, we introduce Siegel's formula and the notion of Siegel lattice.

We follow Zagier [9] in description of Siegel's formula. To introduce Siegel's formula, we need some preliminary notations. Let K be a totally real algebraic number field. First, we recall the definition of the different of K.

The different $\mathfrak{d}$ of K is defined to be the inverse of the fractional ideal

$$\mathfrak{d}^{-1}=\{x\in K \mid \mathrm{tr}(x\mathcal{O}_K)\subseteq\mathbb{Z}\}. \tag{2.1}$$

Here $\mathcal{O}_K$ denote the ring of integers of K. The ideal $\mathfrak{d}$ is an integral ideal and it is related to the discriminant d_K of K by the formula

$$N(\mathfrak{d})=d_K. \tag{2.2}$$

Next, for $r=0,1,2,\ldots$, we define

$$\sigma_r(n)=\sum_{d|n}d^r \quad (n=1,2,\ldots) \tag{2.3}$$

to be the sum of r-th powers of positive divisors of n. We generalize this definition to number fields by setting

$$\sigma_r(\mathfrak{a})=\sum_{\mathfrak{b}|\mathfrak{a}}N(\mathfrak{b})^r \quad (\mathfrak{a}\subset\mathcal{O}_K \text{ an ideal}). \tag{2.4}$$

Here the sum is taken over all ideals $\mathfrak{b}$ of $\mathcal{O}_K$ which divide $\mathfrak{a}$.

Finally, for $l, m = 1, 2, \ldots$, we define

$$s_l^K(2m) = \sum_{\substack{\nu \in \mathfrak{d}^{-1} \\ \nu \gg 0 \\ \mathrm{tr}(\nu) = l}} \sigma_{2m-1}((\nu)\mathfrak{d}). \tag{2.5}$$

The sum extends over all totally positive elements in $\mathfrak{d}^{-1}$ with given trace l. Note that this is a finite sum. Later we shall study this sum more precisely.

We can now state Siegel's formula.

THEOREM 2.1. (Siegel [7]) *Let $m = 1, 2, \ldots$ be a natural number, K a totally real algebraic number field of degree n, and $h = 2mn$. Then*

$$\zeta_K(1 - 2m) = 2^n \sum_{l=1}^{r} b_l(h) s_l^K(2m). \tag{2.6}$$

The numbers $r \geq 1$ and $b_1(h), \ldots, b_r(h) \in \mathbb{Q}$ depend only on h. In particular,

$$r = \dim_{\mathbb{C}} \mathfrak{M}_h, \tag{2.7}$$

where $\mathfrak{M}_h$ is the space of modular forms of weight h; thus by a well-known formula

$$r = \begin{cases} \left[\frac{h}{12}\right], & \text{if } h \equiv 2 \pmod{12}, \\ \left[\frac{h}{12}\right] + 1, & \text{if } h \not\equiv 2 \pmod{12}. \end{cases} \tag{2.8}$$

Proof. See [7] or [9]. □

Remark. Zagier [9] contains a table for the values of Siegel coefficients $b_l(h)$ for $4 \leq h \leq 40$. In our present calculation we only need $b_1(6)$ and its value is $-1/504$. If K is the simplest cubic field and $m = 1$, then $h = 6$. Therefore, by Siegel's formula, we have

$$\zeta_K(-1) = -\frac{8}{504} s_1^K(2). \tag{2.9}$$

To compute $s_l^K(2m)$, we need to analyze the finite sum in the equation (2.5).

Let K be a totally real algebraic number field of degree n and S_K (or simply S) be the set of elements in K which satisfy Siegel conditions

described in (2.5). Fix an integral basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of K. For $\nu \in K$, we can write

$$\nu = x_1\alpha_1 + \cdots + x_n\alpha_n, \quad x_i \in \mathbb{Q}. \tag{2.10}$$

Therefore we have an embedding $\phi : K \to \mathbb{R}^n$ given by

$$\phi(\nu) = (x_1, \ldots, x_n). \tag{2.11}$$

The condition $\nu \in \mathfrak{d}^{-1}$ implies that the denominator of x_i, $i = 1, 2, \ldots, n$, is bounded by $|d_K|$ where d_K is the discriminant of K. The condition $\mathrm{tr}(\nu) = l$ is equivalent to the condition that $\phi(\nu) = (x_1, \ldots, x_n)$ lies in the hyperplane

$$\mathrm{tr}(\alpha_1)x_1 + \cdots + \mathrm{tr}(\alpha_n)x_n = l \tag{2.12}$$

defined over $\mathbb{Q}$. Finally the condition $\nu \gg 0$ becomes n distinct linear inequalities (defined over K) in the variables $x_1, \ldots, x_n$. Therefore the elements $\nu \in S$ can be put in one-to-one correspondence to the lattice points in a bounded $(n-1)$-dimensional region under ϕ. We shall call this lattice (or any set which can be put in one-to-one correspondence with this set under a suitable linear transformation) as a Siegel lattice for K and denote it by $\mathfrak{S}_K$ (or simply $\mathfrak{S}$). Notice that the sum $s_l^K(2m)$ is a weighted sum of divisor functions over a Siegel lattice. Hence the description of Siegel lattice is of crucial importance in computation of $s_l^K(2m)$.

2.2. Description of Siegel lattices for the simplest cubic fields

In this subsection, we shall describe Siegel lattices for the simplest cubic fields and give a formula for the number of points in Siegel lattices.

Let $m \geq 0$ be an integer such that $D = m^2 + 3m + 9$ is square-free and K be the simplest cubic field defined by the irreducible polynomial

$$f(x) = x^3 + mx^2 - (m+3)x + 1. \tag{2.13}$$

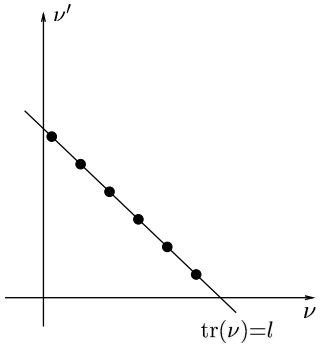
Recall that the discriminant d_K, the ring $\mathcal{O}_K$ of integers, and the different $\mathfrak{d}_K$ (cf. [5, Chap. 10, 7E]) of K are given respectively by

$$d_K = D^2 \qquad = (m^2 + 3m + 9)^2, \tag{2.14}$$

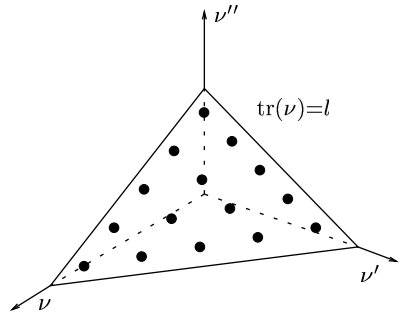
$$\mathcal{O}_K = \mathbb{Z}[\rho] \qquad = \mathbb{Z} \oplus \mathbb{Z}\rho \oplus \mathbb{Z}\rho^2, \tag{2.15}$$

$$\mathfrak{d}_K = (f'(\rho)) = (3\rho^2 + 2m\rho - (m+3)), \tag{2.16}$$

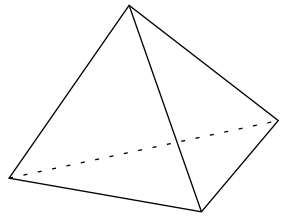
where ρ denotes the negative root of $f(x)$.



Siegel lattice for $n = 2$.



Siegel lattice for $n = 3$.



Siegel lattice for $n = 4$.

Figure 1: Siegel lattice.

Let

$$\nu = \alpha + \beta\rho + \gamma\rho^2, \quad \alpha, \beta, \gamma \in \mathbb{Q}, \tag{2.17}$$

be an element in K.

1. $\nu \in \mathfrak{d}^{-1} \Longleftrightarrow \nu \cdot \mathfrak{d} = ((3\rho^2 + 2m\rho - (m+3))\nu) \subset \mathcal{O}_K$.

Since $\nu \cdot (3\rho^2 + 2m\rho - (m+3)) \in \mathcal{O}_K$, we can write

$$\nu \cdot (3\rho^2 + 2m\rho - (m+3)) = A + B\rho + C\rho^2, \quad A, B, C \in \mathbb{Z}. \tag{2.18}$$

From (2.17), (2.18), we obtain

$$-(m+3)\alpha - 3\beta + m\gamma = A, \tag{2.19}$$

$$2m\alpha + 2(m+3)\beta + (-m^2 - 3m - 3)\gamma = B, \tag{2.20}$$

$$3\alpha - m\beta + (m^2 + 2m + 6)\gamma = C. \tag{2.21}$$

Note that the determinant of the coefficient matrix of the above linear

system is $-D^2$. Using Cramer's rule, we have

$$\alpha = \frac{a}{D},\ \ \beta = \frac{b}{D},\ \ \gamma = \frac{c}{D},\quad a, b, c \in \mathbb{Z}. \tag{2.22}$$

By substitution of (2.22) into (2.19), (2.20), (2.21), we finally have

$$-(m+3)a - 3b + mc = DA \equiv 0 \pmod{D}, \tag{2.23}$$

$$2ma + 2(m+3)b + (-m^2 - 3m - 3)c = DB \equiv 0 \pmod{D}, \tag{2.24}$$

$$3a - mb + (m^2 + 2m + 6)c = DC \equiv 0 \pmod{D}. \tag{2.25}$$

2. $\mathrm{tr}(\nu) = l \Longleftrightarrow 3\alpha + \beta\,\mathrm{tr}(\rho) + \gamma\,\mathrm{tr}(\rho^2) = l$.

From the fact that $\mathrm{tr}(\rho) = -m$, $\mathrm{tr}(\rho^2) = m^2+2m+6$ and by substitution of (2.22) into 2, we have

$$C = l, \tag{2.26}$$

and

$$b = \frac{3a + (m^2 + 2m + 6)c - lD}{m}. \tag{2.27}$$

By substitution of (2.27) into (2.23), we have

$$-a + 3l - 2c = mA. \tag{2.28}$$

In particular, m divides $a + 2c - 3l$. Put

$$t = \frac{a + 2c - 3l}{m}. \tag{2.29}$$

Since we are mainly interested in the value $\zeta_K(-1)$, from now on, we concentrate ourselves on the case $l = 1$. Thus equations (2.27), (2.29) becomes

$$b = \frac{3a + (m^2 + 2m + 6)c - D}{m}, \tag{2.30}$$

and

$$t = \frac{a + 2c - 3}{m}. \tag{2.31}$$

3. $\nu \gg 0 \Longleftrightarrow D\nu = a + b\rho + c\rho^2 \gg 0$.

This condition becomes the following three linear inequalities defined over K:

$$a + b\rho + c\rho^2 > 0, \tag{2.32}$$

$$a + b\rho' + c\rho'^2 > 0, \tag{2.33}$$

$$a + b\rho'' + c\rho''^2 > 0. \tag{2.34}$$

By substitution of (2.30), (2.31) into (2.32), (2.33), (2.34), we have

$$(\rho^2 + (m+2)\rho - 2)c + (m+3\rho)t + (3 - (m+3)\rho) > 0, \tag{2.35}$$

$$(\rho'^2 + (m+2)\rho' - 2)c + (m+3\rho')t + (3 - (m+3)\rho') > 0, \tag{2.36}$$

$$(\rho''^2 + (m+2)\rho'' - 2)c + (m+3\rho'')t + (3 - (m+3)\rho'') > 0. \tag{2.37}$$

Let l_1 (resp. l_2, l_3) denote the line in (c,t)-plane given by the left hand side of the inequality of (2.35) (resp. (2.36), (2.37)). By an actual calculation, we obtain:

$$(-\rho + \rho', 1/\rho'') \text{ is the intersection point of } l_1 = l_2 = 0, \tag{2.38}$$

$$(-\rho' + \rho'', 1/\rho) \text{ is the intersection point of } l_2 = l_3 = 0, \tag{2.39}$$

$$(-\rho'' + \rho, 1/\rho') \text{ is the intersection point of } l_3 = l_1 = 0. \tag{2.40}$$

Note that $g(x) = x^3 - Dx + D$ (resp. $h(x) = x^3 - (m+3)x^2 + mx + 1$) is the cubic polynomial whose roots are the conjugates of $-\rho + \rho'$ (resp. $1/\rho$). By applying simple plotting test on $f(x)$, we obtain

$$-m-2 < \rho < -m-1 < 0 < \rho' < 1 < \rho'' < 2. \tag{2.41}$$

Similarly, we may apply the same argument to $g(x)$ to obtain

$$\begin{aligned} -m-3 < -\rho'' + \rho < -m-2 < 1 < -\rho' + \rho'' < 2 \\ < m+1 < -\rho + \rho' < m+2, \end{aligned} \tag{2.42}$$

if $m \geq 2$. For $m = 1$, we have

$$-5 < -\rho'' + \rho < -4 < 1 < -\rho' + \rho'' < 2 < -\rho + \rho' < 3. \tag{2.43}$$

Similarly, we obtain

$$-1 < \frac{1}{\rho} < 0 < \frac{1}{\rho''} < 1 < m+2 < \frac{1}{\rho'} < m+3. \tag{2.44}$$

We summarize the above computation as in the following proposition.

PROPOSITION 2.2. *Let $m \geq 0$ an integer such that $D = m^2 + 3m + 9$ is square-free and K be the simplest cubic field defined by the irreducible polynomial* (1.1). *Let S be the set of elements in K which satisfy Siegel conditions described in* (2.5) *and $\mathfrak{S}$ be the set of integral points which lie in*

the triangle in (c,t)-plane surrounded by lines $l_1 = l_2 = l_3 = 0$. Let $\nu \in S$. By (2.22), we can write

$$\nu = \frac{a}{D} + \frac{b}{D}\rho + \frac{c}{D}\rho^2, \quad a,b,c \in \mathbb{Z}. \tag{2.45}$$

Then the map $\eta : S \to \mathfrak{S}$ given by $\eta(\nu) = (c,t)$, where

$$c = c \ \text{ and } \ t = \frac{a+2c-3}{m}, \tag{2.46}$$

gives a one-to-one correspondence between S and $\mathfrak{S}$.

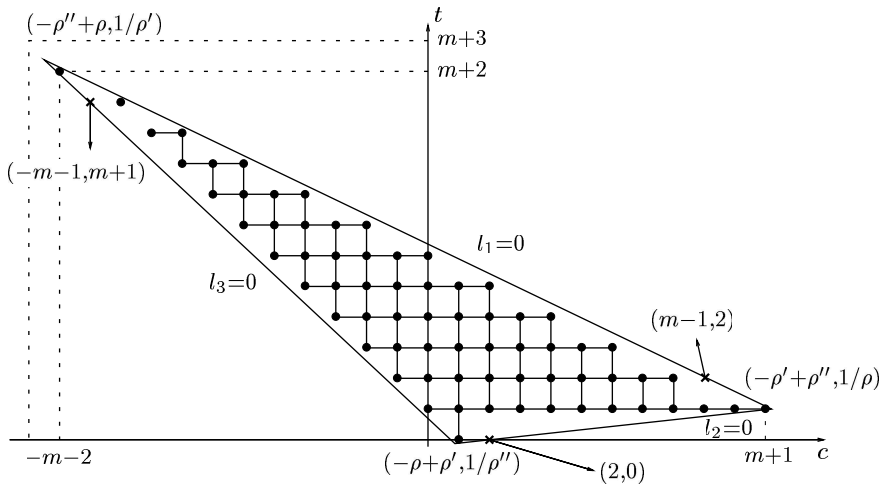


Figure 2: Siegel lattice for the simplest cubic field with $m = 10$.

EXAMPLE. As an illustration of our discussion, we describe an Siegel lattice $\mathfrak{S}$ for the simplest cubic field K with $m = 10$. First note that $(c,t) = (1,0), (-m-2, m+2), (m+1, 1)$ satisfy Siegel conditions, that is, they are inside the triangle. Next $(c,t) = (2,0), (-m-1, m+1), (m-1, 2)$ do not satisfy inequalities (2.35), (2.36), and (2.37). Therefore these points lie outside the triangle. Finally, inequalities (2.42) and (2.44) in conjunction

with (2.38), (2.39), and (2.40) give rough location of three vertices of the triangle. Combining these data, we conclude that Siegel lattice for K is given as in the Figure 2 given above.

The next simple observation gives a crucial point in understanding Siegel lattice of totally real Galois fields.

LEMMA 2.3. *Let K be a totally real Galois extension of $\mathbb{Q}$ with Galois group G. If $\nu \in K$ satisfies Siegel conditions described in* (2.5)*, then so does $\sigma(\nu)$ for $\sigma \in G$.*

Proof. This is almost clear. For example, we have

$$\begin{aligned}\nu \in \mathfrak{d}^{-1} &\Longleftrightarrow \mathrm{tr}(\nu\mathcal{O}_K) \subseteq \mathbb{Z} \Longleftrightarrow \sigma(\mathrm{tr}(\nu\mathcal{O}_K)) \subseteq \mathbb{Z} \\ &\Longleftrightarrow \mathrm{tr}(\sigma(\nu)\sigma(\mathcal{O}_K)) \subseteq \mathbb{Z} \Longleftrightarrow \mathrm{tr}(\sigma(\nu)\mathcal{O}_K) \subseteq \mathbb{Z} \\ &\Longleftrightarrow \sigma(\nu) \in \mathfrak{d}^{-1}.\end{aligned}$$

□

By Lemma 2.3, the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ acts on the set S and S can be put in one-to-one correspondence with a Siegel lattice $\mathfrak{S}$ under η. Therefore we have the induced Galois action on $\mathfrak{S}$.

Now we return to the simplest cubic fields case and describe the Galois action on $\mathfrak{S}$.

PROPOSITION 2.4. *Let $m \geq 0$ be an integer such that $D = m^2+3m+9$ is square-free and K be the simplest cubic field defined by* (1.1)*. Then the Galois group G $(= \langle\sigma\rangle)$ induces an action on $\mathfrak{S}$ given by*

$$\sigma \cdot (c, t) = (-2c - 3t + m + 3, c + t).$$

Moreover, every G-orbit contains three points. In particular, N is divisible by 3, where N is the number of lattice points in $\mathfrak{S}$.

Proof. Let $\nu \in S$. By (2.45), we can write

$$\nu = \frac{1}{D}(a + b\rho + c\rho^2), \quad a, b, c \in \mathbb{Z}.$$

By an actual computation,

$$\begin{aligned}\nu' &= \frac{1}{D}(a+b\rho'+c\rho'^2) \\ &= \frac{1}{D}\{(a+2b+(-m+2)c)+(-(m+1)b \\ &\qquad +(m^2+m+1)c)\rho+(-b+mc)\rho^2\}.\end{aligned} \tag{2.47}$$

By the transformation formula (2.46) and the equation (2.30), we have

$$\eta(\nu') = (-2c-3t+m+3, c+t). \tag{2.48}$$

Suppose $\nu = \sigma(\nu)$. Then ν is fixed also by σ^2, hence contained in $\mathbb{Q}$. Therefore $\nu = a/D,\ \ a \in \mathbb{Z}$. From the equation

$$\mathrm{tr}(\nu) = \frac{3a}{D} = 1,$$

we have $3a = D = m^2+3m+9$. It follows that $3|m$ and that $9|D$. This contradicts to the choice of m. Thus G acts on $\mathfrak{S}$ without fixed points, hence the result. □

We now come to the main result of this subsection.

THEOREM 2.5. *Let $m \geq 0$ be an integer such that $D = m^2+3m+9$ is square-free and K be the simplest cubic field defined by (1.1). Let N be the number of lattice points in $\mathfrak{S}$. Then we have*

$$N = \begin{cases} 3\cdot\left(\frac{3l^2+5l+4}{2}\right) & \text{if } m = 3l+1, \\ 3\cdot\left(\frac{3l^2+7l+6}{2}\right) & \text{if } m = 3l+2. \end{cases}$$

Proof. We only give the detailed proof for the case $m = 3l+1$. The basic idea of proof is to find a set of representatives of "good" shape of the Galois action on $\mathfrak{S}$. First note that $(c,t) = (1,0)$ is the only lattice point in $\mathfrak{S}$ with $t = 0$ and $\sigma\cdot(1,0) = (m+1,1)$, $\sigma^2\cdot(1,0) = (-m-2, m+1)$. Let L_1 denote the set of lattice points which lie on the straight line from $(m+1,1)$ to $(2,1)$. By an actual computation, we can see that $\sigma\cdot L_1$ is the set of lattice points which lie on the straight line from $(-m-2, m+2)$ to $(m-4,3)$ and $\sigma^2\cdot L_1$ is the set of lattice points which lie on the straight line from $(1,0)$ to $(-m+2, m-1)$ (See Figure 3 below). Similarly, for

$1 \le k \le l+1$, let L_k denote the set of lattice points lying on the straight line from $(3(l+1-k)+2, k)$ to $(2, k)$. Then $\sigma \cdot L_k$ becomes the set of lattice points lying on the straight line from $(-3(l+2-k), 3(l+1-k)+2+k)$ to $(3(l-k), 2+k)$ and $\sigma^2 \cdot L_k$ becomes the set of lattice points lying on the straight line from $(1, k-1)$ to $(-3(l-k)-2, 3(l-k)+2+k)$. Finally, let L_{l+2} denote the point $(1, l+1)$. Then $\sigma \cdot L_{l+2} = (-1, l+2)$ and $\sigma^2 \cdot L_{l+2} = (0, l+1)$. This proves that $\mathfrak{S}_0 := \bigcup_{k=1}^{l+2} L_k$ forms a set of representatives of Galois action on $\mathfrak{S}$ (See Figure 4 below). Now, by an easy calculation, the number of lattice points in $\mathfrak{S}_0$ becomes

$$\sum_{k=1}^{l+1}(3(l+1-k)+1)+1 = \frac{3l^2+5l+4}{2}.$$

Therefore we have

$$N = \frac{3(3l^2+5l+4)}{2}.$$

□

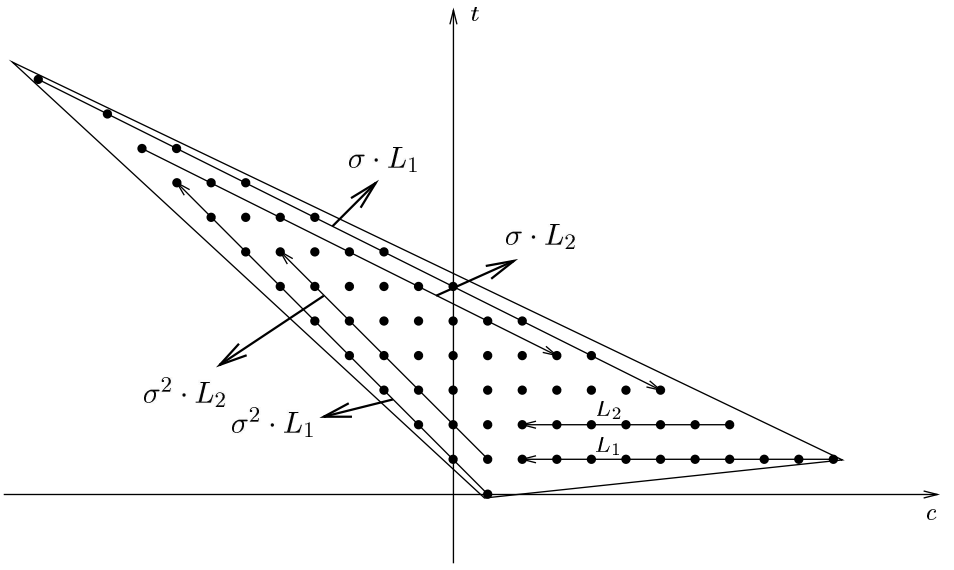


Figure 3: Galois action on $\mathfrak{S}$.

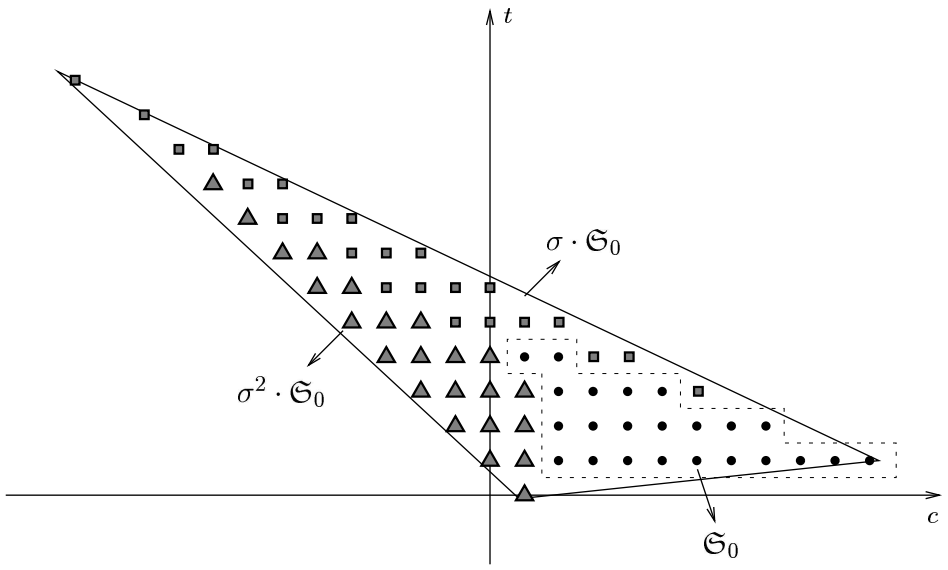


Figure 4: A set of representatative of the Galois action on $\mathfrak{S}$.

2.3. Estimation for $\sigma_1((\nu)\mathfrak{d})$

In this subsection, we introduce a new arithmetic function ψ defined on integral ideals of $\mathcal{O}_K$ and study some properties of ψ. Finally, we give a lower bound for $\sigma_1((\nu)\mathfrak{d})$.

For an integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we define an arithmetic function ψ as follows:

$$\psi(\mathfrak{a}) = \sigma_1(N_{K/\mathbb{Q}}(\mathfrak{a})), \tag{2.49}$$

where σ_1 on the right hand side of (2.49) denote the divisor function on $\mathbb{Z}$ defined by (2.3). Since $K/\mathbb{Q}$ is a cyclic Galois extension of degree 3, we can devide prime ideals of K into three types: Type I (resp. Type II, Type III) prime is a prime ideal which lies over a rational prime p which splits complitely (resp. ramified, remains prime) in $K/\mathbb{Q}$.

LEMMA 2.6. (i) *Let $\mathfrak{p}$ be a prime ideal of K of Type I or Type II. Then, for any $n \geq 0$, we have*

$$\sigma_1(\mathfrak{p}^n) = \psi(\mathfrak{p}^n). \tag{2.50}$$

(ii) *Let* $\mathfrak{a}$, $\mathfrak{b}$ *be ideals of* K. *Then we have*

$$\psi(\mathfrak{ab}) \leq \psi(\mathfrak{a})\psi(\mathfrak{b}), \tag{2.51}$$

and equality holds in (2.51) *if and only if* $N_{K/\mathbb{Q}}(\mathfrak{a})$, $N_{K/\mathbb{Q}}(\mathfrak{b})$ *are relatively prime.*

(iii) *Let* $\mathfrak{a}$ *be an ideal of* K *which does not contain a prime ideal of Type III in its prime factorization. Then we have*

$$\sigma_1(\mathfrak{a}) \geq \psi(\mathfrak{a}) \tag{2.52}$$

and equality holds in (2.52) *if and only if* $\mathfrak{a}$ *satisfies the following condition*:

(∗) $\mathfrak{a}$ *does not contain two prime ideals of Type I in its prime factorization which lie over the same rational prime.*

Proof. (i) By abuse of notation, for an integral ideal $\mathfrak{a}$, we denote $N_{K/\mathbb{Q}}(\mathfrak{a})$ by $N(\mathfrak{a})$. Since $\mathfrak{p}$ is a prime ideal of Type I or Type II, $N(\mathfrak{p}) = p$ is a rational prime. Therefore, we have

$$\sigma_1(\mathfrak{p}^n) = \sum_{\mathfrak{b}|\mathfrak{p}^n} N(\mathfrak{b}) = \sum_{i=0}^{n} N(\mathfrak{p}^i) = \sum_{i=0}^{n} p^i = \sigma_1(p^n) = \psi(\mathfrak{p}^n).$$

(ii) Note that, for any positive integers m and n, we have

$$\sigma_1(m \cdot n) \leq \sigma_1(m) \cdot \sigma_1(n) \tag{2.53}$$

with equality holds if and only if $(m, n) = 1$. Therefore we have

$$\begin{aligned} \psi(\mathfrak{ab}) &= \sigma_1(N(\mathfrak{ab})) \\ &= \sigma_1(N(\mathfrak{a})N(\mathfrak{b})) \\ &\leq \sigma_1(N(\mathfrak{a})) \cdot \sigma_1(N(\mathfrak{b})) \\ &= \psi(\mathfrak{a}) \cdot \psi(\mathfrak{b}), \end{aligned}$$

and the equality holds if and only if $(N(\mathfrak{a}), N(\mathfrak{b})) = 1$.

(iii) Let

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}, \quad \mathfrak{p}_i \text{ a prime ideal of Type I or Type II,}$$

be a factorization of $\mathfrak{a}$ into the product of distinct prime ideals of K. Since σ_1 is mutiplicative on K, we have

$$\begin{aligned}\sigma_1(\mathfrak{a}) &= \sigma_1(\mathfrak{p}_1^{r_1})\cdots\sigma_1(\mathfrak{p}_k^{r_k}) \\ &= \psi(\mathfrak{p}_1^{r_1})\cdots\psi_1(\mathfrak{p}_k^{r_k}) \qquad \text{(by (i))} \\ &\geq \psi(\mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_k^{r_k}) \qquad \text{(by (ii))} \\ &= \psi(\mathfrak{a}).\end{aligned}$$

Here the equality holds if and only if $N(\mathfrak{p}_i^{r_i})$ and $N(\mathfrak{p}_j^{r_j})$ are relatively prime for any distinct pair of i, j, or equivalently, $\mathfrak{a}$ satisfies the condition $(*)$. □

Let ν be an element in K which satisfies Siegel's conditions. Then, by (2.18), $(\nu)\mathfrak{d}$ is the principal ideal generated by $A + B\rho + C\rho^2$ with $A, B, C \in \mathbb{Z}$. Furthermore, by (2.26), we have $C = l$. Since we are mainly interested in the value $\zeta_K(-1)$, we have assumed that $l = 1$. Therefore the ideal $(\nu)\mathfrak{d}$ satisfies the condition of Lemma 2.6 (iii). By applying Lemma 2.6, we have

$$\sigma_1((\nu)\mathfrak{d}) \geq \psi((\nu)\mathfrak{d}) = \sigma_1(N_{K/\mathbb{Q}}((\nu)\mathfrak{d})). \tag{2.54}$$

By an easy calculation, for $a, b, c \in \mathbb{Q}$, we have

$$\begin{aligned}N_{K/\mathbb{Q}}(a + b\rho + c\rho^2) &= a^3 - b^3 + c^3 - ma^2b - (m+3)ab^2 + (m^2+2m+6)a^2c \\ &\quad + (m^2+4m+9)ac^2 + mb^2c + (m+3)bc^2 \\ &\quad + (m^2+3m+3)abc.\end{aligned} \tag{2.55}$$

By (2.22), we can write

$$\nu = \frac{1}{D}(a + b\rho + c\rho^2), \quad a, b, c \in \mathbb{Z}. \tag{2.56}$$

By (2.2) and (2.55), we have

$$\begin{aligned}N_{K/\mathbb{Q}}((\nu)\mathfrak{d}) &= N_{K/\mathbb{Q}}(\nu)\cdot N_{K/\mathbb{Q}}(\mathfrak{d}) \\ &= \frac{1}{D}\{a^3 - b^3 + c^3 - ma^2b - (m+3)ab^2 + (m^2+2m+6)a^2c \\ &\quad + (m^2+4m+9)ac^2 + mb^2c + (m+3)bc^2 \\ &\quad + (m^2+3m+3)abc\}.\end{aligned} \tag{2.57}$$

Now, by (2.30), we may replace b by $(3a+(m^2+2m+6)c-D)/m$ and we have

$$
\begin{aligned}
(2.58)\quad N_{K/\mathbb{Q}}((\nu)\mathfrak{d}) = \frac{1}{m^3}\{&-(2m+3)a^3-3(m^2+4m+6)a^2c\\
&-(m^3+9m^2+24m+36)ac^2-(m^3+6m^2+16m+24)c^3\\
&+(m+3)Da^2+(m^2+4m+12)Dac+(m^2+4m+12)Dc^2\\
&-D^2a-2D^2c+D^2\}.
\end{aligned}
$$

Finally, by (2.31), we may replace a by $-2c+mt+3$ in (2.58), and we obtain

$$
N_{K/\mathbb{Q}}((\nu)\mathfrak{d}) = f_m(c,t), \tag{2.59}
$$

where

$$
\begin{aligned}
(2.60)\quad f_m(c,t) = &[t^2+(c-1)t]m^2\\
&+[-2t^3+(-3c+6)t^2+(-c^2+3c)t+(-c^2+3c-2)]m\\
&+[-3t^3+(3c^2-9c+9)t+(c^3-6c^2+9c-3)].
\end{aligned}
$$

We summarize this result as in the following theorem.

THEOREM 2.7. *Let S be the set of elements in K which satisfy Siegel conditions described in* (2.5) *and $\nu \in S$. Then we have*

$$
\sigma_1((\nu)\mathfrak{d}) \geq \sigma_1(f_m(c,t)), \tag{2.61}
$$

where (c,t) is a point in $\mathfrak{S}$ which corresponds to ν under the correspondence of Proposition 2.2 *and $f_m(c,t)$ is given by the formula* (2.60). *The equality holds in* (2.61) *if and only if the ideal $(\nu)\mathfrak{d}$ satisfies the condition $(*)$.*

§3. Class number 1 criterion for the simplest cubic fields

In this section, as an application of our method, we derive a class number 1 criterion for the simplest cubic fields. We also discuss further problems.

THEOREM 3.1. *Let m be a nonnegative integer such that $D = m^2+3m+9$ is square-free and K be the simplest cubic field defined by* (1.1). *Then we have*

$$
\begin{aligned}
&h_K = 1 \text{ if and only if } f_m(c,t) \text{ is a prime for}\\
&(c,t) \in \mathfrak{S} - \{(1,0),(m+1,1),(-m-2,m+2)\}.
\end{aligned} \tag{3.1}
$$

Proof. We only give the proof for the case $m = 3l + 1 \equiv 1 \pmod 3$. By Siegel's formula (2.9), we have

$$\zeta_K(-1) = -\frac{8}{504} s_1^K(2) = -\frac{8}{504} \sum_{\nu \in S} \sigma_1((\nu)\mathfrak{d}).$$

By Theorem 2.7, we have

$$\zeta_K(-1) \le -\frac{8}{504} \sum_{(c,t)\in\mathfrak{S}} \sigma_1(f_m(c,t)), \tag{3.2}$$

and equality holds in (3.2) if and only if $(\nu)\mathfrak{d}$ satisfies the condition $(*)$ for all $\nu \in S$. From (2.59), we can easily see that

$$f_m(c,t) = f_m(\sigma \cdot (c,t)), \tag{3.3}$$

for all $(c,t) \in \mathfrak{S}$. Therefore, (3.2) becomes

$$\begin{aligned} \zeta_K(-1) &\le -\frac{8}{504} \cdot 3 \cdot \sum_{(c,t)\in\mathfrak{S}_0} \sigma_1(f_m(c,t)) \\ &\le -\frac{24}{504} \left\{ \sum_{(c,t)\in\mathfrak{S}_0} 1 + \sum_{(c,t)\in\mathfrak{S}_0 - \{(m+1,1)\}} f_m(c,t) \right\}. \end{aligned} \tag{3.4}$$

(Note that $f_m(m+1,1) = 1$.) The equality holds in (3.4) if and only if $f_m(c,t)$ is a prime for all $(c,t) \in \mathfrak{S}_0 - \{(m+1,1)\}$. Recall that $\mathfrak{S}_0 = \bigcup_{k=1}^{l+2} L_k$ (see Figure 4). The formula (3.4) becomes

$$\begin{aligned} &-\frac{24}{504} \left\{ \sum_{(c,t)\in\mathfrak{S}_0 - \{(m+1,1)\}} 1 + \sum_{(c,t)\in\mathfrak{S}_0} f_m(c,t) \right\} \\ &= -\frac{24}{504} \left\{ \frac{3l^2+5l+2}{2} + f_m(1,l+1) + \sum_{t=1}^{l+1} \sum_{c=2}^{3(l+1-t)+2} f_m(c,t) \right\} \\ &= -\frac{24}{504} \cdot \frac{1}{360} (m^6 + 9m^5 + 55m^4 + 195m^3 + 544m^2 + 876m + 840) \\ &\quad \text{(We checked this result by Maple II)} \\ &= -\frac{1}{2^3 \cdot 3^3 \cdot 5 \cdot 7} P(m) \\ &= \zeta_K(-1, C), \end{aligned}$$

where C denote the principal ideal class of K.

This proves that

$$\zeta_K(-1) \leq \zeta_K(-1, C) \tag{3.5}$$

and, by (3.2), (3.4), the equality holds in (3.5) if and only if $f_m(c,t)$ is a prime for all $(c,t) \in \mathfrak{S} - \{(1,0), (m+1,1), (-m-2, m+2)\}$ and $(\nu)\mathfrak{d}$ satisfies the condition $(*)$ for all $\nu \in S$. Now suppose that $f_m(c,t)$ is a prime for all $(c,t) \in \mathfrak{S} - \{(1,0), (m+1,1), (-m-2, m+2)\}$. Then, by (2.59), $(\nu)\mathfrak{d}$ is a prime ideal, hence it satisfies the condition $(*)$. Therefore we conclude that

$$\begin{aligned} h_K = 1 &\Longleftrightarrow \text{equality holds in (3.5)} \\ &\Longleftrightarrow f_m(c,t) \text{ is a prime for all} \\ &\qquad (c,t) \in \mathfrak{S} - \{(1,0), (m+1,1), (-m-2, m+2)\}. \end{aligned}$$

□

Remark 1. (i) Note that $f_m(0,1) = 2m+3$. Therefore Theorem 3.1 says the condition that $2m+3$ is a prime is a necessary condition for $h_K = 1$. This proves (A) in Section 1.

(ii) For $m = 17$, $f_m(0,1) = 37$ is a prime. Note that $f_m(0,2) = 671 = 11 \cdot 61$ is not a prime. Therefore the condition that $2m+3$ is a prime is not a sufficient condition for $h_K = 1$. This proves (B) in Section 1.

Remark 2. Let K, m be as in Theorem 3.1. Then, by (2.14), the discriminant d_K of K is given as follows:

$$d_K = D^2 = (m^2 + 3m + 9)^2.$$

By the genus theory for cyclic cubic fields (see, for example, [6, Section 7]), $h_K = 1$ implies that d_K has only one prime factor. Therefore, from Theorem 3.1, we can conclude that

$$\begin{aligned} &f_m(c,t) \text{ is a prime for all } (c,t) \in \mathfrak{S} - \{(1,0), (m+1,1), (-m-2, m+2)\} \\ &\quad \Longrightarrow D = m^2 + 3m + 9 \text{ is a prime.} \end{aligned}$$

Can we prove this in an elementary way?

Remark 3. In [4], using a lower bounds for $L(1,\chi) \cdot L(1,\bar{\chi})$ for certain cubic charater, Lettl had showed:

$m = -1, 1, 2, 4, 7, 8, 10$ gives all the values of m such that $h_K = 1$.

From Theorem 3.1 and Lettl's result, we can conclude that:

> if $m \geq 11$ and $m^2 + 3m + 9$ is square-free, then $f_m(c,t)$ is not a prime for some $(c,t) \in \mathfrak{S} - \{(1,0), (m+1,1), (-m-2, m+2)\}$.

Can we prove this in an elementary way?

References

[1] D. Byeon, *Special values of zeta functions of the simplest cubic fields and their applications*, Proc. Japan Acad., Ser. A, **74** (1998), 13–15.

[2] T. Cusick, *Lower bounds for regulators*, Number theory (Noordwijkerhout, 1983), Lecture Notes in Math. Vol. 1068, Springer-Verlag, Berlin and NewYork (1984), pp. 63–73.

[3] U. Halbtitter and M. Phost, *On the computation of the values of zeta functions of totally real cubic fields*, J. Number Theory, **36** (1990), 266–288.

[4] G. Lettl, *A lower bound for the class number of certain cubic number fields*, Math. Comp., **46** (1986), 659–666.

[5] P. Ribenboim, Algebraic Numbers, Jhon Wiley, NewYork, 1972.

[6] D. Shanks, *The simplest cubic fields*, Math. Comp., **28** (1974), 1137–1152.

[7] C. L. Siegel, *Berechnung von Zetafuncktionen an ganzzahligen Stellen*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Klasse, **10** (1969), 87–102.

[8] L. C. Washington, *Class numbers of the simplest cubic fields*, Math. Comp., **48** (1987), 371–384.

[9] D. B. Zagier, *On the values at negative integers of the zeta function of a real quadratic field*, Enseig. Math., **22** (1976), 55–95.

Hyun Kwang Kim
Department of Mathematics
Pohang University of Science and Technology
San 31 Hyoja Dong
Pohang, 790-784
Korea
hkkim@postech.ac.kr

Hyung Ju Hwang
Department of Mathematics
Brown University
Providence, RI 02912
U.S.A.
hjhwang@math.brown.edu