Trends in Mathematics
Information Center for Mathematical Sciences
Volume 1, Number 1, September 1998, Pages 46–51

RECENT RESULTS ON ARITHMETIC OF THE SIMPLEST CUBIC FIELDS

HYUN KWANG KIM

Abstract. The purpose of this paper is to survey recent results on arithmetic properties of the simplest cubic fields. First, we introduce the notion of the simplest cubic fields and develop basic materials. Next, we shall discuss arithmetic of the simplest cubic fields such as computation of class number, class number problem, computation of special values of zeta function, and structure of ideal class group.

Let K be an algebraic number field and O_K be the ring of algebraic integers of K. One of the main theme of algebraic number theory is to study arithmetic properties (structure of unit group, class number, structure of ideal class group, etc) of the ring O_K. If we classify algebraic number fields by their extension degree, quadratic fields are the simplest object except the field of rationals $\mathbb{Q}$. In fact, there were intensive studies for arithmetic proprerties of quadratic fields after Gauss. As a result, we accumulate lots of information about arithmetic of quadratic fields. Maybe cubic fields are next target to study after the study of quadratic fields. For the case of cubic fields, the situation is totally different. Very little is known to us about arithmetic of cubic fields and the study of arithmetic of general cubic field is too difficult to attack at this moment. To overcome this difficulty, Shanks [5] introduced the notion of the simplest cubic fields in 1974 and studiesd arithmetic of these fields. In this paper, we shall review basic properties of the simplest cubic fields and will survey recent results about arithmetic of the simplest cubic fields.

1. Simplest Cubic Fields

In this section, we shall introduce the notion of the simplest cubic fields and develop basic proprties. Let $m(\geq -1)$ be an integer such that $m \not\equiv 3 \pmod 9$ and consider the polynomial

$$f(X) = X^3 + mX^2 - (m+3)X + 1 \tag{1}$$

which is irreducible over $\mathbb{Q}$. Then the discriminant of f(X) is given by

$$D^2 = (m^2 + 3m + 9)^2. \tag{2}$$

Note that $D \not\equiv 0 (\mathrm{mod} 27)$ since $m \not\equiv 3 (\mathrm{mod}\ 9)$. Let ρ be the negative root of f(X). Then $\rho' = 1/(1-\rho)$ and $\rho'' = 1 - 1/\rho$ are the other roots of f(X). Hence K=$\mathbb{Q}(\rho)$ is

1991 *Mathematics Subject Classification.* 11R16, 11R42.
Key words and phrases. Simplest cubic fields, Dedekind zeta function, class number formula, p-adic claass number formula, elliptic curve, 2-rank of ideal class group.

a totally real cyclic cubic field. K is called a simplest cubic field and the arithmetic of this field was studied in [5],[6]. Since

$$-m-2<\rho<-m-1<0<\rho'<1<\rho''<2, \tag{3}$$

all eight combinations of signs are obtained from the units and their conjugates. From this, we know that every totally positive unit is a square. For the discriminant, ring of integers, and unit group of K, we have the following result. For a proof, we refer [6].

Theorem A. Let $m \not\equiv 3(\mathrm{mod}9)$ and $D = m^2+3m+9 = bc^3$ with b cube-free. Then the discriminant d_K of K is given by

$$d_K = (\delta \prod_{p|b} p)^2, \tag{4}$$

where $\delta = 1, 3$ according as $3 \nmid b$ or not.

Theorem B. Suppose $D = m^2+3m+9$ is square -free,then $\{1, \rho, \rho'\}$ forms an integral basis for K, and $\{-1, \rho, \rho'\}$ generates the unit group of K.

2. The class numbers of the simplest cubic fields

In this section, we shall develop two ways of computing class numbers of the simplest cubic fields which corresponds to m with $D = m^2+3m+9$ is a prime.

D.Shanks's method: Let $(m \geq -1)$ be an integer such that $D = m^2+3m+9$ is a prime , and let K be the simplest cubic field corresponds to m. The regulator R of K is given by

$$R = log^2(-\rho) - log(-\rho)log(1-\rho) + log^2(1-\rho). \tag{5}$$

Let $\zeta_K(s)$ denote the Dedekind zeta function of K. By Euler product expansion, we have

$$\zeta_K(s) = \prod_p \prod_{\wp|p} \frac{1}{1-(N\wp)^{-s}}, \tag{6}$$

where p runs over all rational primes. The Riemann zeta function $\zeta(s)$ is given by

$$\zeta(s) = \prod \frac{1}{1-p^{-s}}, \tag{7}$$

where p runs over all rational primes. Note that

$$\prod_{\wp|p} \frac{1}{(1-N\wp)^{-s}} = \begin{cases} \dfrac{1}{1-p^{-s}} & \text{if } p \text{ is ramified in } \mathrm{K}/\mathbb{Q}, \\ \dfrac{1}{(1-p^{-s})^3} & \text{if } p \text{ splits in } \mathrm{K}/\mathbb{Q}, \\ \dfrac{1}{1-p^{-3s}} & \text{if } p \text{ remains prime in } \mathrm{K}/\mathbb{Q}. \end{cases} \tag{8}$$

It follows from (6),(7),and (8) that

$$\lim_{s\to 1^+} \frac{\zeta_K(s)}{\zeta(s)} = \prod_p g(p), \tag{9}$$

where

$$g(p) = \begin{cases} 1 & \text{if} \quad \text{p=D}, \\ (\dfrac{p}{p-1})^2 & \text{if} \quad p^{\frac{p-1}{3}} \equiv 1 \pmod{\text{D}}, \\ \dfrac{p^2}{p^2+p+1} & \text{otherwise.} \end{cases} \tag{10}$$

On the other hand, we have from class number formula that

$$\lim_{s \to 1^+} \frac{\zeta_K(s)}{\zeta(s)} = \frac{4Rh}{D}, \tag{11}$$

where h is the class number of K. From (9),(10),and (11), we have

$$h = \frac{D}{4R} \prod_p g(p). \tag{12}$$

Since we know R, we may compute the class number h from (12) by calculat ing the infinite product on the right hand side of (12) with sufficient accuracy.

Kim and Kim's method:(Caution:In this subsection, p will denote the prime m^2+3m+9, which is denoted by D in the previous subsection.) Since K is a totally real field, we may apply p-adic class number formula to obtain a congruence relation for class number of the simplest cubic fields. As a result, we get

$$4h \equiv -27 B_{\frac{p-1}{3}} B_{\frac{2(p-1)}{3}} (\text{mod p}), \tag{13}$$

where B_n denote the n-th Bernoulli number. We remark that (13) may be considered as a cubic analogue of the famous Ankeny-Artin-Chowla's theorem which gives a congruence relation for the class numbers of real quadratic fields. By a suitable estimation of the value $L(1,\chi)$,where χ is the cubic character associated to K, we can obtain an upper bound for h, namely,

$$h < p. \tag{14}$$

Note that (13) and (14) determine the class number h.

Example Consider the simplest cubic field with m=11. In this case p=163. By (13),

$$h \equiv -\frac{27}{4} B_{54} B_{108} \equiv \frac{-27*69*58}{4*146*118} \equiv 4 (\text{mod} 163).$$

Since $h < 163$ by (14), we conclude that

3. Class number problem for the simplest cubic fields

We can formulate class number problem for the simplest cubic fields as follows:

Given (small) natural number l, find all the values of m
(or, equivalently, the values of conductor $D = m^2+3m+9$)
such that $h_m = l$, where h_m denotes the class number of
the simplest cubic field associated to m.

This gives us 'proper' (not very easy, and not very difficult) problem. We state two results in this line without proofs. For a proof, we refer [1],[4].

Theorem C (Lettl) There are exactly 7 simplest cubic fields of class number 1 and their conductors (resp. corresponding values of m) are
D=7,13,19,37,79,97,139 (resp. m=-1,1,2,4,7,8,10).

Theorem D (Byeon) There are exactly 5 simplest cubic fields of class number 3 and their conductors (resp. corresponding values of m) are
D=217,247,427,469,559 (resp. m=13,14,19,20,22).

4. Values of zeta functions

Let K be a number field and $\zeta_K(s)$ be the Dedekind zeta function of K. The function $\zeta_K(s)$ contains many arithmetic information of K and it is of great important in number theory. If K is a real quadratic field, there is a method of computing special values of a partial zeta function $\zeta_K(s, A)$, where A is an ideal class of K, and that of the Dedekind zeta function $\zeta_K(s)$. This results stimulate us to attempt to the problem of evaluating special values of zeta function of the simplest cubic fields. In this section, we state results about special values of zeta functions of the simplest cubic fields without proofs. We refer [2] for a proof.

Theorem E.Let K be the simplest cubic field associated to m, and C be the principal ideal class of K. Then

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

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

Using finite dimensionality of elliptic modular forms of given weight, Siegel developed a method of expressing special value $\zeta_K(b)$, where K is a totally real algebraic number field and b is a negative odd integer, as a finite weighted sum of divisor function over the Siegel lattice for K. Therefore, to apply Siegel's formula for a totally real number field K, we need to know

(i) number of lattice points on the Siegel lattice for K,
(ii) the method of evaluating divisor function which is defined on the ideals of O_K.

For the simplest cubic fields, we have

Theorem F Let K be the simplest cubic field associated to m. Then
(a)we can count the number of lattice points in the Siegel lattice for K,
(b)we can find a lower bound for the divisor function on K.

As a consequence, we obtain

$$\zeta_K(-1) \leq -\frac{1}{504} \sum_{(c,t) \in S} \sigma_1(f_m(c, t)),$$

where S denote a set of representatives of the Siegel lattice for K and $f_m(c, t)$ is a polynomiaal defined on S given by

$$f_m(c, t) = [t^2 - (c-1)t]m^2 + [-2t^3 + (-3c+6)t^2 + (-c^2+3c)t + (-c^2+3c-2)]m$$

$$+[-3t^3+(3c^2-9c+9)t+(c^3-6c^2+9c-3)].$$

5. Structure of ideal class groups

The topic which will be discussed in this section is more difficult than the topics in previous sections. In this section, we first state basic theorems which are useful in determining the structure of ideal class groups of the simplest cubic fields. Next, we suggest a method of using elliptic curves to investigate the structure of 2-part(or 3-part) of ideal class group. The reference for this section is [5],[6].

Theorem G. If p is a prime which is a congruent to 2 mod3, then p-rank of the ideal class group of a cyclic cubic field must be even.

Example. Consider the case of m=11. From section 2, h=4. By theotem G,

$$C(K) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Theorem H. Let $n \geq 2$ be an integer. Let $x, y \in \mathbb{Q}$,and suppose

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

If D is not cube-free, we also assume that the g.c.d. of the numerator of x^2-x+1, the numerator of y, and c (defined in theorem A) is 1. If n$\not\equiv$ 0 (mod3) or if $x \in \mathbb{Z}$, then the principal ideal $(x-\rho)$ is the n-th power of an ideal of K. If $x \notin \mathbb{Z}$ and $n \equiv 0(\text{mod}3)$, it is the (n/3)rd power of an ideal.

2-part of the ideal class group of K: Let E be an elliptic curve defined over $\mathbb{Q}$ by an equation.

$$E : Y^2 = X^3 + mX^2 - (m+3)X + 1.$$

Let C be the ideal class group of K and let $C_2 = \{x \in C / x^2 = 1\}$ denote the 2-part of C. Finally, let E^o be the connected component of $E(\mathbb{R})$ containing O.

Theorem I. There are exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & E^o(\mathbb{Q})/2E(\mathbb{Q}) & \longrightarrow & C_2 & \longrightarrow & Ш_2 & \longrightarrow & 1, \\ 1 & \longrightarrow & \{1,-\rho\}(K^*)^2/(K^*)^2 & \longrightarrow & S_2 & \longrightarrow & C_2 & \longrightarrow & 1, \end{array}$$

where S_2, $Ш_2$ denote the 2-Selmer group, 2-Tate-Shafarevich group of E,respectively. In particular, we have

$$rank E(\mathbb{Q}) \leq 1 + rk_2(C_2).$$

3-part of the ideal class group of K: Let K be a cyclic cubic field. Let r_3 be the 3-rank of C(K) and k denote the number of rational primes which are ramified in K/$\mathbb{Q}$. Then, from the genus theory for cyclic cubic fields, we have

$$k-1 \leq r_3 \leq 2(k-1). \tag{15}$$

Remark. If k is large, the ineqquality (15) is not sufficient to study the 3-part of C(K). To study 3-part of ideal class groups using elliptic curve, we need to find an elliptic curve E defined over $\mathbb{Q}$ whose 3 division points are K-rational, i.e., $\mathbb{Q}(E[3]) = K$. For a simplest cubic field K, we remark that the elliptic curve

$$E : Y^3 = X^3 + mX^2 - (m+3)X + 1$$

satisfies the conditions.

References

[1] D.Byeon,"Class number 3 problem for the simplest cubic fields," preprint.
[2] H.K.Kim and H.J.Hwang,"Values of zeta functions and class number 1 criterion for the simplest cubic fields", preprint.
[3] H.K.Kim and J.S.Kim, "Computation of class numbers of the simplest cubic fields",preprint
[4] G.Lettl," A lower bound for the class number of certain cubic number fields", Math. Comp. 46 (1986), 659-666.
[5] D.Shanks," The Simplest Cubic Fields", Math.Comp.(1974),1137-1152.
[6] L.C.Washington,"Class Numbers of the Simplest Cubic Fields", Math. Comp. 48 (1987), 371-384.

Department of Mathematics, Pohang University of Science and Technology, Pohang,, 790-784,Korea
E-mail address: h.k.kim@euclid.postech.ac.kr