Nakano, S.
Osaka J. Math.
25 (1988), 161-170

CONSTRUCTION OF PURE CUBIC FIELDS WITH LARGE 2-CLASS GROUPS

SHIN NAKANO

(Received November 18, 1986)

Introduction

In [5], the author showed the existence of infinitely many pure number fields of any given odd degree $n(\geqq 3)$ whose ideal class groups have 2-rank at least $3\Delta_n$, where Δ_n is the number of divisors of n which are smaller than n. This result was approached via Diophantine equations of the type $Y^2=X^n+D$, which was also applied to the research on "n-rank" of the ideal class groups of quadratic fields (Yamamoto [9], Craig [1], [2]). Particularly, in case $n=3$, Craig gave one of the ways to generate the elliptic curves given by $Y^2=4X^3+D$ possessing suitably many integral points, and utilized it to obtain a precise result on 3-rank of the ideal class groups of quadratic fields.

The aim of the present paper is to apply Craig's elliptic curves to the proof of a 2-rank theorem on pure cubic fields. We shall namely show the following

Theorem. *There exist infinitely many pure cubic fields whose ideal class groups have 2-rank at least* 6.

This theorem is stronger than the above result of [5] in case $n=3$, because $\Delta_3=1$. The proof is given by the method largely due to Craig [2]. To check some results of Craig and to calculate the various numerical values, one can make effective use of an electric computer. In particular, the computer algebra system REDUCE was suited to our purpose (cf. [3]). REDUCE has been implemented on the M680H computer at the Computer Centre University of Tokyo, and able to be utilized at the Gakushuin University Computer Centre (GUCC), by way of the computer network N1. The calculations in Section 3 were carried out by FORTRAN on the COSMO800 III computer at GUCC. The author would like to thank the staff of GUCC for their assistance given to him during the work for the paper. Thanks are also due to Professor H. Wada who kindly supplied valuable information about calculations of larger numbers.

1. Craig's elliptic curves

In this section, we summerize Craig's result on the integer solutions of $Y^2=4X^3+D$. For details, refer to [2].

We start with the symmetric polynomial in X, Y, Z;

$$\begin{aligned} D(X, Y, Z) &= (X^2+Y^2+Z^2)-2(XY+YZ+ZX) \\ &= (-X+Y+Z)^2-4YZ = (X-Y+Z)^2-4ZX=(X+Y-Z)^2-4XY\,. \end{aligned}$$

From these three expressions, we obtain the three points

$$(yz,\ -x^3+y^3+z^3),\ (zx,\ x^3-y^3+z^3),\ (xy,\ x^3+y^3-z^3)$$

on the curve $Y^2=4X^3+D(x^3, y^3, z^3)$ over $\boldsymbol{Q}(x, y, z)$. In order to find curves of this type having many integral points, Craig studied the simultaneous equations

$$(1)\qquad \begin{cases} x_0z_0 = x_1z_1\,, & x_0^3-y_0^3+z_0^3 = -(x_1^3-y_1^3+z_1^3)\,, \\ x_0y_0 = x_2y_2\,, & x_0^3+y_0^3-z_0^3 = -(x_2^3+y_2^3-z_2^3)\,, \end{cases}$$

which yield immediately

$$D(x_0^3, y_0^3, z_0^3) = D(x_1^3, y_1^3, z_1^3) = D(x_2^3, y_2^3, z_2^3)\,.$$

He gave the solution as follows; For α, β, γ such that

$$\alpha+\beta+\gamma = 0\,,$$

let

$$(2)\qquad \phi = \begin{vmatrix} \alpha-\beta & \gamma-\alpha \\ \beta-\gamma & \alpha-\beta \end{vmatrix},$$

$$(3)\qquad \begin{bmatrix} L & U \\ M & V \\ N & W \end{bmatrix} = \begin{bmatrix} 1+3\alpha\phi & \phi^2+3\alpha \\ 1+3\beta\phi & \phi^2+3\beta \\ 1+3\gamma\phi & \phi^2+3\gamma \end{bmatrix},$$

$$(4)\qquad \begin{cases} K = M+V+3\phi \\ \lambda = -W(2L^2-LW+W^2) \\ \mu/K = (N+U)^2+W(M-V) \\ \nu = L^2(N+U)-KW(M-V) \\ a = -LW(L-W)(N-U) \\ Kb = -\lambda(3\phi K-LU)-\mu KN \\ c/L = 3\phi(-\lambda/W)+U(-a/LW) \\ N\mu b_1 = 3\phi\lambda a-L\mu b \\ K\nu c_1 = W\lambda a-K\mu b_1\,. \end{cases}$$

Then

$$\begin{bmatrix} x_0 & y_0 & z_0 \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{bmatrix} = \begin{bmatrix} \lambda a & \mu b & \nu c \\ \lambda c & \mu b_1 & \nu a \\ \lambda b & \mu a & \nu c_1 \end{bmatrix}$$

gives a solution of the equations (1).

In particular, putting $[\alpha, \beta, \gamma]=[0, T, -T]$, we may consider that the parameters appearing above and $x_0, \cdots, z_2$ are rational functions in one variable T. In fact, we can write them down by a tedious calculation or an electric computer (see Appendix A). Let $D(T)=D(x_0^3, y_0^3, z_0^3)$ and $A_i(T)$, $B_i(T)$ $(1\leqq i\leqq 6)$ be as in the table below.

i	A_i	B_i
1	$x_0z_0=x_1z_1$	$x_0^3-y_0^3+z_0^3=-x_1^3+y_1^3-z_1^3$
2	y_2z_2	$-x_2^3+y_2^3+z_2^3$
3	x_1y_1	$x_1^3+y_1^3-z_1^3$
4	$x_0y_0=x_2y_2$	$x_0^3+y_0^3-z_0^3=-x_2^3-y_2^3+z_2^3$
5	y_0z_0	$-x_0^3+y_0^3+z_0^3$
6	y_1z_1	$-x_1^3+y_1^3+z_1^3$

For $1\leqq i\leqq 6$, $A_i(T)$ and $B_i(T)$ are all polynomials in $\boldsymbol{Z}[T]$. Thus we obtain the family of the elliptic curves;

$$Y^2 = 4X^3+D(t)\,, \qquad \text{for} \quad t\in\boldsymbol{Z}\,,$$

having the six integral points $P_i=(A_i(t), B_i(t))$ $(1\leqq i\leqq 6)$.

In Craig [2], the last two points P_5, P_6 are not used, since the classes of ideals of a quadratic field corresponding to three points, for example, P_1, P_4, P_5 satisfy an identical relation (see [1] pp. 451). However, in the proof of our theorem, we can take full advantage of these six points.

We now state, as lemmas, a few properties of the polynomials $A_i(T)$, $B_i(T)$ and $D(T)$ required later. The first lemma is shown by patient modular calculations.

Lemma 1. *For any rational integer t, we have*

(5) $B_i(t)\not\equiv 0 \pmod 3$ $\quad (1\leqq i\leqq 6)$,

(6) $D(t)\equiv 1 \pmod 4$,

(7) $A_i(t)\equiv 0 \pmod 4$ $\quad (1\leqq i\leqq 6)$, *if* $t\equiv 0 \pmod 4$.

Lemma 2. *$A_i(T)$ and $B_i(T)$ are relatively prime in $\boldsymbol{Q}[T]$, for $1\leqq i\leqq 6$.*

Proof. For $1 \leqq i \leqq 4$, the assertions are shown in [2] pp. 391–396. The others can be verified from them without difficulty.

Lemma 3. *$D(T)$ has at least one root whose multiplicity is prime to 3.*

Proof. Since $D(T)=1+\cdots-2^{23}3^{72}T^{141}$ (see [2] pp. 390), it is easy to see that $D(T)$ cannot be equal to $rE(T)^3$ for any $r \in \boldsymbol{Q}$, and $E(T) \in \boldsymbol{Q}[T]$. The lemma follows from this obviously. (In fact, it has been proved in [2] that there are at least three simple roots of $D(T)$, which shall not be required in our article.)

REMARK. Lemmas 2 and 3 are immediate consequences of the irreducibility of $D(T)$ which can be shown by a computer calculation. Indeed, the factorizer of REDUCE reveals the fact that $D(T)$ modulo 79 is irreducible in $(\boldsymbol{Z}/79\boldsymbol{Z})[T]$.

2. Unramified extensions

We now consider the pure cubic fields

$$K_t = \boldsymbol{Q}(\theta(t)) \qquad \text{where} \quad 4\theta(t)^3 = D(t)\,,$$

for $t \in \boldsymbol{Z}$. Note that K_t is actually pure cubic because $D(t)/4$ is not a cube by (6). Let

$$L_t = K_t(\sqrt{\theta(t)+A_1(t)}, \cdots, \sqrt{\theta(t)+A_6(t)})\,.$$

Then we have

Lemma 4. *Suppose, for $1 \leqq i \leqq 6$, $A_i(t)$ and $B_i(t)$ are relatively prime in the ring $\boldsymbol{Z}[2^{-1}]$ and $t \equiv 0 \pmod 4$. Then L_t/K_t is unramified at all primes of K_t.*

Proof. We write simply A_i instead of $A_i(t)$, and so on. It suffices to prove that the quadratic extension $K_t(\sqrt{\theta+A_i})/K_t$ is unramified for each i. First, since $\theta^3+A_i^3=(B_i/2)^2>0$ and consequently $\theta+A_i$ is totally positive, all infinite primes of K_t are unramified. Next, let $\mathfrak{p}$ be any prime ideal of K_t prime to 2. $\mathfrak{p}$ is unramified for $K_t(\sqrt{\theta+A_i})$ if it does not divide $\theta+A_i$. Assume that $\theta+A_i$ is divisible by $\mathfrak{p}$. Then we have

$$(B_i/2)^2 = \theta^3+A_i^3 = (\theta+A_i)(\theta^2-\theta A_i+A_i^2) \equiv 0 \pmod{\mathfrak{p}}\,.$$

If $\theta^2-\theta A_i+A_i^2 \equiv 0 \pmod{\mathfrak{p}}$, then $B_i \equiv 3A_i \equiv 0 \pmod{\mathfrak{p}}$ which contradicts (5) or the assumption of the lemma. Therefore

$$\mathrm{ord}_{\mathfrak{p}}(\theta+A_i) = \mathrm{ord}_{\mathfrak{p}}(\theta^3+A_i^3) = \mathrm{ord}_{\mathfrak{p}}((B_i/2)^2) \equiv 0 \pmod 2\,.$$

This impiles that $\mathfrak{p}$ is unramified for $K_t(\sqrt{\theta+A_i})$. Lastly, as $\mathrm{ord}_2(D/4)=-2$

by (6), there is a unique prime ideal $\mathfrak{q}$ of K_t lying above 2 which is totally ramified for $K_t/\boldsymbol{Q}$. We have

$$\mathrm{ord}_{\mathfrak{q}}(2\theta) = \mathrm{ord}_{\mathfrak{q}}(2)+\mathrm{ord}_{\mathfrak{q}}(\theta) = 3-2 = 1\,.$$

Thus, by (6), (7) and the assumption $t\equiv 0 \pmod 4$, we have

$$(2\theta)^2(\theta+A_i)\equiv 4\theta^3 = D\equiv 1 \qquad (\mathrm{mod}\ 4)\,.$$

Hence $\mathfrak{q}$ is unramified for $K_t(\sqrt{(2\theta)^2(\theta+A_i)})=K_t(\sqrt{\theta+A_i})$. This completes the proof.

3. A specific example

After Craig [2], we will give a specific numerical example and utilize it to infer the existence of infinitely many fields mentioned in the theorem.

We will examine the case $t=-1$, that is, $[\alpha, \beta, \gamma]=[0, -1, 1]$. By (2)–(4), we obtain the following values;

$$\phi = 3\,,$$

$$\begin{bmatrix} L & U \\ M & V \\ N & W \end{bmatrix} = \begin{bmatrix} 1 & 9 \\ -8 & 6 \\ 10 & 12 \end{bmatrix},$$

$$\begin{cases} K = 7 \\ \lambda = -1608 = -2^3\cdot 3\cdot 67 \\ \mu/K = 193 \quad (\text{prime}) \\ \nu = 1195 = 5\cdot 239 \\ a = 132 = 2^2\cdot 3\cdot 11 \\ Kb = -7738 = -2\cdot 53\cdot 73 \\ c = 1107 = 3^3\cdot 41 \\ \mu b_1 = -41687 \quad (\text{prime}) \\ K\nu c_1 = -2255263 \quad (\text{prime}). \end{cases}$$

With the same procedure as in [2] pp. 383–386, we can show that $A_i(-1)$ and $B_i(-1)$ are relatively prime for all $1\leqq i\leqq 6$ (cf. Appendix B). Let R_i be the resultant of $A_i(T)$ and $B_i(T)$ $(1\leqq i\leqq 6)$. By Lemma 2, R_i is a non-zero rational integer. Lte M_1 be the product of all odd prime factors of $\prod_{i=1}^{6} R_i$.

Lemma 5. *If $t\equiv -1 \pmod{M_1}$, then $A_i(t)$ and $B_i(t)$ are relatively prime in $\boldsymbol{Z}[2^{-1}]$ for $1\leqq i\leqq 6$.*

Proof. If an odd prime l divides both of $A_i(t)$ and $B_i(t)$, then we have

$R_i \equiv 0 \pmod{l}$ thus $M_1 \equiv 0 \pmod{l}$. Therefore, if $t \equiv -1 \pmod{M_1}$, then $A_i(-1) \equiv B_i(-1) \equiv 0 \pmod{l}$ which is a contradiction.

Next we are concerned with the independency of $\theta(t)+A_i(t)$ $(1 \leqq i \leqq 6)$ in $K_t^\times / K_t^{\times 2}$. Let p be a prime for which $D(-1)/4$ is a cubic residue modulo p. We define $c_i(p) \in \boldsymbol{Z}/2\boldsymbol{Z}$ as

$$\left(\frac{r+A_i(-1)}{p}\right) = (-1)^{c_i(p)},$$

where $r^3 \equiv D(-1)/4 \pmod{p}$ and $(—)$ is the quadratic residue symbol. It should be noted that $c_i(p)$ is dependent on the choice of r. We will fix r suitably for each p. A computer search gives the following table;

p	$D/4$	r	c_1	c_2	c_3	c_4	c_5	c_6
17	10	3	1	0	1	1	1	1
19	12	10	0	1	1	0	1	1
23	4	3	0	1	0	0	1	0
31	1	25	1	0	0	0	0	0
37	1	1	0	1	0	0	0	1
41	16	10	0	0	0	0	0	1

The second and third columns are given modulo p. Let $[p_1, \cdots, p_6] = [17, 19, 23, 31, 37, 41]$ and $M_2 = \prod_{j=1}^{6} p_j$. We need the fact that $\det(c_i(p_j)) \neq 0$ in $\boldsymbol{Z}/2\boldsymbol{Z}$, which is easily verified.

Lemma 6. *If $t \equiv -1 \pmod{M_2}$, then $\theta(t)+A_1(t), \cdots, \theta(t)+A_6(t)$ are independent in $K_t^\times / K_t^{\times 2}$.*

Proof. Suppose $t \equiv -1 \pmod{M_2}$. It is not difficult to show that there exist a prime ideal $\mathfrak{p}_j$ of K_t such that

$$\left(\frac{\theta(t)+A_i(t)}{\mathfrak{p}_j}\right) = (-1)^{c_i(p_j)} \qquad (1 \leqq j \leqq 6).$$

Assume

$$\prod_{i=1}^{6} (\theta(t)+A_i(t))^{a_i} \in K_t^{\times 2}$$

for some $a_i \in \boldsymbol{Z}/2\boldsymbol{Z}$. Considering this modulo $\mathfrak{p}_j$, we have

$$\sum_{i=1}^{6} c_i(p_j) a_i = 0 \qquad (1 \leqq j \leqq 6).$$

As $\det(c_i(p_j))\neq 0$, we see $a_i=0$ for all $1\leqq i\leqq 6$. This proves the lemma.

REMARK. For $t\in \boldsymbol{Z}$, let E_t be the elliptic curve defined by $Y^2=4X^3+D(t)$, and $E_t(\boldsymbol{Q})$ be the set of $\boldsymbol{Q}$-rational points of E_t. Then there is an injective homomorphism

$$E_t(\boldsymbol{Q})/2E_t(\boldsymbol{Q}) \to K_t^{\times}/K_t^{\times 2}$$

given by

$$(x, y) \to \theta(t)+x\,.$$

(See [7] Chap. X.) Therefore the above lemma implies that, for infinitely many rational integers t, the six points $(A_i(t), B_i(t))$ $(1\leqq i\leqq 6)$ are independent in $E_t(\boldsymbol{Q})/2E_t(\boldsymbol{Q})$, and consequently,

$$\operatorname{rank} E_t(\boldsymbol{Q})\geqq 6\,.$$

On the other hand, Kihara [4] showed a result of this type using the duplication formula on elliptic curves, for the case $[\alpha, \beta, \gamma]=[-t, t, 0]$. Kihara's argument can be applied to the proof of the independency of $\theta(t)+A_i(t)$ $(1\leqq i\leqq 6)$ in $K_t^{\times}/K_t^{\times 2}$.

4. Proof of Theorem

We are now ready to prove the theorem. Let t be a rational integer such that

$$(8)\qquad \begin{cases} t\equiv 0 & (\mathrm{mod}\ 4)\,, \\ t\equiv -1 & (\mathrm{mod}\ M_0)\,, \end{cases}$$

where M_0 is the least common multiple of M_1 and M_2. Then, by Lemmas 4, 5 and 6, L_t is an unramified abelian extension of K_t with Galois group isomorphic to the elementary 2-abelian group of rank 6. Hence K_t is a pure cubic field whose ideal class group has 2-rank at least 6.

Lastly, we must make sure of existence of infinitely many such fields. From Lemma 3, we can take a root τ of $D(T)$ with multiplicity m prime to 3. Write

$$D(T) = (T-\tau)^m D_0(T)\,.$$

It is well known that there exist infinitely many prime ideals of $\boldsymbol{Q}(\tau)$ of degree 1 which are unramified for $\boldsymbol{Q}(\tau)/\boldsymbol{Q}$. We choose a prime ideal $\mathfrak{p}$ of this kind such that

$$\operatorname{ord}_{\mathfrak{p}}(6M_0) = \operatorname{ord}_{\mathfrak{p}}(\tau) = \operatorname{ord}_{\mathfrak{p}}(D_0(\tau)) = 0\,.$$

Then it is possible to find a rational integer t satisfying in addition to (8) also the congruence;

$$t \equiv \tau + p \pmod{\mathfrak{p}^2},$$

where p is the rational prime contained in $\mathfrak{p}$. Since

$$\mathrm{ord}_{\mathfrak{p}}(t-\tau) = \mathrm{ord}_{\mathfrak{p}}(p) = 1 \quad \text{and} \quad \mathrm{ord}_{\mathfrak{p}}(D_0(t)) = \mathrm{ord}_{\mathfrak{p}}(D_0(\tau)) = 0,$$

we have

$$\mathrm{ord}_{\mathfrak{p}}(D(t)) = m \not\equiv 0 \pmod{3}.$$

Hence p is ramified for K_t. The various choices of $\mathfrak{p}$ prove our assertion.

Appendix

A. The following explicit expressions in the case $[\alpha, \beta, \gamma]=[0, T, -T]$ are obtained, in an instant, by means of REDUCE.

$$\phi = 3T^2,$$

$$\begin{bmatrix} L & U \\ M & V \\ N & W \end{bmatrix} = \begin{bmatrix} 1 & 9T^4 \\ 1+9T^3 & 3T+9T^4 \\ 1-9T^3 & -3T+9T^4 \end{bmatrix},$$

$$K = 1+3T+9T^2+9T^3+9T^4,$$

$$\lambda = 6T+9T^2+27T^3-18T^4-54T^5-243T^6+81T^8+729T^9-729T^{12},$$

$$\mu/K = 1-3T+9T^2-18T^3+81T^6-81T^7,$$

$$\nu = 1+3T-9T^3-27T^4+81T^6+81T^7-486T^9+729T^{12},$$

$$a = 3T+9T^2-36T^4-162T^5-81T^6+81T^7+648T^8+486T^9-729T^{11} -729T^{12},$$

$$Kb = -1-3T-18T^2-72T^3-288T^4-675T^5-1215T^6-567T^7+1701T^8 +7047T^9+9477T^{10}+8019T^{11}-3645T^{12}-13122T^{13}-19683T^{14} -13122T^{15}-6561T^{16},$$

$$c = 18T^2+27T^3+90T^4+27T^5-81T^6-567T^7-405T^8-243T^9+729T^{10} +729T^{11}+729T^{12},$$

$$\mu b_1 = y_1 \text{ (see below)},$$

$$K\nu c_1 = Kz_2 \text{ (see below)}.$$

The following expressions are given with coefficients which are factorized into prime factors;

$$x_0 = 2\cdot 3^2T^2+3^4T^3+2\cdot 3^4T^4-3^3T^5-2^2\cdot 3^4\cdot 5T^6-3^5\cdot 17T^7-2^2\cdot 3^4\cdot 19T^8 +3^5\cdot 31T^9+3^8\cdot 5T^{10}+3^6\cdot 97T^{11}+3^6\cdot 13T^{12}-3^7\cdot 53T^{13}-2^2\cdot 3^8\cdot 13T^{14} -3^{11}T^{15}+3^8\cdot 29T^{16}+3^9\cdot 43T^{17}+2\cdot 3^{10}\cdot 5T^{18}-2\cdot 3^{10}T^{19}-2\cdot 3^{12}T^{20} -3^{11}\cdot 5T^{21}+3^{12}T^{23}+3^{12}T^{24},$$

$$y_0 = -1-2\cdot 3^2T^2-3^3T^3-2^2\cdot 3^2\cdot 5T^4-3^3\cdot 5T^5-3^4\cdot 7T^6+3^4\cdot 5^2T^7$$
$$+2\cdot 3^5\cdot 7T^8+3^5\cdot 59T^9-3^6\cdot 5T^{10}-2\cdot 3^6\cdot 13T^{11}-3^6\cdot 5\cdot 31T^{12}$$
$$-2\cdot 3^7\cdot 11T^{13}+2^2\cdot 3^8T^{14}+3^8\cdot 5\cdot 13T^{15}+2^2\cdot 3^8\cdot 11T^{16}+3^9\cdot 7T^{17}$$
$$-3^{10}\cdot 13T^{18}-3^{10}\cdot 11T^{19}-3^{12}T^{20}+3^{12}T^{21}+3^{12}T^{22}+3^{12}T^{23},$$

$$z_0 = 2\cdot 3^2T^2+3^4T^3+3^2\cdot 19T^4+3^3\cdot 5T^5-3^6T^6-3^4\cdot 29T^7-3^4\cdot 41T^8+3^7T^9$$
$$+3^6\cdot 23T^{10}+3^6\cdot 31T^{11}-2\cdot 3^6T^{12}-3^7\cdot 43T^{13}-2^4\cdot 3^8T^{14}-3^9T^{15}$$
$$+3^8\cdot 5\cdot 11T^{16}+3^9\cdot 17T^{17}+3^{11}T^{28}-2^2\cdot 3^{11}T^{19}-3^{10}\cdot 11T^{20}-3^{12}T^{21}$$
$$+3^{12}T^{22}+3^{12}T^{23}+3^{12}T^{24},$$

$$x_1 = 2^2\cdot 3^3T^3+2^2\cdot 3^4T^4+3^3\cdot 47T^5+3^4\cdot 17T^6+3^6T^7-2\cdot 3^4\cdot 67T^8-3^5\cdot 89T^9$$
$$-2^3\cdot 3^6\cdot 7T^{10}+2^2\cdot 3^6\cdot 5T^{11}+2\cdot 3^6\cdot 61T^{12}+2^3\cdot 3^8\cdot 5T^{13}+3^8\cdot 19T^{14}$$
$$-3^9\cdot 5T^{15}-3^8\cdot 113T^{16}-2^2\cdot 3^9\cdot 7T^{17}-2^2\cdot 3^{10}T^{18}+3^{10}\cdot 17T^{19}+3^{11}\cdot 5T^{20}$$
$$+2^2\cdot 3^{11}T^{21}-3^{12}T^{22}-3^{12}T^{23}-3^{12}T^{24},$$

$$y_1 = 1+2\cdot 3^2T^2+2^2\cdot 3^2T^3+2\cdot 3^2\cdot 19T^4+2\cdot 3^3\cdot 19T^5+3^4\cdot 29T^6+2\cdot 3^4\cdot 5T^7$$
$$-2^2\cdot 3^7T^8-3^5\cdot 5^3T^9-3^6\cdot 61T^{10}+3^6\cdot 11T^{11}+3^6\cdot 5\cdot 37T^{12}$$
$$+2\cdot 3^7\cdot 5\cdot 13T^{13}+2^2\cdot 3^8\cdot 5T^{14}-3^9\cdot 13T^{15}-2\cdot 3^8\cdot 61T^{16}-2^2\cdot 3^9\cdot 7T^{17}$$
$$+3^{11}T^{18}+2\cdot 3^{12}T^{19}+3^{11}\cdot 5T^{20}-3^{12}T^{22}-3^{12}T^{23},$$

$$z_1 = 3T+2\cdot 3^2T^2+3^3T^3-3^2\cdot 7T^4-2^4\cdot 3^3T^5-2\cdot 3^4\cdot 5T^6+3^4\cdot 5T^7+3^4\cdot 53T^8$$
$$+2\cdot 3^5\cdot 17T^9-2\cdot 3^6T^{10}-2^3\cdot 3^6\cdot 5T^{11}-3^6\cdot 61T^{12}+2\cdot 3^7T^{13}+3^8\cdot 23T^{14}$$
$$+2^3\cdot 3^9T^{15}-3^8T^{16}-3^9\cdot 5^2T^{17}-3^{10}\cdot 7T^{18}+2\cdot 3^{10}\cdot 7T^{20}+2^2\cdot 3^{11}T^{21}$$
$$-3^{12}T^{23}-3^{12}T^{24},$$

$$Kx_2 = -2\cdot 3T-3^3T^2-2\cdot 3^4T^3-3^2\cdot 73T^4-2\cdot 3^4\cdot 17T^5-3^4\cdot 97T^6-2^5\cdot 3^4\cdot 7T^7$$
$$-3^5\cdot 79T^8+2^2\cdot 3^5\cdot 17T^9+3^6\cdot 229T^{10}+3^8\cdot 59T^{11}+2\cdot 3^6\cdot 373T^{12}$$
$$-3^7\cdot 17T^{13}-3^9\cdot 73T^{14}-2\cdot 3^9\cdot 7\cdot 13T^{15}-2\cdot 3^9\cdot 5\cdot 17T^{16}+3^9\cdot 5T^{17}$$
$$+3^{11}\cdot 47T^{18}+2^4\cdot 3^{10}\cdot 13T^{19}+2^3\cdot 3^{11}\cdot 7T^{20}-2\cdot 3^{12}\cdot 5T^{21}-3^{12}\cdot 31T^{22}$$
$$-2^3\cdot 3^{12}\cdot 5T^{23}-2\cdot 3^{12}\cdot 7T^{24}+3^{14}T^{25}+3^{15}T^{26}+2\cdot 3^{14}T^{27}+3^{14}T^{28},$$

$$y_2/K = 3T-3^2T^4-2^3\cdot 3^3T^5+3^4T^6-3^5T^7+2\cdot 3^4\cdot 19T^8-3^6\cdot 5^2T^{11}-3^6T^{12}$$
$$+2^2\cdot 3^7T^{13}+2^3\cdot 3^8T^{14}-2\cdot 3^9T^{16}-3^{10}T^{17}+3^{10}T^{19},$$

$$Kz_2 = -1-3T-3^3T^2-3^2\cdot 17T^3-2^5\cdot 3^3T^4-2^4\cdot 3^3\cdot 7T^5-2^2\cdot 3^7T^6-2^3\cdot 3^4\cdot 23T^7$$
$$-2^2\cdot 3^4\cdot 41T^8+3^7\cdot 17T^9+2^2\cdot 3^7\cdot 17T^{10}+3^9\cdot 17T^{11}+3^7\cdot 149T^{12}$$
$$-2\cdot 3^7\cdot 11T^{13}-3^8\cdot 11\cdot 17T^{14}-2\cdot 3^9\cdot 59T^{15}-2\cdot 3^8\cdot 211T^{16}-3^9\cdot 5T^{17}$$
$$+3^{10}\cdot 71T^{18}+3^{10}\cdot 7\cdot 23T^{19}+3^{10}\cdot 5\cdot 29T^{20}+3^{11}\cdot 11T^{21}-2^2\cdot 3^{12}\cdot 5T^{22}$$
$$-3^{12}\cdot 31T^{23}-2^3\cdot 3^{13}T^{24}+2\cdot 3^{14}T^{26}+2\cdot 3^{14}T^{27}+3^{14}T^{28}.$$

B. To check quickly that $(A_i(-1), B_i(-1))=1$ $(1\leqq i\leqq 6)$, one can use the Euclidian algorithm, directly for $A_i(-1)$ and $B_i(-1)$, which is carried out on an

electric computer. Another method is to factorize them into primes. Our assertion is verified by the following complete factorizations;

$$A_1 = -2^5 \cdot 3^5 \cdot 5 \cdot 11 \cdot 41 \cdot 67 \cdot 239 \qquad B_1 = 401 \cdot 1229 \cdot 2153 \cdot 5311935749$$
$$A_2 = -2^2 \cdot 3 \cdot 11 \cdot 193 \cdot 2255263 \qquad B_2 = -750719 \cdot 7518218706311$$
$$A_3 = 2^3 \cdot 3^4 \cdot 41 \cdot 67 \cdot 41687 \qquad B_3 = -11 \cdot 23304629 \cdot 22017793601$$
$$A_4 = 2^6 \cdot 3^2 \cdot 11 \cdot 53 \cdot 67 \cdot 73 \cdot 193 \qquad B_4 = -5 \cdot 61 \cdot 18542335623945929$$
$$A_5 = -2 \cdot 3^3 \cdot 5 \cdot 41 \cdot 53 \cdot 73 \cdot 193 \cdot 239 \qquad B_5 = -29 \cdot 34701175163759747$$
$$A_6 = -2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 239 \cdot 41687 \qquad B_6 = 139 \cdot 40605300259955467$$

Lastly, we append the factorization of $D=D(-1)$;

$$D = 185478257 \cdot 1717521026386810359301809036 17 .$$

These factorizations were performed in consulting of Riesel [6] or Wada [8].

References

[1] M. Craig: *A type of class group for imaginary quadratic fields,* Acta Arith. **22** (1973), 449–459.

[2] M. Craig: *A construction for irregular discriminants,* Osaka J. Math. **14** (1977), 365–402.

[3] A.C. Hearn: REDUCE user's manual, Version3.0, The Rand Corporation, Santa Monica, 1983.

[4] S. Kihara: *On elliptic curves of the form $y^2=x^3+k$ with rank at least* 6 *over* $\boldsymbol{Q}$, (preprint).

[5] S. Nakano: *On the construction of pure number fields of odd degrees with large* 2*-class groups,* Proc. Japan Acad. **62A** (1986), 61–64.

[6] H. Riesel: Prime numbers and computer methods for factorization, Progress in Math. 57, Birkhäuser, Boston, 1985.

[7] J.H. Silverman: The arithmetic of elliptic curves, Graduate Texts in Math. 106, Springer-Verlag, New York, 1986.

[8] H. Wada: High-precision multiplication and testing for primarity (in Japanese), Sophia Kokyuroku in Math. 15, Sophia Univ., Tokyo, 1983.

[9] Y. Yamamoto: *On unramified Galois extensions of quadratic number fields,* Osaka J. Math. **7** (1970), 57–76.

Department of Mathematics
Faculty of Science
Gakushuin University
Mejiro, Toshima-ku, Tokyo 171
Japan