ACTA ARITHMETICA
XCVI.3 (2001)

A family of infinite pairs of quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{-D})$ whose class numbers are both divisible by 3

by

TORU KOMATSU (Tokyo)

Introduction. In [N] and [A-C] it was shown that, for any positive integer n, there exist infinitely many imaginary quadratic fields whose class numbers are divisible by n. The same result for real quadratic fields was shown in [Y] and [W]. Earlier, Honda [Ho] had shown the case where $n = 3$ for real quadratic fields. Hartung [H1] showed that there exist infinitely many imaginary quadratic fields whose class numbers are divisible by 3. In [H2] he also showed the existence of infinitely many imaginary quadratic fields whose class numbers are not divisible by 3. Scholz [Sc] gave a relation between the 3-rank r of the ideal class group of a real quadratic field $\mathbb{Q}(\sqrt{D})$ and the 3-rank s of an imaginary quadratic field $\mathbb{Q}(\sqrt{-3D})$.

THEOREM (A. Scholz). *We have*

$$r \le s \le r + 1.$$

In particular, *for a positive integer* D, *if* $3 \mid h(\mathbb{Q}(\sqrt{D}))$, *then* $3 \mid h(\mathbb{Q}(\sqrt{-3D}))$.

This relation is an original version of the "reflection". From the results above there exist infinitely many quadratic fields $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{-3D})$ with class numbers both divisible by 3. On the other hand, Zhang [Z] showed some relations between the class numbers $h(\mathbb{Q}(\sqrt{D}))$ and $h(\mathbb{Q}(\sqrt{-D}))$ by means of the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{D})$.

In this paper we prove the existence of infinite families of quadratic fields $\mathbb{Q}(\sqrt{D})$ with $3 \mid h(\mathbb{Q}(\sqrt{D}))$ and $3 \mid h(\mathbb{Q}(\sqrt{-D}))$. We also give explicit integers $\{D_n\}_{n\ge1}$ such that $3 \mid h(\mathbb{Q}(\sqrt{D_n})), 3 \mid h(\mathbb{Q}(\sqrt{-D_n}))$ and $\sharp\{\mathbb{Q}(\sqrt{D_n}) \mid n \ge 1\} = \infty$ (cf. Examples 2.6, 2.7 and Proposition 2.8). Our method is explicit, and the divisibility of the class number by 3 is shown by constructing explicit cubic polynomials which give unramified cyclic cubic extensions of quadratic fields.

2000 *Mathematics Subject Classification*: Primary 11R29; Secondary 11R11.

First we state sufficient conditions for $3 \mid h(\mathbb{Q}(\sqrt{D}))$ and $3 \mid h(\mathbb{Q}(\sqrt{-D}))$. Let d be a square-free integer. Let integers a, b and c be pairwise relatively prime, and satisfy $a^2 + db^2 = c^2$. Put $D_1 = d(c^4 + c^2a^2 + a^4)/3$.

Theorem I. *Suppose that*:

(1) *there exists a prime number p such that $p \mid a$ and $2 \notin \mathbb{F}_p^3$*,
(2) $6 \mid b$,
(3) *there exists a prime number q such that $q \mid c$ and $2 \notin \mathbb{F}_q^3$.*

Then

$$3 \mid h(\mathbb{Q}(\sqrt{D_1})) \quad \textit{and} \quad 3 \mid h(\mathbb{Q}(\sqrt{-D_1})).$$

Here, $\mathbb{F}_p$ is the finite field of p elements.

Under the same conditions as in Theorem I, let us define sequences $\{a_n\}_{n\geq 1}$, $\{b_n\}_{n\geq 1}$ and $\{c_n\}_{n\geq 1}$ of integers recursively by

$$a_1 = a, \quad b_1 = b, \quad c_1 = c,$$
$$a_{n+1} = (a^2 - db^2)a_n - 2abdb_n,$$
$$b_{n+1} = 2aba_n + (a^2 - db^2)b_n, \quad c_{n+1} = c^2 c_n.$$

Moreover we define $D_n = D_n(a, b, c)$ by

$$D_n = \frac{d(c_n^4 + c_n^2 a_n^2 + a_n^4)}{3}.$$

In Section 2 we will see that $D_n \in \mathbb{Z}$.

Theorem II. *The number D_n satisfies both*

$$3 \mid h(\mathbb{Q}(\sqrt{D_n})) \quad \textit{and} \quad 3 \mid h(\mathbb{Q}(\sqrt{-D_n})).$$

Moreover, $\sharp\{\mathbb{Q}(\sqrt{D_n}) \mid n \in \mathbb{N}\} = \infty$.

Thus, as a corollary of Theorem II we obtain

Corollary I. *There exist infinitely many quadratic fields $\mathbb{Q}(\sqrt{D})$ satisfying both $3 \mid h(\mathbb{Q}(\sqrt{D}))$ and $3 \mid h(\mathbb{Q}(\sqrt{-D}))$.*

Remark 1. Let S_R and S_I be the sets of square-free positive integers D such that $3 \mid h(\mathbb{Q}(\sqrt{D}))$ and $3 \mid h(\mathbb{Q}(\sqrt{-D}))$, respectively. Then we have

$$\sharp(S_R \cap \{1 < D < 10000\}) = 554,$$
$$\sharp(S_I \cap \{1 < D < 10000\}) = 2151,$$
$$\sharp(S_R \cap S_I \cap \{1 < D < 10000\}) = 152.$$

For example,

$$S_R \cap S_I \cap \{1 < D < 2000\} = \{473, 730, 839, 898, 985, 993, 1090, 1191, 1373, 1478, 1567, 1599, 1882, 1901, 1937\}.$$

Let $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{F}_p$ and $\mathbb{Q}^*$ be the set of positive integers, the ring of rational integers, the field of rational numbers, the finite field of p elements and the multiplicative group of non-zero rational numbers, respectively. For a prime number p and an integer m, $v_p(m)$ is the greatest exponent n such that $p^n \mid m$. The class number of an algebraic number field F is denoted by $h(F)$. The notation $f(Z) \in \mathrm{Ir}(L)$ means that a polynomial $f(Z) \in L[Z]$ is irreducible over a field L.

I wish to express my deepest gratitude to Professor Masato Kurihara, for his guidance, encouragement and criticism throughout my study, and I especially thank Professor Takao Sasai for his many helpful comments.

I would like to thank the referee who pointed out to me the existence of [R].

1. A sufficient condition for $3 \mid h(\mathbb{Q}(\sqrt{D}))$ and $3 \mid h(\mathbb{Q}(\sqrt{-D}))$. For a square-free integer d, T_d denotes the set of triples (a, b, c) defined by

$$T_d = \{(a, b, c) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \mid a^2 + db^2 = c^2,\ \gcd(a, b, c) = 1\}.$$

Remark 1.1. Let a, b and c be integers satisfying

$$a^2 + db^2 = c^2. \tag{1.1}$$

Then $\gcd(a, b, c) = 1$ if and only if a, b and c are pairwise relatively prime, that is, $\gcd(a, b) = \gcd(b, c) = \gcd(c, a) = 1$ since d is square-free.

A polynomial $f_{a,c}(Z)$ is defined by

$$f_{a,c}(Z) = Z^3 - 3c^2 Z - 2a^3.$$

Let $K_{a,c}$ be the minimal splitting field of $f_{a,c}(Z)$ over $\mathbb{Q}$. Denote the discriminant of $f_{a,c}(Z)$ by $D_{a,c}$ and put $k_{a,c} = \mathbb{Q}(\sqrt{D_{a,c}})$.

Lemma 1.2. *For (a, b, c) in T_d, assume that $f_{a,c}(Z) \in \mathrm{Ir}(\mathbb{Q})$. Then the conditions $2 \nmid c$ and $3 \mid ab$ hold if and only if the extension $K_{a,c}/k_{a,c}$ is unramified.*

For the proof we will use [L-N], which gave a necessary and sufficient condition for the unramifiedness of such extensions. Let $f(Z)$ be an irreducible polynomial of the form

$$f(Z) = Z^3 - mZ - n$$

with $m, n \in \mathbb{Z}$ and K_f be the minimal splitting field of $f(Z)$ over $\mathbb{Q}$. We denote the discriminant of $f(Z)$ by D_f and put $k_f = \mathbb{Q}(\sqrt{D_f})$. Assume that, for each prime number p, either $v_p(m) < 2$ or $v_p(n) < 3$.

Proposition LN (P. Llorente and E. Nart). (1) *For a prime number $p \neq 3$, the extension K_f/k_f is ramified at a prime ideal $\mathfrak{p}$ above p if and only if $1 \leq v_p(n) \leq v_p(m)$.*

(2) *For a prime number* $p = 3$, *the extension* K_f/k_f *is ramified at a prime ideal* $\mathfrak{p}$ *above* 3 *if and only if one of the following three conditions holds*:

$$\text{(2.i)} \quad 1 \le v_3(n) \le v_3(m),$$

$$\text{(2.ii)} \quad 3 \nmid n, \quad m \equiv 0, 6 \pmod 9 \quad \textit{and} \quad n^2 \not\equiv m+1 \pmod 9,$$

$$\text{(2.iii)} \quad 3 \nmid n, \quad m \equiv 3 \pmod 9 \quad \textit{and} \quad n^2 \not\equiv m+1 \pmod{27}.$$

Proof of Lemma 1.2. Let (a, b, c) be a triple in T_d. For a prime number p with $p \nmid 6$, it follows obviously from Proposition LN that the extension $K_{a,c}/k_{a,c}$ is unramified at prime ideals $\mathfrak{p}$ above p since $\gcd(c, a) = 1$. Also, by Proposition LN, $K_{a,c}/k_{a,c}$ is unramified at prime ideals $\mathfrak{p}$ above 2 if and only if $2 \nmid c$.

We discuss the ramifiedness of $K_{a,c}/k_{a,c}$ at prime ideals above 3. Let $\mathfrak{p}$ be a prime ideal above 3. First we assume $3 \mid a$. Then $v_3(3c^2) = 1$ and $v_3(2a^3) \ge 3$. From Proposition LN, $K_{a,c}/k_{a,c}$ is unramified at $\mathfrak{p}$.

Next we consider the case where $3 \nmid a$ and $3 \mid c$. Then $3 \nmid 2a^3$ and $3c^2 \equiv 0 \pmod 9$. Here, $(2a^3)^2 \equiv 4 \pmod 9$ and $3c^2 + 1 \equiv 1 \pmod 9$. Proposition LN implies that $K_{a,c}/k_{a,c}$ is ramified at $\mathfrak{p}$.

Finally assume that $3 \nmid a$ and $3 \nmid c$. Then $3 \nmid 2a^3$ and $3c^2 \equiv 3 \pmod 9$. By Proposition LN, $K_{a,c}/k_{a,c}$ is unramified at $\mathfrak{p}$ if and only if $(2a^3)^2 \equiv (3c^2+1) \pmod{27}$. Here,

$$\begin{aligned} (2a^3)^2 - (3c^2+1) &= (2a^2+1)^2(a^2-1) - 3db^2 \quad \text{(by (1.1))} \\ &\equiv -3db^2 \pmod{27} \quad \text{(since } 3 \nmid a\text{)}. \end{aligned}$$

Thus, $K_{a,c}/k_{a,c}$ is unramified at $\mathfrak{p}$ if and only if $3 \mid b$ since d is square-free. Hence $K_{a,c}/k_{a,c}$ is unramified at prime ideals $\mathfrak{p}$ above 3 if and only if $3 \mid a$ or $3 \mid b$, i.e., $3 \mid ab$. This completes the proof. ∎

Remark 1.3. The referee suggested to me that [R] can be used for the proof of Lemma 1.2 instead of [LN]. However, the proof above is my original version.

Corresponding to $f_{a,c}(Z)$, we consider $f_{c,a}(Z)$. As Lemma 1.2, we have

Lemma 1.4. *Let* (a, b, c) *be in* T_d, *and* $f_{c,a}(Z) \in \mathrm{Ir}(\mathbb{Q})$. *Then the conditions* $2 \nmid a$ *and* $3 \mid bc$ *hold if and only if the extension* $K_{c,a}/k_{c,a}$ *is unramified.*

Lemmas 1.2 and 1.4 imply

Proposition 1.5. *For* (a, b, c) *in* T_d, *assume that* $f_{a,c}(Z), f_{c,a}(Z) \in \mathrm{Ir}(\mathbb{Q})$. *Then* $6 \mid b$ *if and only if both the extensions* $K_{a,c}/k_{a,c}$ *and* $K_{c,a}/k_{c,a}$ *are unramified.*

Proof. It is sufficient to show that $6 \mid b$ if and only if $2 \nmid c$, $3 \mid ab$, $2 \nmid a$ and $3 \mid bc$. Assume $6 \mid b$. Then $3 \mid ab$ and $3 \mid bc$. As $\gcd(a, b) = 1$ and $\gcd(b, c) = 1$, it follows that $2\nmid c$ and $2\nmid a$. Conversely, since $\gcd(c,a)=\gcd(a,b)=1$ and $3\,|\,bc$, we have $3\nmid a$. Thus $3\,|\,b$ since $3\,|\,ab$. From $2\nmid c$, $2\nmid a$ and (1.1), it follows that $1+db^2\equiv 1 \pmod 8$ and $2\,|\,b$ since d is square-free. Hence $6\,|\,b$. ■

Here, it follows from the definitions and $(a,b,c)\in T_d$ that $D_{a,c}=3d(c^4+c^2a^2+a^4)(6b)^2$. And we also note that $D_{c,a}=-D_{a,c}$. Proposition 1.5 and class field theory give a sufficient condition for $3\,|\,h(\mathbb{Q}(\sqrt{D}))$ and $3\,|\,h(\mathbb{Q}(\sqrt{-D}))$.

PROPOSITION 1.6. *Let* (a,b,c) *be in* T_d. *If* $f_{a,c}(Z), f_{c,a}(Z)\in \mathrm{Ir}(\mathbb{Q})$ *and* $6\,|\,b$, *then* $3\,|\,h(\mathbb{Q}(\sqrt{D_{a,c}}))$ *and* $3\,|\,h(\mathbb{Q}(\sqrt{-D_{a,c}}))$.

On the irreducibility of $f_{a,c}(Z)$ we obtain

LEMMA 1.7. *If there exists a prime number* q *such that* $q\,|\,c$ *and* $2\notin \mathbb{F}_q^3$, *then* $f_{a,c}(Z)\in \mathrm{Ir}(\mathbb{Q})$.

Proof. If such a q exists, $f_{a,c}(Z)\equiv Z^3-2a^3\not\equiv Z^3 \pmod q$ since $\gcd(c,a)=1$ and $q\nmid 2a$. From $2\notin\mathbb{F}_q^3$, we have $f_{a,c}(Z)\in\mathrm{Ir}(\mathbb{F}_q)$. Hence, $f_{a,c}(Z)\in\mathrm{Ir}(\mathbb{Q})$. ■

Now we can show Theorem I.

Proof of Theorem I. By Lemma 1.7 and the relation between $f_{a,c}(Z)$ and $f_{c,a}(Z)$, it is clear that if there exists a prime number p with $p\,|\,a$ and $2\notin\mathbb{F}_p^3$, then $f_{c,a}(Z)\in\mathrm{Ir}(\mathbb{Q})$. Note that $D_{a,c}\equiv d(c^4+c^2a^2+a^4)/3 \pmod{\mathbb{Q}^{*2}}$ and $\mathbb{Q}(\sqrt{D_{a,c}})=\mathbb{Q}(\sqrt{D_1})$. Thus Proposition 1.6 and Lemma 1.7 imply the assertion of Theorem I. ■

2. Proof of Theorem II and examples. First we show that every D_n satisfies both $3\,|\,h(\mathbb{Q}(\sqrt{D_n}))$ and $3\,|\,h(\mathbb{Q}(\sqrt{-D_n}))$. It is sufficient to see that, for each n, the triple (a_n,b_n,c_n) satisfies all the assumptions in Theorem I. From the definition stated in the introduction we can prove inductively the following.

LEMMA 2.1. *We have*

$$a_n^2+db_n^2=c_n^2. \tag{2.1}$$

Proof. This is obvious when $n=1$. Assume that (2.1) holds for $n=k$. Then, by definition,

$$a_{k+1}^2+db_{k+1}^2=(a^2+db^2)^2(a_k^2+db_k^2)=c^4c_k^2=c_{k+1}^2. \ ■$$

LEMMA 2.2. *The integers* a_n, b_n *and* c_n *are pairwise relatively prime.*

Proof. By (2.1) and Remark 1.1, it is enough to show $\gcd(a_n,b_n)=1$. The definition of a_n and b_n implies

$$a_{n+1}+b_{n+1}\sqrt{-d}=(a+b\sqrt{-d})^2(a_n+b_n\sqrt{-d}). \tag{2.2}$$

Thus $(a_n + b_n\sqrt{-d}) = (a + b\sqrt{-d})^{2n-1}$. Suppose $\gcd(a_n, b_n) \neq 1$. Let l be a prime number such that $l \mid \gcd(a_n, b_n)$. Then (2.1) implies that $l \mid c_n$. From definition we have $c_n = c^{2n-1}$ and $l \mid c$. Note that $l \nmid a$ since $\gcd(c, a) = 1$. Since $\gcd(b, c) = 1$ and $6 \mid b$, both c and l are odd. It follows from $l \mid \gcd(a_n, b_n)$ that $(l) \mid (a_n \pm b_n\sqrt{-d}) = (a \pm b\sqrt{-d})^{2n-1}$ as ideals of $\mathbb{Q}(\sqrt{-d})$.

First we consider the case where the prime l does not ramify in the extension $\mathbb{Q}(\sqrt{-d})/\mathbb{Q}$. Then $(l) \mid (a \pm b\sqrt{-d})^{2n-1}$ implies $(l) \mid (a \pm b\sqrt{-d})$. So $2a \in (l)$ and $(l) \mid (2a)$. Since l is odd, we get $l \mid a$. This contradicts $l \nmid a$.

Next, consider the case where l ramifies. This implies that $l \mid d$ since l is odd. From $a^2 + db^2 = c^2$ and $l \mid c$, we have $l \mid a$. This is also a contradiction. Thus $\gcd(a_n, b_n) = 1$. ∎

Remark 2.3. We note that the sequences in the introduction are defined so as to satisfy (2.2).

Lemma 2.4. *The integers a_n, b_n and c_n satisfy the conditions* (1), (2) *and* (3) *in Theorem* I.

Proof. It is obvious from the definition that $a \mid a_n$, $b \mid b_n$ and $c \mid c_n$. ∎

We need the following version of Siegel's theorem. Let $M_{\mathbb{Q}}$ be the set of standard absolute values on $\mathbb{Q}$.

Theorem (C. Siegel, cf. [Si] and [Sil; IX Theorem 4.3]). *Let S be a finite set of absolute values such that $\{\infty\} \subset S \subset M_{\mathbb{Q}}$ and $f(x) \in \mathbb{Q}[x]$ be a polynomial of degree $d \geq 3$ with distinct roots* (*in* $\overline{\mathbb{Q}}$). *Then*

$$\sharp\{(x, y) \in R_S \times R_S \mid y^2 = f(x)\} < \infty,$$

where R_S is the ring of S-integers of $\mathbb{Q}$, *i.e.*, $R_S = \{x \in \mathbb{Q} \mid |x|_v \leq 1$ *for all* $v \in M_{\mathbb{Q}} \setminus S\}$.

Lemma 2.5. *For any square-free integer D*,

$$\sharp\{n \in \mathbb{N} \mid D_n \equiv D \pmod{\mathbb{Q}^{*2}}\} < \infty.$$

Proof. Let N_D be the set $\{n \in \mathbb{N} \mid D_n \equiv D \pmod{\mathbb{Q}^{*2}}\}$. If $N_D = \emptyset$, then the assertion is trivial. When $N_D \neq \emptyset$ and $n \in N_D$, there exists $x_n \in \mathbb{Z}$ such that

$$Dx_n^2 = D_n = d(c_n^4 + c_n^2 a_n^2 + a_n^4)/3$$

for D is square-free and D_n is an integer. In fact, from $\gcd(a_n, b_n) = \gcd(b_n, c_n) = 1$ and $3 \mid b_n$, we have $c_n^4 + c_n^2 a_n^2 + a_n^4 \equiv 0 \pmod 3$ and $D_n \in \mathbb{Z}$. By the equation above, we have

$$\left(\frac{x_n}{c_n^2}\right)^2 = \frac{d}{3D}\left(\left(\frac{a_n}{c_n}\right)^4 + \left(\frac{a_n}{c_n}\right)^2 + 1\right).$$

Let S be the finite set defined by

$$S = \{\infty\} \cup \{l \in \mathbb{N} \mid l \text{ is a prime number such that } l \mid c\},$$

and set

$$E_{D,S} = \left\{ (X, Y) \in R_S \times R_S \;\middle|\; Y^2 = \frac{d}{3D}(X^4 + X^2 + 1) \right\}.$$

Then we have $(a_n/c_n, x_n/c_n^2) \in E_{D,S}$ since $c_n = c^{2n-1}$. On the other hand, since S and the polynomial $d(X^4+X^2+1)/(3D)$ satisfy all the assumptions of Siegel's theorem, the set $E_{D,S}$ is finite. Thus the number of a_n/c_n with $(a_n/c_n, x_n/c_n^2) \in E_{D,S}$ is also finite. Let l be a prime number such that $l \mid c$. It follows from Lemma 2.2 that $v_l(a_n/c_n) = -(2n-1)v_l(c)$. Then we have $a_n/c_n \neq a_{n'}/c_{n'}$ if $n \neq n'$. Therefore the number of n with $(a_n/c_n, x_n/c_n^2) \in E_{D,S}$ is finite and so is the number of n such that $D_n \equiv D \pmod{\mathbb{Q}^{*2}}$. ■

Now we can show Theorem II.

Proof of Theorem II. From the arguments in the proof of Lemma 2.5, we see that $D_n \in \mathbb{Z}$. Lemmas 2.1, 2.2 and 2.4 show that a_n, b_n and c_n satisfy all the assumptions in Theorem I. So Theorem I implies both $3 \mid h(\mathbb{Q}(\sqrt{D_n}))$ and $3 \mid h(\mathbb{Q}(\sqrt{-D_n}))$. Lemma 2.5 implies that $\{\mathbb{Q}(\sqrt{D_n}) \mid n \in \mathbb{N}\}$ has infinitely many different quadratic fields. We have completed the proof of Theorem II. ■

Example 2.6. Let $d = 1$, $a_1 = 35$, $b_1 = 12$ and $c_1 = 37$. It is easy to see that d, a_1, b_1 and c_1 satisfy all the assumptions in Theorem I. Theorem II says that D_n satisfy both $3 \mid h(\mathbb{Q}(\sqrt{D_n}))$ and $3 \mid h(\mathbb{Q}(\sqrt{-D_n}))$, and $\sharp\{\mathbb{Q}(\sqrt{D_n}) \mid n \in \mathbb{N}\} = \infty$. We have

$$\begin{aligned}
D_1 &= 1683937 = 433 \cdot 3889, \quad h(\mathbb{Q}(\sqrt{D_1})) = 12, \quad h(\mathbb{Q}(\sqrt{-D_1})) = 672,\\
D_2 &= 3050952502003085377 = 853 \cdot 5791 \cdot 111103 \cdot 5559133,\\
D_3 &= 775789415946976934474767562601 7\\
&= 31 \cdot 601 \cdot 7537 \cdot 24091 \cdot 41737 \cdot 142837 \cdot 384673609,\\
D_4 &= 45043879740675646345801459024027040863145857\\
&= 571 \cdot 2383 \cdot 3706819 \cdot 70642129 \cdot 38030787199 \cdot 3324108301201,\\
D_5 &= 2772873398095278629579791047909088599300845534390350 84897\\
&= 67 \cdot 691 \cdot 919 \cdot 28537 \cdot 14312569 \cdot 40767057750432961\\
&\quad \times 39140503009222022 9263.
\end{aligned}$$

The last term of each equality above is a prime factorization of D_n. We can check that, for every integer $1 \leq n \leq 7$, D_n is square-free.

Example 2.7. Let $d = 7$, $a_1 = 19$, $b_1 = 12$ and $c_1 = 37$. They also satisfy the assumptions of Theorem I. In this case

$$
\begin{aligned}
D_1 &= 5830279 = 7\cdot 13\cdot 79\cdot 811,\ h(\mathbb{Q}(\sqrt{D_1})) = 24,\ h(\mathbb{Q}(\sqrt{-D_1})) = 1128,\\
D_2 &= 459789053738070369 67 = 7\cdot 31\cdot 73\cdot 3187\cdot 8647\cdot 105324283,\\
D_3 &= 65814604465782226589968415476039\\
&= 7\cdot 13\cdot 787\cdot 1291\cdot 2551\cdot 34603\cdot 73681\cdot 177907\cdot 615187,\\
D_4 &= 279133894082503704397304381251464503374521319\\
&= 7\cdot 67\cdot 304583551\cdot 334934627311\cdot 583409150362848437289 1,\\
D_5 &= 19576944562662332552761857321727883617359442836774433 61287\\
&= 7\cdot 13^2\cdot 103\cdot 823\cdot 1237\cdot 9870577\cdot 5386011953359\\
&\quad\times 29685444284233378536033 7291.
\end{aligned}
$$

We can construct many families by using a, b, c in the following Proposition 2.8 as initial terms of the sequences.

PROPOSITION 2.8. *Let p and q be distinct prime numbers which are inert in the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Let integers a, b, c and a square-free integer d be such that*

$$a = p^3, \quad c = q^3, \quad db^2 = q^6 - p^6.$$

Then a, b, c and d satisfy all the assumptions of Theorem I, *and*

$$D_1 = d(p^{12} + p^6q^6 + q^{12})/3.$$

Proof. It is enough to see that a prime l is inert in $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ if and only if $2 \notin \mathbb{F}_l^3$. Here, $q^6 - p^6 \equiv 1 - 1 \equiv 0 \pmod{36}$ since $p \equiv q \equiv 1 \pmod{6}$. Thus we have $6 \mid b$. ∎

REMARK 2.9. Let T be the set of primes which are inert in $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. It follows from the Chebotarev density theorem that $\sharp T = \infty$. Siegel's theorem above implies that Proposition 2.8 also gives an infinite family we desire.

References

[A-C] N. C. Ankeny and S. Chowla, *On the divisibility of the class number of quadratic fields*, Pacific J. Math. 5 (1955), 321–324.

[H1] P. Hartung, *Explicit construction of a class of infinitely many imaginary quadratic fields whose class number is divisible by* 3, J. Number Theory 6 (1974), 279–281.

[H2] —, *Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by* 3, ibid., 276–278.

[Ho] T. Honda, *On real quadratic fields whose class numbers are multiples of* 3, J. Reine Angew. Math. 233 (1968), 101–102.

[L-N] P. Llorente and E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc. 87 (1983), 579–585.

[N] T. Nagell, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg 1 (1922), 140–150.

[R] H. Reichardt, *Arithmetische Theorie der kubischen Körper als Radikalkörper*, Monatsh. Math.-Phys. 40 (1933), 323–350.

[Sc] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander*, J. Reine Angew. Math. 166 (1932), 201–203.

[Si] C. Siegel, *Über einige Anwendungen diophantischer Approximationen*, in: Collected Works, Springer, 1966, 209–266.

[Sil] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

[W] P. J. Weinberger, *Real quadratic fields with class numbers divisible by n*, J. Number Theory 5 (1973), 237–241.

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

[Z] X. K. Zhang, *Congruences modulo* 8 *for class numbers of general quadratic fields* $\mathbb{Q}(\sqrt{m})$ *and* $\mathbb{Q}(\sqrt{-m})$, J. Number Theory 32 (1989), 332–338.

Department of Mathematics
Tokyo Metropolitan University
Hachioji, Tokyo 192-0397, Japan
E-mail: trkomatu@comp.metro-u.ac.jp

Received on 8.6.1999
and in revised form 16.5.2000 (3614)