ACTA ARITHMETICA
104.2 (2002)

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

by

TORU KOMATSU (Tokyo)

Introduction. In [A-C], [H1], [Ho], [N], [W] and [Y] their authors study the divisibility of the class number of a quadratic field and state that there exist infinitely many quadratic fields whose class numbers are divisible by 3. Hartung [H2] proves the existence of infinitely many imaginary quadratic fields whose class numbers are not divisible by 3. In this paper we show

THEOREM A. *Fix a rational integer $m \in \mathbb{Z}$ $(m \neq 0)$. Then there exist infinitely many quadratic fields $\mathbb{Q}(\sqrt{D})$ such that the class numbers of $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{mD})$ are both divisible by* 3.

In the case $m = -3$, this theorem is deduced from Scholz's theorem and a result of Honda. In fact, 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 the inequality $r \le s \le r+1$. In particular, if $3 \mid h(\mathbb{Q}(\sqrt{D}))$ for a positive integer D, then $3 \mid h(\mathbb{Q}(\sqrt{-3D}))$.*

Honda [Ho] constructed an infinite family of real quadratic fields whose class numbers are divisible by 3. These results imply that there exist infinitely many quadratic fields $\mathbb{Q}(\sqrt{D})$ such that the class numbers of $\mathbb{Q}(\sqrt{D})$ and $\mathbb{Q}(\sqrt{-3D})$ are both divisible by 3.

In [K] we showed the existence of an infinite family of quadratic fields $\mathbb{Q}(\sqrt{D})$ with $3 \mid h(\mathbb{Q}(\sqrt{D}))$ and $3 \mid h(\mathbb{Q}(\sqrt{-D}))$. Our Theorem A is a generalization of this result. The divisibility of the class number by 3 is verified by the construction of an explicit cubic polynomial which gives an unramified cyclic cubic extension of the quadratic field.

We prove Theorem A by the following construction.

Let $m \in \mathbb{Z}$ be a square-free integer with $m \neq 1$. Let l be a prime number which splits in the extension $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ and is inert in the extension

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

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. We take an integer $n \in \mathbb{Z}$ such that

$$n \equiv \begin{cases} \pm(4m-3) \pmod{27} & \text{if } m \equiv 1 \pmod 3, \\ \pm(4m+12) \pmod{27} & \text{if } m \equiv 2 \pmod 3, \\ \pm 4m \pmod{27} & \text{if } m \equiv 3 \pmod 9, \\ \pm 1 \pmod 3 & \text{otherwise,} \end{cases}$$

and $mn^2 \equiv 1 \pmod l$. Now put $r = mn^2$. Let P be the set of all prime divisors of $r(r-1)$ except 3. We denote by T the set of integers $t \in \mathbb{Z}$ which satisfy the conditions:

$$t \equiv \begin{cases} 4 \text{ or } 7 \pmod 9 & \text{if } m \equiv 1 \pmod 3, \\ 3 \pmod 9 & \text{if } m \equiv 2 \pmod 3, \\ -3 \pmod{27} & \text{if } m \equiv 3 \pmod 9, \\ \pm(r/3)^2 \pmod 9 & \text{otherwise,} \end{cases}$$

$t \equiv -1 \pmod l$ and $t \not\equiv r \pmod p$ for every $p \in P$. Decompose T into two subsets T_1 and T_2 where $T_1 = \{t \in T \mid t \geq 3r/2\}$ and $T_2 = \{t \in T \mid t < 3r/2\}$. Define

$$D_r(X) = (3X^2 + r)(2X^3 - 3(r+1)X^2 + 6rX - r(r+1))/27.$$

Let $\mathcal{F}(S)$ denote the family $\{\mathbb{Q}(\sqrt{D_r(t)}) \mid t \in S\}$ for a subset S of $\mathbb{Z}$. Then we have

THEOREM B. *For every $t \in T$, the class numbers of $\mathbb{Q}(\sqrt{D_r(t)})$ and $\mathbb{Q}(\sqrt{mD_r(t)})$ are both divisible by* 3. *Moreover, the families $\mathcal{F}(T_1)$, $\mathcal{F}(T_2)$ and $\mathcal{F}(T)$ each include infinitely many quadratic fields. In particular, when $m > 0$, the quadratic fields $\mathbb{Q}(\sqrt{D_r(t)})$ and $\mathbb{Q}(\sqrt{mD_r(t)})$ are both real* (*resp. both imaginary*) *if $t \in T_1$* (*resp. $t \in T_2$*).

Let $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{F}_p$ be the ring of rational integers, the field of rational numbers and the finite field of p elements, respectively. For a prime number p and an integer a, $v_p(a)$ is the greatest exponent n such that $p^n \mid a$. The class number of an algebraic number field F is denoted by $h(F)$.

I wish to express my deepest gratitude to Professor Masato Kurihara for his guidance, encouragement and criticism throughout my study.

1. Existence of the prime number l and the integer n. First of all we claim that there exists a prime number l which splits in $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ and is inert in $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Let $\mathcal{L}$ be the set of all such primes l.

LEMMA 1.1. *The set $\mathcal{L}$ is infinite.*

Proof. Put $M_1 = \mathbb{Q}(\sqrt{m}, \sqrt{-3}, \sqrt[3]{2})$ and $M_2 = \mathbb{Q}(\sqrt{m}, \sqrt{-3})$. Then M_1 is Galois over $\mathbb{Q}$. Let σ be an element of the Galois group $G = \mathrm{Gal}(M_1/\mathbb{Q})$ such that $\langle\sigma\rangle = \mathrm{Gal}(M_1/M_2)$. It is easy to see that the conjugate class C of σ in G is $\{\sigma, \sigma^2\}$. We note that $l \in \mathcal{L}$ splits in $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ since l is inert in

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. In fact, $\mathbb{Q}(\sqrt{-3},\sqrt[3]{2})/\mathbb{Q}$ is a Galois extension whose group is not cyclic. Thus, for every prime ideal $\mathfrak{l}$ of M_1 lying above $l \in \mathcal{L}$, the Frobenius automorphism of $\mathfrak{l}$ is σ or σ^2. Conversely, if the Frobenius automorphism of a prime $\mathfrak{l}_0$ of M_1 is σ or σ^2, then the prime l_0 below $\mathfrak{l}_0$ belongs to $\mathcal{L}$. It follows from the Chebotarev density theorem [T] that

$$\lim_{s\to 1+0}\left(\log\frac{1}{s-1}\right)^{-1}\sum_{l\in\mathcal{L}}\frac{1}{l^s}=\frac{|C|}{|G|}=\begin{cases}1/3 & \text{if } m=-3,\\ 1/6 & \text{otherwise.}\end{cases}$$

In particular, the set $\mathcal{L}$ has infinitely many primes. ∎

To end this section we show the existence of the integer n which is taken for our construction in the introduction. Note that $l\neq 3$. Indeed, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is totally ramified at 3. From the assumption that l splits in $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$, we have $m\in\mathbb{F}_l^{\times 2}$, that is, there exists an integer z_0 satisfying $z_0^2\equiv m \pmod{l}$. Then we also have an integer z_1 such that $z_0z_1=1 \pmod{l}$ since z_0 is invertible in $\mathbb{F}_l$. Let z_2 be an integer. The Chinese remainder theorem implies that there exist infinitely many integers z so that $z\equiv \pm z_1 \pmod{l}$ and $z\equiv z_2 \pmod{3^3}$. The integer n is one of such z's.

So Theorem A follows from Theorem B.

2. Proof of Theorem B. Let m,l,n,r,P and T be as in the introduction. Here T is an infinite set by the Chinese remainder theorem. We shall show that $3\,|\,h(\mathbb{Q}(\sqrt{D_r(t)}))$ and $3\,|\,h(\mathbb{Q}(\sqrt{mD_r(t)}))$ for each $t\in T$. For a fixed $t\in T$, we put $u=t^3+3tr$, $w=3t^2+r$, $a=u-w$, $b=u-rw$ and $c=t^2-r$. Then u,w,a,b and c are integers such that $(t+\sqrt{r})^3=u+w\sqrt{r}$ and $ra^2-b^2=(r-1)c^3$.

Lemma 2.1. *The integer c is odd and* $\gcd(ab,c)=3^e$ *for some* $e\in\mathbb{Z}$.

Proof. Note that $2\in P$ since $r(r-1)$ is even. By the assumption $t\not\equiv r \pmod{2}$, $c=t^2-r$ is odd. Let p be a prime divisor of $\gcd(ab,c)$. Then we have $r\equiv t^2 \pmod{p}$ and $ab=(u-w)(u-rw)\equiv -2^4t^5(t-1)^2\equiv 0 \pmod{p}$. Here, c is odd and so is p. This means that $t\equiv 0$ or $1 \pmod{p}$. If $t\equiv 0 \pmod{p}$, then $r\equiv 0 \pmod{p}$. This implies that $p\in P$ or $p=3$. Since $t\equiv r\equiv 0 \pmod{p}$, we see $p\notin P$ and thus $p=3$. When $t\equiv 1 \pmod{p}$, we have $r\equiv 1 \pmod{p}$, which also yields $p=3$. Hence, $\gcd(ab,c)=3^e$ for some $e\in\mathbb{Z}$. ∎

Define $f_1(Z)=Z^3-3cZ-2a$ and $f_2(Z)=Z^3-3cZ-2b$.

Lemma 2.2. *The polynomials $f_1(Z)$ and $f_2(Z)$ are both irreducible over $\mathbb{F}_l$. In particular, $f_1(Z)$ and $f_2(Z)$ are both irreducible over $\mathbb{Q}$.*

Proof. It follows from the definition that $r\equiv 1 \pmod{l}$ and $t\equiv -1 \pmod{l}$. Then $a\equiv b\equiv -2^3 \pmod{l}$ and $c\equiv 0 \pmod{l}$. Thus, $f_i(Z)\equiv Z^3+2^4 \pmod{l}$ for each $i=1,2$. Since l is inert in $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, Z^3-2 is irreducible over $\mathbb{F}_l$ and so is Z^3+2^4. Therefore $f_i(Z)$ is irreducible over $\mathbb{F}_l$, and hence also over $\mathbb{Q}$. ∎

Let $f(Z)$ be an irreducible cubic polynomial of the form $f(Z)=Z^3-\alpha Z-\beta$ for $\alpha,\beta\in\mathbb{Z}$. We denote by K_f the minimal splitting field of $f(Z)$ over $\mathbb{Q}$, and $k_f=\mathbb{Q}(\sqrt{4\alpha^3-27\beta^2})$ ($\subset K_f$). Assume $\gcd(\alpha,\beta)=3^\varepsilon$ for some $\varepsilon\in\mathbb{Z}$. Let δ be the maximal integer such that $\alpha/3^{2\delta},\beta/3^{3\delta}\in\mathbb{Z}$. We put $\alpha_0=\alpha/3^{2\delta}$ and $\beta_0=\beta/3^{3\delta}$.

PROPOSITION LN ([L-N], [R]). *The extension K_f/k_f is unramified if one of the following conditions holds*:

(i) $3\nmid\alpha_0$,
(ii) $v_3(\alpha_0)=1$ *and* $v_3(\beta_0)\geq 2$,
(iii) $\alpha_0\equiv 3\pmod 9$ *and* $\beta_0^2\equiv\alpha_0+1\pmod{27}$.

REMARK 2.3. In [L-N] and [R] more general conditions are considered. However, Proposition LN is enough for us to show Lemma 2.4 below.

LEMMA 2.4. *The extensions K_{f_1}/k_{f_1} and K_{f_2}/k_{f_2} are both unramified.*

We need the following lemma.

LEMMA 2.5. *We have*

$$r\equiv\begin{cases}1\pmod{3^3} & \textit{if } m\equiv 1\pmod 3,\\ -10\pmod{3^3} & \textit{if } m\equiv 2\pmod 3,\\ -2\cdot 3^3\pmod{3^5} & \textit{if } m\equiv 3\pmod 9,\\ -3\pmod{3^2} & \textit{otherwise.}\end{cases}$$

Proof. When $m\equiv 1\pmod 3$, we have

$$r\equiv m(4m-3)^2=(m-1)(4m-1)^2+1\equiv 1\pmod{27}.$$

If $m\equiv 2\pmod 3$, then $r\equiv m(4m+12)^2=16(m+1)^2(m+4)-64\equiv -10\pmod{27}$. Assume $m\equiv 3\pmod 9$. Then we have $r/3^3=(m/3)(n/3)^2\equiv 16(m/3)^3\pmod 9$. It follows from $m/3\equiv 1\pmod 3$ that $(m/3)^3\equiv 1\pmod 9$. Thus, $r/3^3\equiv -2\pmod 9$ and $r\equiv -2\cdot 3^3\pmod{3^5}$. For the case $m\equiv 6\pmod 9$, we have $r\equiv m\equiv -3\pmod 9$. ∎

Proof of Lemma 2.4. We first assume $m\equiv 1\pmod 3$. By the definition, $t\equiv 4$ or $7\pmod 9$. Then $c=t^2-r\equiv 0\pmod 3$ and $c\not\equiv 0\pmod 9$. This means $v_3(c)=1$. On the other hand, $u\equiv t^3+3t\pmod{27}$ and $w\equiv 3t^2+1\pmod{27}$. Thus we have $a\equiv b\equiv(t-1)^3\equiv 0\pmod{27}$, that is, $v_3(a)\geq 3$ and $v_3(b)\geq 3$. It follows from Lemmas 2.1 and 2.2 that $f_1(Z)$ and $f_2(Z)$ satisfy the assumptions of Proposition LN. Hence Proposition LN(i) shows that K_{f_1}/k_{f_1} and K_{f_2}/k_{f_2} are both unramified.

When $m\equiv 2\pmod 3$, we have $r\equiv -10\pmod{27}$ and $t\equiv 3\pmod 9$. This implies that $a\equiv 1\pmod{27}$, $b\equiv -1\pmod{27}$ and $c\equiv 1\pmod 9$. Thus K_{f_1}/k_{f_1} and K_{f_2}/k_{f_2} are both unramified by Proposition LN(iii).

If $m \equiv 3 \pmod 9$, then $v_3(a) \geq 3$, $v_3(b) \geq 3$ and $v_3(c) = 2$. Put $r_0 = r/3^3$ and $t_0 = t/3$. Then $r_0 \equiv -2 \pmod 9$ and $t_0 \equiv -1 \pmod 9$. This means that $a/3^3 = t_0^3 - t_0^2 + 9t_0r_0 - r_0 \equiv 0 \pmod 9$ and $c/3^2 = t_0^2 - 3r_0 \equiv 1 \pmod 3$. Proposition LN(ii) implies that K_{f_1}/k_{f_1} is unramified. On the other hand, we have $b/3^3 \equiv t_0^3 + 9t_0r_0 \pmod{27}$. Then $(2b/3^3)^2 - 3c/3^2 - 1 \equiv 4(t_0^6 + 18t_0^4 r_0) - 3t_0^2 + 9r_0 - 1 = (t_0^2 - 1)(2t_0^2 + 1)^2 + 9(8t_0^4 + 1)r_0 \equiv 0 \pmod{27}$. Thus Proposition LN(iii) shows that K_{f_2}/k_{f_2} is unramified.

Finally we consider the case $m \equiv 6 \pmod 9$. It follows from $t \equiv \pm(r/3)^2 \pmod 9$ that $t^2 \equiv (r/3)^4 \pmod 9$. By Lemma 2.5 we have $r/3 \equiv -1 \pmod 3$ and $(r/3)^3 \equiv -1 \pmod 9$. Thus, $t^2 \equiv -r/3 \pmod 9$ and $r \equiv -3t^2 \pmod{27}$. This implies that $a \equiv b \equiv -8t^3 \pmod{27}$ and $c \equiv 4t^2 \pmod{27}$. Then we have $4a^2 - 3c - 1 \equiv 4b^2 - 3c - 1 \equiv 13t^6 - 12t^2 - 1 = (t^2 - 1)(2t^2 + 1)^2 + 9t^2(t^4 - 1) \equiv 0 \pmod{27}$. Hence K_{f_1}/k_{f_1} and K_{f_2}/k_{f_2} are both unramified from Proposition LN(iii). ∎

By the definition we have

$$\begin{aligned} 4(3c)^3 - 27(2a)^2 &= 108(3t^2 + r)(2t^3 - 3(r+1)t^2 + 6rt - r(r+1)) \\ &= 54^2 D_r(t), \\ 4(3c)^3 - 27(2b)^2 &= 108r(3t^2 + r)(2t^3 - 3(r+1)t^2 + 6rt - r(r+1)) \\ &= (54n)^2 m D_r(t). \end{aligned}$$

Thus, $k_{f_1} = \mathbb{Q}(\sqrt{D_r(t)})$ and $k_{f_2} = \mathbb{Q}(\sqrt{mD_r(t)})$. Lemma 2.4 and class field theory imply

PROPOSITION 2.6. *The class numbers of* $\mathbb{Q}(\sqrt{D_r(t)})$ *and* $\mathbb{Q}(\sqrt{mD_r(t)})$ *are both divisible by* 3 *for every* $t \in T$.

Recall that $\mathcal{F}(S)$ is the family $\{\mathbb{Q}(\sqrt{D_r(t)}) \mid t \in S\}$ for $S \subset \mathbb{Z}$. We next show

PROPOSITION 2.7. *The families* $\mathcal{F}(T_1)$, $\mathcal{F}(T_2)$ *and* $\mathcal{F}(T)$ *each include infinitely many quadratic fields.*

Proof. Assume $S \neq \emptyset$ is a subset of T such that $\mathcal{F}(S)$ is finite. We will choose t_0 from T so that $\mathcal{F}(S) \subsetneq \mathcal{F}(S \cup \{t_0\})$. Let M_S be the composite field of all quadratic fields which belong to $\mathcal{F}(S)$, and P_S the set of prime numbers ramifying in $M_S/\mathbb{Q}$. We note that P_S is finite since $M_S/\mathbb{Q}$ is of finite degree. Thus there exists a prime number q such that $q \notin P \cup P_S \cup \{3\}$ and $3x^2 + r \equiv 0 \pmod q$ for some $x \in \mathbb{Z}$. Taking such a q with x, we define $x_0 = x$ or $x_0 = x + q$ according to whether $3x^2 + r \not\equiv 0 \pmod{q^2}$ or not. This implies that $3x_0^2 + r \equiv 0 \pmod q$ and $3x_0^2 + r \not\equiv 0 \pmod{q^2}$.

Now we put $g_r(X) = 2X^3 - 3(r+1)X^2 + 6rX - r(r+1)$. Then $D_r(X) = (3X^2 + r)g_r(X)/27$ and $3g_r(X) = (2X - 3r - 3)(3X^2 + r) + 16rX$. When

$g_r(x_0) \equiv 0 \pmod{q}$, we have $16rx_0 \equiv 0 \pmod{q}$, which contradicts the assumption on q and x. Hence, $D_r(x_0) \equiv 0 \pmod{q}$ and $D_r(x_0) \not\equiv 0 \pmod{q^2}$. On the other hand, there exists $t_0 \in T$ such that $t_0 \equiv x_0 \pmod{q^2}$ by $q \notin P \cup \{3\}$ and the Chinese remainder theorem. Then we have $D_r(t_0) \equiv D_r(x_0) \equiv 0 \pmod{q}$ and $D_r(t_0) \equiv D_r(x_0) \not\equiv 0 \pmod{q^2}$. This shows that q ramifies in $\mathbb{Q}(\sqrt{D_r(t_0)})/\mathbb{Q}$ and in $M_S(\sqrt{D_r(t_0)})/\mathbb{Q}$. Since $M_S/\mathbb{Q}$ is not ramified at q, we have $M_S \subsetneq M_S(\sqrt{D_r(t_0)})$ and $\mathcal{F}(S) \subsetneq \mathcal{F}(S \cup \{t_0\})$.

Here the family $\mathcal{F}(S \cup \{t_0\})$ is also finite. Hence we may construct an infinite increasing sequence of subsets S_i of T such that $\mathcal{F}(S) \subsetneq \mathcal{F}(S_1) \subsetneq \mathcal{F}(S_2) \subsetneq \ldots$ where $S \subsetneq S_1 \subsetneq S_2 \subsetneq \ldots$ This means that $\mathcal{F}(T)$ is infinite. In the same way we show that $\mathcal{F}(T_1)$ and $\mathcal{F}(T_2)$ are also infinite. ∎

REMARK 2.8. By using Siegel's theorem (cf. [Si] or [Sil]) we can prove Proposition 2.7 in the same manner as in [K].

Finally we study when $\mathbb{Q}(\sqrt{D_r(t)})$ and $\mathbb{Q}(\sqrt{mD_r(t)})$ are both real (or both imaginary). If $m < 0$, then one of $\mathbb{Q}(\sqrt{D_r(t)})$ and $\mathbb{Q}(\sqrt{mD_r(t)})$ is real, and the other imaginary. For the case $m > 0$, we have the following criterion:

PROPOSITION 2.9. *Assume $m > 0$. Then $\mathbb{Q}(\sqrt{D_r(t)})$ and $\mathbb{Q}(\sqrt{mD_r(t)})$ are both real* (*resp. both imaginary*) *if $t \in T_1$* (*resp. $t \in T_2$*).

This follows immediately from

LEMMA 2.10. *When $r \geq 2$, we have $D_r(t) > 0$ if and only if $t \geq 3r/2$.*

Proof. Recall that $D_r(t) = (3t^2+r)g_r(t)/27$ where $g_r(t) = 2t^3 - 3(r+1)t^2 + 6rt - r(r+1)$. Since r is positive, the sign of $D_r(t)$ coincides with that of $g_r(t)$. The derivative of $g_r(X)$ is equal to $\partial g_r(X)/\partial X = 6(X-1)(X-r)$. It is easily seen that $g_r(1) = -(r-1)^2 < 0$. This means that $g_r(X) = 0$ has only one real root. By some calculation we find that $g_r(3r/2 - 1/2) = -(r-1)^2 < 0$ and $g_r(3r/2) = r(5r-4)/4 > 0$. This shows that $g_r(t) > 0$ if and only if $t \geq 3r/2$. Hence $D_r(t) > 0$ is equivalent to $t \geq 3r/2$. ∎

Concerning the $D_r(X)$, we make the following remark. Generally $D_r(x)$ is not an integer for some $x \in \mathbb{Z}$. However,

LEMMA 2.11. *For every m and every $t \in T$, $D_r(t)$ is an integer.*

Proof. If $m \equiv 1$ or $2 \pmod{3}$, then $g_r(t) \equiv 0 \pmod{27}$ from Lemma 2.5 and the definition of t in the introduction. When $m \equiv 3 \pmod{9}$, we have $3t^2 + r \equiv 0 \pmod{27}$ since $27 \mid r$ and $3 \mid t$. For the case $m \equiv 6 \pmod{9}$, it is already shown in the proof of Lemma 2.4 that $3t^2 + r \equiv 0 \pmod{27}$. Hence $D_r(t) = (3t^2+r)g_r(t)/27 \in \mathbb{Z}$. ∎

Propositions 2.6, 2.7 and 2.9 imply Theorem B.

3. Some examples and remarks pertaining to Theorem B. For each square-free integer $m \neq 1$ in a range of m we calculated the smallest l, the smallest $|n|$ and several $t \in T$ as in the introduction. Table 3.1 contains the results for the case $1 < m \le 10$. Here we take the integers t from T_1 and T_2 nearest to $3r/2$. In Table 3.2, $-10 < m \le -1$. For each m in Table 3.2, t is the smallest positive integer in T. We set $P_0 = P \setminus \{2, l\}$.

Table 3.1 ($m > 0$)

m	l	n	r	P_0	t	$D_r(t)$
2	7	47	4418	$\{47, 631\}$	6663	15886218131390125
					6537	−36400989613740975
3	13	42	5292	$\{7, 11, 37\}$	8475	615850683070207599
					7773	−133604270796204909
5	19	59	17405	$\{5, 59, 229\}$	26238	13772800490106893922
					25896	−21107438412836157274
6	19	4	96	$\{5\}$	227	48814901243
					−115	−10260589521
7	19	83	48223	$\{7, 47, 83\}$	72484	918746050940607703528
					72256	−473811154617323131552
10	13	37	13690	$\{5, 37\}$	20617	3303268105263818329
					20383	−5819433986897632763

Table 3.2 ($m < 0$)

m	l	n	r	P_0	t	$D_r(t)$
−1	13	8	−64	$\{5\}$	129	13637284103
−2	19	16	−512	$\emptyset$	151	103381223923
−3	7	4	−48	$\emptyset$	13	377791
−5	7	23	−2645	$\{5, 23\}$	34	52276960
−6	7	57	−19494	$\{5, 19, 557\}$	699	1542419323812333
−7	37	124	−107632	$\{7, 31, 2909\}$	813	14056744007830975

REMARK 3.1. Tables 3.1 and 3.2 enable us to guess that the absolute values $|D_r(t)|$ would be too big in general. We could probably find D smaller than $|D_r(t)|$ such that both $3 \mid h(\mathbb{Q}(\sqrt{D}))$ and $3 \mid h(\mathbb{Q}(\sqrt{mD}))$.

For each integer $m \neq 0$, let $\mathfrak{D}_m$ be the set of integers D such that $3 \mid h(\mathbb{Q}(\sqrt{D}))$ and $3 \mid h(\mathbb{Q}(\sqrt{mD}))$. Put $\mathfrak{D}_m^+ = \{D \in \mathfrak{D}_m \mid D > 0\}$ and $\mathfrak{D}_m^- = \{D \in \mathfrak{D}_m \mid D < 0\}$. Theorem B implies that $\mathfrak{D}_m^+$ and $\mathfrak{D}_m^-$ are both infinite. Some values of $D_m^+ = \min \mathfrak{D}_m^+$ and $D_m^- = \max \mathfrak{D}_m^-$ are given in Table 3.3.

REMARK 3.2. Theorem B presents an infinite family of pairs of quadratic fields $k_1 = \mathbb{Q}(\sqrt{D})$ and $k_2 = \mathbb{Q}(\sqrt{mD})$ which have unramified cyclic cubic extensions K_1 and K_2 satisfying the condition that any prime ideals of k_1 and k_2 above the fixed l are inert in K_1/k_1 and K_2/k_2, respectively (cf. Lemma 2.2). Without this condition we may find D smaller than in Table 3.3.

Table 3.3

m	D_m^+	D_m^-	m	D_m^+	D_m^-
2	761	-53	-1	473	-473
3	1478	-29	-2	359	-393
5	934	-139	-3	79	-107
6	1229	-29	-5	229	-157
7	733	-26	-6	321	-214
10	223	-61	-7	229	-61

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.

[K] T. Komatsu, *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, Acta Arith. 96 (2001), 213–221.

[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. Nagel, *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 Curve*, Springer, New York, 1986.

[T] N. Tschebotareff [N. Chebotarev], *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*, Math. Ann. 95 (1926), 191–228.

[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.

Department of Mathematics
Tokyo Metropolitan University
Minami-Ohsawa 1-1, Hachioji-shi
Tokyo 192-0397, Japan
E-mail: trkomatu@comp.metro-u.ac.jp

Received on 27.12.2000 (3935)