36. Determination of Certain Real Quadratic Fields with Class Number Two

By Hisao TAYA and Nobuhiro TERAI
Department of Mathematics, Waseda University

(Communicated by Shokichi IYANAGA, M. J. A., May 13, 1991)

§1. Introduction. Let D be a square-free integer of the form $D=m^2+r$ where $-m<r\leq m$ and $r\mid 4m$. Then a real quadratic field $\boldsymbol{Q}(\sqrt{D})$, or simply D, is said to be of *R-D type*. If $r=\pm 1$ or ± 4, then D is said to be of *narrow R-D type*. Let $k=\boldsymbol{Q}(\sqrt{D})$ be a real quadratic field of R-D type with discriminant d_k. We denote by h_k and χ_k the class number and the Kronecker character of k, respectively.

In 1951, Tatuzawa [6] proved that for $v\geq 11.2$ and $d_k\geq e^v$,

$$L(1,\chi_k)>\frac{0.655 d_k^{-1/v}}{v}$$

with one possible exception of d_k, where $L(s,\chi_k)$ is the Dirichlet L-function for χ_k. Using this result, the problem of determining all k's of R-D type under given conditions, with one possible exception which can be eliminated under the assumption of the generalized Riemann Hypothesis (cf. Remark 2), has been successfully solved by the following authors: $h_k=1$ for $r=1$ or 4 by Kim, Leu and Ono [2], $h_k=2$ for $r=1$ or 4 by Leu [3] and $h_k=1$ for general R-D type by Mollin and Williams [4].

In this paper we shall solve this problem for $h_k=2$, k being of narrow R-D type, by using the theory of the 2-part of the ideal class group of quadratic fields in addition to the usual methods.

Throughout this paper, we denote by h_k^+ and ε_k (>1) the class number in the narrow sense and the fundamental unit of k, respectively. Let N be the absolute norm from k and t be the number of distinct prime factors of d_k.

§2. Some lemmas. We first prepare some lemmas. For a square-free integer $d>1$ and a natural number $n>1$, we say that an integral solution (x,y) of the equation $x^2-dy^2=\pm 4n$ is *trivial* if and only if $n=s^2$ is a square and $x\equiv y\equiv 0 \pmod{s}$.

Lemma 1 (Yokoi [8]). *Let $d>1$ be a square-free integer and $n>1$ a natural number. We denote the fundamental unit of the real quadratic field $k=\boldsymbol{Q}(\sqrt{d})$ by $\varepsilon_k=(u+v\sqrt{d})/2>1$, and put $B_k=u/v^2$ or $(u-2)/v^2$ according as $N(\varepsilon_k)=-1$ or 1. Then the equation $x^2-dy^2=\pm 4n$ has no non-trivial integral solutions unless $n\geq B_k$.*

Lemma 2. *We fix a positive integer c. Let d and B_k be as in Lemma 1 and p any prime dividing d.*

(a) *If there exists a prime l such that $\chi_k(l)=1$ and $l^c<B_k$, then $h_k>c$.*

(b) *If there exists a prime l such that $\chi_k(l)=1$ and $pl^c<B_k$, then $h_k>2c+1$.*

Proof. (a) Let l be a prime number such that $\chi_k(l)=1$ and $l^c<B_k$. Then $(l)=\mathfrak{l}\mathfrak{l}'$ in k, where $\mathfrak{l}\neq\mathfrak{l}'$. We assume that $\mathfrak{l}^e$ is a principal ideal for some e $(1\leq e\leq c)$, so that $\mathfrak{l}^e=((x+y\sqrt{d})/2)$ for some integers x, y, where x, y are not divisible by l. Since $l^e=|N(\mathfrak{l}^e)|=|N((x+y\sqrt{d})/2)|$, we have

$$x^2-dy^2=\pm 4l^e \qquad \text{for some integers } x, y.$$

However, this contradicts Lemma 1. Therefore $\mathfrak{l}^e$ is non-principal for each e, so we have $h_k>c$.

(b) Let l be a prime number such that $\chi_k(l)=1$ and $pl^c<B_k$. Then $(l)=\mathfrak{l}\mathfrak{l}'$ $(\mathfrak{l}\neq\mathfrak{l}')$ and $(p)=\mathfrak{p}^2$ in k. Since p, l^i and pl^j $(1\leq i, j\leq c)$ are less than B_k, Lemma 1 implies that $\mathfrak{p}, \mathfrak{l}^i$ and $\mathfrak{p}\mathfrak{l}^j$ are non-principal ideals. Now it is easy to see that the above $2c+1$ ideals belong to distinct ideal classes. Therefore we have $h_k>2c+1$. Q.E.D.

Lemma 3. *The possible forms of narrow R-D type are as follows.*

(1) *Case $D=m^2+4$: If $h_k=2$, then $D=pq$ and m is odd.*

(2) *Case $D=m^2+1$: If $h_k=2$, then $D=pq$ and m is even, or $D=2p$ and m is odd.*

(3) *Case $D=m^2-4$: If $h_k=2$, then $D=pq$ or pqr, and m is odd.*

(4) *Case $D=m^2-1$: If $h_k=2$, then $D=pq$ and m is even.*

In the above, p, q and r are odd primes such that $p<q<r$.

Proof. (1) and (2) are proved in [3]. We first prove (3). Let h_k^* be the number of genera. Here we note that, if the discriminant of a quadratic field has only one prime factor, then its class number is odd. Since $N(\varepsilon_k)=1$, we have $2h_k=h_k^+=2^{t-1}h_k^*$. Hence if $h_k=2$, then $4=2^{t-1}h_k^*$. So we have $t=2$ or 3, $D=d_k=pq$ or pqr and m is odd.

We can prove (4) similarly, noting that $N(\varepsilon_k)=1$ and $d_k=4(m+1)(m-1)$. Q.E.D.

In the cases $D=m^2+4$ and $D=m^2+1$, Leu proved the following lemma in [3].

Lemma 4. *The possible forms of m are as follows.*

(1) *Case $D=m^2+4$: If $h_k=2$, then $m=s^d$.*

(2) *Case $D=m^2+1$: If $h_k=2$, then $m=8, 2s^d$ (resp. $m=s$) for even (resp. odd) m.*

In the above, s is odd prime number and $d=1, 2$.

We further consider the 2-part of ideal class groups. Genus theory of quadratic fields tells us that the 2-rank of a narrow class group is equal to $t-1$. So if the narrow class group of a quadratic field has a cyclic subgroup of degree 4, then its class number in the narrow sense is divisible by 2^t.

As is well-known, we have $d_k=d_1d_2$, where $(d_1, d_2)=1$ and d_i is the discriminant of some quadratic field or equal to one $(i=1, 2)$. This decomposition of d_k is called *d-decomposition*. We now assume that $d_k=d_1d_2$ is a non-trivial d-decomposition, i.e. $d_1\neq 1$ and $d_2\neq 1$. Then we say that a

d-decomposition is of *the second kind* when there exists an unramified cyclic extension over k of degree 4 including $k(\sqrt{d_1})$ in the narrow absolute class field of k. Then Rédei-Reichardt [5] proved the following theorem.

Theorem A (Rédei-Reichardt [5]). *Let $d_k=d_1d_2$ be a non-trivial d-decomposition. Then $d_k=d_1d_2$ is of the second kind if and only if $(d_2/p)=1$ for all prime factors p of d_1 and $(d_1/q)=1$ for all prime factors q of d_2, where $(*/*)$ denotes the Kronecker symbol.*

Moreover, Yamamoto [7] gave necessary and sufficient conditions for h_k^+ to be divisible by a power of 2 when $t=2$. Using those results, we obtain the following lemma.

Lemma 5. *Let $(*/*)_4$ be the biquadratic residue symbol and p, q, r be odd primes.*

(1) *Case $D=m^2+4$: For $D=pq$ $(d_k=pq)$, $(p/q)=1\Longleftrightarrow 4\mid h_k$.*

(2) *Case $D=m^2+1$:*

(A) *For $D=pq$ $(d_k=pq)$ and even m, $(p/q)=1\Longleftrightarrow 4\mid h_k$.*

(B) *For $D=2p$ $(d_k=8p)$ and odd m, $p\equiv 1 \pmod 8\Longleftrightarrow 4\mid h_k$.*

(3) *Case $D=m^2-4$:*

(A) *For $D=pq$ $(d_k=pq)$,*

a. *if $p\equiv q\equiv 3 \pmod 4$, then h_k is odd,*

b. *if $p\equiv q\equiv 1 \pmod 4$, then $(p/q)=1\Longleftrightarrow 2\mid h_k$, and $(p/q)_4=(q/p)_4=1\Longleftrightarrow 4\mid h_k$.*

(B) *For $D=pqr$ $(d_k=pqr)$,*

a. *if $p\equiv q\equiv r\equiv 1 \pmod 4$, then at most one value of (p/q), (p/r), (q/r) is $-1\Longleftrightarrow 4\mid h_k$,*

b. *if two of the prime factors are congruent to 3 (mod. 4) and the other is congruent to 1 (mod. 4), say $p\equiv q\equiv 3$, $r\equiv 1 \pmod 4$, then $(r/p)=(r/q)=1\Longleftrightarrow 4\mid h_k$.*

(4) *Case $D=m^2-1$: For $D=pq$ $(d_k=4pq)$, if $p\equiv 3$ and $q\equiv 1 \pmod 4$, then $q\equiv 1 \pmod 8$ and $(q/p)=1\Longleftrightarrow 4\mid h_k$.*

Proof. (1) and (2). Assume that $D=m^2+4=pq$ or $D=m^2+1=pq, 2p$. Note that $p\equiv 1 \pmod 4$ for all odd prime factors p of D, since $N(\varepsilon_k)=-1$. The 2-part of the narrow ideal class group is cyclic, so $4\mid h_k^+$ is equivalent to the fact that the d-decomposition $d_k=D=pq$ (or $2p$) is of the second kind. Hence from Theorem A, we have

$$\begin{cases} 4\mid h_k=h_k^+ \Longleftrightarrow (p/q)=1 \text{ and } (q/p)=1 \Longleftrightarrow (p/q)=1. \\ 4\mid h_k=h_k^+ \Longleftrightarrow (8/p)=1 \text{ and } (p/2)=1 \Longleftrightarrow p\equiv 1 \pmod 8. \end{cases}$$

(3) Assume that $D=m^2-4=pq$ or pqr. We then note that $2h_k=h_k^+$. Similarly from Theorem A we obtain the condition for h_k^+ to be divisible by 2^t. Also when $t=2$, we obtain the condition for h_k^+ to be divisible by 8 from Proposition 3.3 of Yamamoto [7]. Therefore the conclusion follows immediately.

The other case follows from a similar argument. Q.E.D.

§ 3. Determination of quadratic fields with class number two. From

lemmas in the previous section, we immediately obtain the following theorems.

Theorem 1. *For $k=\boldsymbol{Q}(\sqrt{D})$ and $D=m^2+4$, if $h_k=2$, then we have*

(1) *$D=pq$, where p and q $(p<q)$ are odd primes,*

(2) *$m=s^d$, where s is an odd prime and $d=1$ or 2,*

(3) *if a prime l is such that $\chi_k(l)=1$, then $l^2\geq m$ and $pl\geq m$,*

(4) *$(p/q)=-1$.*

Theorem 2. *For $k=\boldsymbol{Q}(\sqrt{D})$ and $D=m^2+1$, if $h_k=2$, then we have the following. When m is even (resp. odd),*

(1) *$D=pq$ (resp. $D=2p$), where p and q $(p<q)$ are odd primes,*

(2) *$m=8$ or $2s^d$ (resp. $m=s$), where s is an odd prime and $d=1$ or 2,*

(3) *if a prime l is such that $\chi_k(l)=1$, then $4l^2\geq 2m$ and $4pl\geq 2m$ (resp. $2l\geq 2m$),*

(4) *$(p/q)=-1$ (resp. $p\not\equiv 1 \pmod 8$).*

Theorem 3. *For $k=\boldsymbol{Q}(\sqrt{D})$ and $D=m^2-4$, if $h_k=2$, then we have*

(1) *$D=pq$ or pqr, where p, q and r $(p<q<r)$ are odd primes,*

(2) *if a prime l is such that $\chi_k(l)=1$, then $l^2\geq m-2$ and $pl\geq m-2$.*

Moreover if $D=pq$, then

(3) *$p\equiv q\equiv 1 \pmod 4$ and $(p/q)=1$ and at least one value of $(p/q)_4$, $(q/p)_4$ is -1.*

Moreover if $D=pqr$, then

(4) *if $p\equiv q\equiv r\equiv 1 \pmod 4$, then at most one value of (p/q), (p/r), (q/r) is 1,*

(5) *if two of the prime factors are congruent to 3 (mod. 4) and the other is congruent to 1 (mod. 4), say $p\equiv q\equiv 3$, $r\equiv 1 \pmod 4$, then $(r/p)\neq 1$, or $(r/q)\neq 1$.*

Theorem 4. *For $k=\boldsymbol{Q}(\sqrt{D})$ and $D=m^2-1$, if $h_k=2$, then we have*

(1) *$D=pq$, where p and q $(p<q)$ are odd primes,*

(2) *if a prime l is such that $\chi_k(l)=1$, then $2l\geq 2m-2$,*

(3) *if one of the prime factors is congruent to 3 (mod. 4) and the other is congruent to 1 (mod. 4), say $p\equiv 3$, $q\equiv 1 \pmod 4$, then $(q/p)\neq 1$ or $q\not\equiv 1 \pmod 8$.*

On the other hand, by applying Siegel-Tatuzawa theorem [6], we obtain an upper bound for D of narrow R-D type with class number two.

Proposition 1. *There exists at most one D of narrow R-D type with $D\geq e^{16}$ and $h_k\leq 2$.*

Proof. By Dirichlet's class number formula and Theorem 2 of [6], for $v\geq 11.2$ and $d_k\geq e^v$, we have

$$h_k=\frac{\sqrt{d_k}}{2\log\varepsilon_k}L(1,\chi_k)>\frac{\sqrt{d_k}}{2\log\varepsilon_k}\frac{0.655d^{-1/v}}{v}$$

with one possible exception of d_k. We note that $\varepsilon_k=(m+\sqrt{D})/2$ (resp. $m+\sqrt{D}$) if $D=m^2\pm 4$ (resp. $D=m^2\pm 1$), so we have $\varepsilon_k<2\sqrt{D}+1$, $d_k\geq D$ in each case. Hence if we put $v=16$, then we get

$$h_k > \frac{0.655}{2\log(2\sqrt{D}+1)}\frac{D^{7/16}}{16} > \frac{0.655}{16}\frac{D^{7/16}}{2\log 3\sqrt{D}} > \frac{0.655}{16}\frac{D^{7/16}}{3+\log D}.$$

Since $f(x)=x^{7/16}/(3+\log x)$ is increasing in $[e^{16}, \infty)$, we obtain

$$h_k > \frac{0.655}{16} f(e^{16}) = 2.36\cdots > 2.$$

This proves that $h_k>2$ for all $D\geq e^{16}$ with one possible exception of D. Q.E.D.

By the help of a computer (using Kida's UBASIC 86), we can list all D's of narrow R-D type which satisfy the necessary conditions of each theorem of ours and $D\leq e^{16}$. The table is given below. Then, checking the class number of these quadratic fields, we have the following theorem.

Theorem 5. *There exist* 28 *D's of narrow R-D type such that* $h_k=2$ *with one possible exception of* D.

(1) *If* $D=m^2+4$, *then* $D=85$, 365, 533, 629, 965, 1685, 1853, 2813.

(2) *If* $D=m^2+1$, *then* $D=10$, 26, 65, 122, 362, 485, 1157, 2117, 3365*.

(3) *If* $D=m^2-4$, *then* $D=165$, 221, 285, 357, 957, 1085, 1517, 2397.

(4) *If* $D=m^2-1$, *then* $D=15$, 35, 143.

Remark 1. It should be noted that the number marked with $*$ in the above theorem, i.e. $D=3365=58^2+1$, is lacking in Leu's paper [3]. We think that our method is more effective for determination of quadratic fields with $h_k=4$.

Remark 2. Assuming the generalized Riemann Hypothesis, Kim [1] proved that the Siegel-Tatuzawa theorem [6] is true without exception. So if we assume this, then one possible exception in Theorem 5 can be eliminated.

Table. The D's of R-D type$\leq e^{16}$ which satisfy the necessary conditions of each theorem

$D=m^2+4$			$D=m^2+1$			$D=m^2-4$			$D=m^2-1$		
D	m	h_k	D	m	h_k	D	m	h_k	D	m	h_k
85	9	2	10	3	2	165	13	2	15	4	2
365	19	2	26	5	2	221	15	2	35	6	2
533	23	2	65	8	2	285	17	2	143	12	2
629	25	2	122	11	2	357	19	2	—	—	—
965	31	2	362	19	2	957	31	2	—	—	—
1685	41	2	485	22	2	1085	33	2	—	—	—
1853	43	2	1157	34	2	1517	39	2	—	—	—
2813	53	2	2117	46	2	2397	49	2	—	—	—
49733	223	6	3365	58	2	35717	189	6	—	—	—
—	—	—	24965	158	6	53357	231	6	—	—	—
—	—	—	27557	166	6	—	—	—	—	—	—
—	—	—	37637	194	6	—	—	—	—	—	—
—	—	—	64517	254	6	—	—	—	—	—	—
—	—	—	264197	514	10	—	—	—	—	—	—
—	—	—	343397	586	10	—	—	—	—	—	—

Acknowledgement. The authors would like to thank M. Kida for his generous assistance.

References

[1] H. K. Kim: A conjecture of S. Chowla and related topics in analytic number theory. Ph. D. thesis, Johns Hopkins University (1988).
[2] H. K. Kim, M.-G. Leu and T. Ono: On two conjectures on real quadratic fields. Proc. Japan Acad., **63A**, 222–224 (1987).
[3] M.-G. Leu: On a determination of certain real quadratic fields of class number two. J. Number Theory, **33**, 101–106 (1989).
[4] R.-A. Mollin and H. C. Williams: Prime producing quadratic polynomials and real quadratic fields of class number one. Number Theory (eds. J.-M. De Koninck and C. Levesque). Walter de Gruyter, Berlin, New York, pp. 654–663 (1988).
[5] L. Rédei and H. Reichardt: Die Anzahl der durch 4 teilbaren Invariant der Klassengruppe eines beliebigen quadratischen Zahlkörpers. J. Reine Angew. Math., **170**, 69–74 (1933).
[6] T. Tatuzawa: On a theorem of Siegel. Japanese J. Math., **21**, 163–178 (1951).
[7] Y. Yamamoto: Divisibility by 16 of class number of quadratic fields whose 2-class groups are cyclic. Osaka J. Math., **21**, 1–22 (1984).
[8] H. Yokoi: Some relations among new invariants of prime number p congruent to 1 mod 4. Advanced Studies in Pure Math., **13**, 493–501 (1988).