On a Determination of Certain Real Quadratic Fields of Class Number Two

MING-GUANG LEU

Department of Mathematics, Johns Hopkins University.
Baltimore, Maryland 21218

Communicated by Hans Zassenhuss
Received September 13, 1988

We use the Siegel-Tatuzawa theorem to determine real quadratic fields \( \mathbb{Q}(\sqrt{m^2 + 4}) \) and \( \mathbb{Q}(\sqrt{m^2 + 1}) \) which have class number two.

Let \( D \) be a square-free rational integer of the form \( D = m^2 + 4 \) or \( m^2 + 1 \) \((m \in \mathbb{N})\). By the results in [5] and [7], we can almost say that there are exactly 11 real quadratic fields \( \mathbb{Q}(\sqrt{D}) \) of class number one: \( D = 5, 13, 17, 29, 37, 53, 101, 173, 197, 293, 677 \). In this paper, we shall prove, without assuming the generalized Riemann Hypothesis, that at most 17 real quadratic fields \( \mathbb{Q}(\sqrt{D}) \) are of class number two. We shall also prove that if we assume the generalized Riemann Hypothesis there are exactly 16 real quadratic fields \( \mathbb{Q}(\sqrt{D}) \) of class number two: \( D = 10, 26, 65, 85, 122, 362, 365, 485, 533, 629, 965, 1157, 1685, 1853, 2117, 2813 \).

In the sequel, let \( k = \mathbb{Q}(\sqrt{D}) \) be a quadratic field where \( D = m^2 + 4 \) or \( m^2 + 1 \) \((m \in \mathbb{N})\), a square-free rational integer. We shall denote by \( h_k \) and \( \chi_k \) the class number and the Kronecker character of \( k \), respectively.

First we prove the following proposition:

**Proposition 1.** If \( h_k = 2 \), then \( D = m^2 + 4 = pq \) (resp. \( D = m^2 + 1 = pq \)), where \( p < q \) are both prime.

To prove this proposition, we need the following well-known lemma (see, e.g., H. Cohn [2, pp. 187], for proof):

**Lemma 1.** If the discriminant of a quadratic field contains only one prime factor, then the class number of the field is odd.

1 By the genus theory of quadratic number fields, the class number of \( \mathbb{Q}(\sqrt{D}) \) is even, where \( D = m^2 + 1 \) is square-free and \( m \) is odd (cf. the proof of Proposition 1).
Proof of Proposition 1. Since the fundamental unit of $k$ is $u = (m + \sqrt{D})/2$ (resp. $u = m + \sqrt{D}$), the norm $N(u) = -1$. Therefore, by the genus theory of quadratic number fields, we have $2 = h_k = h_k^+ = 2^{t-1}h^*$, where $h_k^+$ is the class number of $k$ in the narrow sense, $h^*$ is the number of classes in a genus, and $t$ is the number of distinct prime factors of $D$. Our assertion follows from Lemma 1. Q.E.D.

From now on, we only have to consider the case $D = m^2 + 4 = pq$ (resp. $D = m^2 + 1 = pq$), the product of two different primes $p, q, p < q$. We need the following lemmas, propositions, and theorems to derive some properties of $k$, which has class number two. Similarly, we only give the details of the case $D = m^2 + 4 = pq$.

Lemma 2 (S.-D. Lang [6]). Let $m, n$ be positive integers. Assume that $m > 2$ and $n$ is not a square. Then the equation

$$x^2 - (m^2 + 4)y^2 = fn$$

has no solution in integers $x, y$, unless $n > m$.

Lemma 3. For $k = \mathbb{Q}(\sqrt{D}), D = m^2 + 4 = pq$, if there exists a prime $r$ such that $\chi_k(r) = 1$ and $r^2 < m$, then $h_k > 2$.

Proof. By the assumption $\chi_k(r) = 1$ the ideal $(r)$ splits as the product of prime ideals; $(r) = pp'$, where $p'$ is the conjugate of $p$, $p' \neq p$, and $p \mid (r)$. Also, $r = N(p) = N(p') < m$ and by Lemma 2, we see that $p$ and $p'$ are not principal ideals.

For our quadratic field $k$, we have $h_k \geq 2$. We claim that $h_k > 2$. So suppose that $h_k = 2$. Then

$$p^2 \sim (1),$$

i.e., $p^2 = (x + y\sqrt{D})/2$ for some integers $x, y$. Since

$$r^2 = N(p^2) = \left|N\left(\frac{x + y\sqrt{D}}{2}\right)\right| = \left|\frac{x^2 - Dy^2}{4}\right|,$$

we have

$$x^2 - Dy^2 = x^2 - (m^2 + 4)y^2 = \pm 4r^2.$$ 

This implies $y \neq 0$; otherwise we have $p^2 = (r) = pp'$, i.e., $p = p'$, a contradiction.

Now, we claim that there is no integral solution $x, y (y \neq 0)$ such that $p^2 = (x + y\sqrt{D})/2$. Suppose that there is an integral solution $x, y (y \neq 0)$
such that $p^2 = (x + y \sqrt{D})/2$. Among all solutions $x, y$ ($y > 0$), choose $x_0, y_0$ with the smallest $y_0$; thus $p^2 = (x_0 + y_0 \sqrt{D})/2$. Since $(m - \sqrt{D})/2$ is a unit we can also write

$$p^2 = \left(\frac{x_0 + y_0 \sqrt{D}}{2}\right)\left(\frac{m - \sqrt{D}}{2}\right) = \left(\frac{(mx_0 - Dy_0)}{2} + \frac{(my_0 - x_0) \sqrt{D}}{2}\right).$$

so we have

$$\pm 4r^2 = \left(\frac{mx_0 - (m^2 + 4)y_0}{2}\right)^2 - (m^2 + 4) \left(\frac{x_0 - my_0}{2}\right)^2.$$

Since integer $(x_0 - my_0)/2 \neq 0$ as above, we have

$$\left|\frac{x_0 - my_0}{2}\right| \geq y_0.$$

Hence either $x_0 - my_0 \geq 2y_0$ or $x_0 - my_0 \leq -2y_0$. So either

$$+ 4r^2 = x_0^2 - (m^2 + 4)y_0^2 \geq (m^2 + 4)y_0^2 - (m^2 + 4)y_0^2 = 4my_0^2 \geq 4m$$

or

$$\pm 4r^2 = x_0^2 - (m^2 + 4)y_0^2 \leq (m^2 + 4)y_0^2 - (m^2 + 4)y_0^2 = -4my_0^2 \leq -4m.$$

Clearly, in each case $r^2 \geq m$, a contradiction. This implies that $h_k > 2$.

Q.E.D.

As a corollary of Lemma 3, we have the following lemma:

**Lemma 4.** For $k = \mathbb{Q}(\sqrt{D})$, $D = m^2 + 4 = pq$, if $h_k = 2$, then $m = t^s$, where $t$ is a prime and $s = 1$ or 2.

**Proof.** Let $t$ be the smallest prime factor of $m$. If $t^2 < m$ then we must have

$$-1 = \chi_k(t) = \left(\frac{D}{t}\right) = \left(\frac{m^2 + 4}{t}\right) = \left(\frac{4}{t}\right) = 1,$$

a contradiction, where $(D/t)$ denotes the Jacobi symbol.

Q.E.D.
From Lemmas 2, 3, and 4, we obtain immediately the following theorem:

**THEOREM 1.** For \( k = \mathbb{Q}(\sqrt{D}) \), \( D = m^2 + 4 = pq \), and \( h_k = 2 \), we have

1. \( D = pq = t^{2s} + 4 \), where \( t \) is a prime and \( s = 1 \) or \( 2 \),
2. if a prime \( r \) is such that \( \chi_k(r) = 1 \), then \( r^2 \geq m \) and \( pr \geq m \).

By applying the Siegel–Tatuzawa theorem [3], we obtain an upper bound for \( D = m^2 + 4 \):

**PROPOSITION 2.** If \( h_k = 2 \), then \( D < 18,900,000 \) with one possible exception of \( D \).

*Proof.* By Dirichlet's class number formula, we have

\[
h_k = \frac{\sqrt{D}}{2 \log u} L(1, \chi_k),
\]

where \( \chi_k \) is the Kronecker character belonging to the quadratic field \( k \) and \( u = (m + \sqrt{D})/2 \) is the fundamental unit of \( k \).

Assume that \( D \geq 18,900,000 \). By Theorem 1 of [3], we have

\[
h_k = \frac{\sqrt{D}}{2 \log u} L(1, \chi_k) > \frac{\sqrt{D}}{2 \log \sqrt{D}} \frac{1}{7.735 \log D} = \frac{\sqrt{D}}{7.735(\log D)^2},
\]

with one possible exception of \( D \). Since \( f(x) = \sqrt{x}/7.735(\log x)^2 \) is increasing on \([18,900,000, \infty)\), we have

\[
h_k > \frac{\sqrt{D}}{7.735(\log D)^2} = 2.002 \cdots > 2,
\]

Q.E.D.

By the help of a computer, we find that there are exactly 12 positive integers smaller than 18,900,000 which satisfy the necessary conditions (1) and (2) of Theorem 1: \( D = 85, 365, 533, 629, 965, 1,685, 1,853, 2,813, 6,893, 12,773, 24,653, 49,733 \). Then, by checking a table of class numbers of quadratic fields [9], we have the following theorem:

**THEOREM 2.** If \( h_k = 2 \) and \( D \leq 18,900,000 \), then \( D = 85, 365, 533, 629, 965, 1,685, 1,853, 2,813 \).

For the case \( D = m^2 + 1 = pq \), we have similar results.

* Put \( d = D \) and \( \varepsilon = 0.07 \) in Theorem 1 of [3].
Lemma 2' (Ankeny, Chowla, Hasse [1]). Let \( m, n \) be positive integers and \( n \) not a square. Then the equation

\[
x^2 - (m^2 + 1) y^2 = \pm n
\]

has no solution in integers \( x, y \), unless \( n \geq 2m \).

Lemma 3'. For \( k = \mathbb{Q}(\sqrt{D}) \), \( D = m^2 + 1 = pq \) an odd integer (resp. an even integer), if there exists a prime \( r \) such that \( \chi_k(r) = 1 \) and \( 4r^2 < 2m \) (resp. \( r^2 < 2m \)), then \( h_k > 2 \).

As a corollary of Lemma 3', we have the following lemma:

Lemma 4'. For \( k = \mathbb{Q}(\sqrt{D}) \), \( D = m^2 + 1 = pq \), and \( h_k = 2 \),

1. if \( D \) is odd, then \( m = 2t^2 \), where \( t \) is a prime and \( s = 1 \) or \( 2 \);
2. if \( D \) is even, then \( m = t \), where \( t \) is a prime.

Similarly, from Lemmas 2', 3', and 4', we have the following theorem:

Theorem 1'. For \( k = \mathbb{Q}(\sqrt{D}) \), \( D = m^2 + 1 = pq \) an odd integer (resp. an even integer), and \( h_k = 2 \), we have that

1. \( D = pq = 4t^{2s} + 1 \) (resp. \( D = 2q = t^2 + 1 \)), where \( t \) is a prime and \( s = 1 \) or \( 2 \);
2. if there exists a prime \( r \) such that \( \chi_k(r) = 1 \), then \( 4r^2 \geq 2m \) (resp. \( r^2 \geq 2m \)) and \( 4pr \geq 2m \) (resp. \( 2r \geq 2m \)).

Also, by applying the Siegel-Tatuzawa theorem [3], we obtain an upper bound for \( D = m^2 + 1 \):

Proposition 2'. If \( h_k = 2 \), then \( D \leq 25,000,000 \) with one possible exception of \( D \).

As above, by the help of a computer, we have the following theorem:

Theorem 2'. If \( h_k = 2 \) and \( D \leq 25,000,000 \), then \( D = 10, 26, 65, 122, 362, 485, 1157, 2117 \).

Remark. Assuming the generalized Riemann Hypothesis, Kim [4] proves that the Tatuzawa theorem [8] is true without any exception. So, if we assume this, then \( D = m^2 + 4 \) or \( m^2 + 1 \) and \( h_k = 2 \) implies that \( D = 10, 26, 65, 85, 122, 362, 365, 485, 533, 629, 965, 1157, 1685, 2117, 2813 \).
REFERENCES

7. R. A. MOLLIN AND H. C. WILLIAMS, Prime producing quadratic polynomials and real quadratic fields of class number one, "Proceedings International Conference on Number, Quebec, July, 1987."
9. H. WADA, "A Table of Ideal Class Number of Real Quadratic Fields," Kōkyuroku in Mathematics, No. 10, Sophia University, Tokyo, 1981.