91. On a Conjecture of Ono on Real Quadratic Fields

By Ming-Guang LEU
Department of Mathematics, The Johns Hopkins University

(Communicated by Shokichi IYANAGA, M. J. A., Oct. 12, 1987)

Let k be a quadratic field. We shall denote by Δ_k, M_k, h_k and χ_k, the discriminant, the Minkowski constant, the class number and the Kronecker character, respectively. Consider the following set

$$S_k=\{p, \text{ rational prime}\,;\ p\leqq M_k,\ \chi_k(p)\neq -1\}.$$

It is easy to see that the ideal class group H_k of k is generated by the classes of prime ideals $\mathfrak{p}$, $\mathfrak{p}\,|\,p$, $p\in S_k$. In particular, we have

(1) $$S_k=\phi \implies h_k=1.$$

If k is *imaginary*, it is easy to prove the stronger relation:

(2) $$S_k=\phi \iff h_k=1.$$ [1]

However, if k is *real*, (2) is not always true; e.g. $h_k=1$ but $S_k=\{2\}$ for $k=\boldsymbol{Q}(\sqrt{6})$. In view of the celebrated conjecture of Gauss on the class number of real quadratic fields, it is interesting to determine all k's such that $S_k=\phi$. Recently Prof. Ono conjectured that these must be exactly the following 11 fields $k=\boldsymbol{Q}(\sqrt{m})$ with $m=2, 3, 5, 13, 21, 29, 53, 77, 173, 293$ and 437.

In this paper, we shall prove the following:

Theorem. *There are at most* 12 *real quadratic fields k such that $S_k=\phi$.*

In the sequel, m will denote a square-free natural number $\geqq 5$ and $h(m)$ the class number h_k with $k=\boldsymbol{Q}(\sqrt{m})$.[2] We remind the reader that $M_k=\sqrt{\Delta_k}/2$ and that

$$\chi_k(p)=\begin{cases}\left(\dfrac{\Delta_k}{p}\right) & \text{if } p\neq 2,\ p\nmid \Delta_k,\\ (-1)^{(\Delta_k^2-1)/8} & \text{if } p=2,\ 2\nmid \Delta_k,\\ 0 & \text{if } p\,|\,\Delta_k.\end{cases}$$

Since $\chi_k(2)=0$ for $m\equiv 2, 3 \pmod 4$ and $\chi_k(2)=1$ for $m\equiv 1 \pmod 8$, S_k contains 2, i.e. $S_k\neq\phi$. *So from now on we can assume that* $m\equiv 5 \pmod 8$. Under this assumption, we shall try to determine k for which $S_k=\phi$.

The theorem obviously follows from the following two Propositions (A), (B).

Proposition (A). *There exists at most one $m\geqq e^{16}$ with $S_k=\phi$.*

Proposition (B). *If $S_k=\phi$ and $m<e^{16}$, then* $m=2, 3, 5, 13, 21, 29, 53, 77, 173, 293, 437$.

---

1) The relation (2) is independent of deep results such as [1], [3].

2) Clearly, $S_k=\phi$ for $m=2$ or 3.

The proof of Proposition (B) is obtained by the table 1 of [2] and the following table.

Table ($m=p_1p_2$, p_1, p_2: prime)

m	r_0	m	r_0	m	r_0
21	—	416021	5	3186221	5
77	—	549077	7	3493157	19
437	—	680621	5	4003997	7
2021	5	741317	11	4347221	5
4757	7	783221	5	4862021	5
6557	11	826277	7	5022077	7
11021	5	938957	17	5517797	13
16637	11	1185917	29	6456677	17
27221	5	1640957	17	7080917	7
50621	5	1703021	5	7209221	5
95477	7	2030621	5	7338677	11
145157	11	2099597	11	$9126437>e^{16}$	
194477	13	2205221	5		
216221	5	2461757	7		
239117	7	2499557	7		
250997	17	2772221	5		

In the column r_0 of the table, the smallest odd prime $r_0 \leqq M_k$ such that $\chi_k(r_0) \neq -1$ is given.

The proof of Proposition (A) follows from the following three lemmas together with Tatuzawa's lower bound for $L(1, \chi_k)$ ([4]).

Lemma 1. *If $S_k=\phi$, then either $m=p$ or $m=p_1p_2$, where p, p_1, p_2 are primes.*

Proof. Suppose $m=p_1p_2p_3\cdots p_n$, $n\geqq 3$, where p_i is prime for $i=1, 2, \cdots, n$. Without loss of generality, let $p_1=\min\{p_1, p_2, \cdots, p_n\}$. Then we have $p_1^2<p_1p_2p_3\cdots p_n/4$ which implies that $p_1 \leqq M_k$. Since $\chi_k(p_1)=0$, so $p_1 \in S_k$ and we have $S_k \neq \phi$, Q.E.D.

Lemma 2. *If $m=a^2+b^2$ with positive integers a, b, and $S_k=\phi$, then $m=q^2+4$ where q is prime or 1.*[3)]

Proof. For $m=5$, since $M_k<2$, we have $S_k=\phi$ and $q=1$. Assume that $m>5$.

Case 1. If $b=1$, then a is even and $m>a^2=4(a/2)^2$. Since $1<a/2<\sqrt{m}/2=M_k$ and $a/2$ is odd as $m\equiv 5 \pmod 8$, there exists a prime $r\leqq M_k$ such that $r|a/2$. This implies that $\chi_k(r)=(m/r)=(\Delta_k/r)=1$, i.e. $r \in S_k$.

Case 2. If $b\neq 1$, we may assume that a is even and b is odd. Then, we have $a/2<M_k$.

(I) If $a/2\neq 2^s$, $s\geqq 0$, then there exists a prime r such that $r|a/2$, which implies, as above, that $r \in S_k$.

(II) If $a/2\neq 2^s$, $s\geqq 0$, then we consider two cases separately. (a) If

3) Lemma 2 can be applied to the case $m=p$ because $p\equiv 1 \pmod 4$.

b is not a prime number, then there exists a prime r such that $b=rt$, $t\geqq 3$. We have $r<M_k$, which implies again that $r\in S_k$. (b) If $b=q$ is prime, then

$$m=\begin{cases}2^2+q^2\\ (2^s)^2+q^2, \quad \text{with} \quad s>1.\end{cases}$$

Since $m\equiv 5 \pmod 8$, we must have $m=2^2+q^2$, Q.E.D.

Lemma 3. *If $m=p_1p_2$ and $S_k=\phi$, then $p_1-p_2=\pm 4$ and $p_i\equiv 3 \pmod 4)$, $i=1, 2$.*

Proof. If $p_i\equiv 1 \pmod 4$ for $i=1, 2$, then $m=p_1p_2=a^2+b^2$, where a and b are both positive integers. By Lemma 2, we have $m=4+q^2$, where q is prime. By Theorem 1 of [5], m is prime. This contradicts our assumption on m. Now, without loss of generality, we may assume that $p_2>p_1$. Suppose that $p_2-p_1>4$. We divide our argument into two cases.

Case 1. $p_1=8n+3$, $p_2=8(n+s)+7$, where $n\geqq 0$ and $s\geqq 1$ are integers. Then we have

$$\begin{aligned}m=p_1p_2&=(8n+3)(8(n+s)+7)\\ &=(8n+3)(8n+3+8s+4)=(8n+3)^2+4(8n+3)(2s+1).\end{aligned}$$

Since $m/4>(8n+3)(2s+1)$, we have $S_k\neq\phi$, because for the smallest prime factor r of either $(8n+3)$ or $(2s+1)$, we have $r\leqq M_k$ and $\chi_k(r)=1$.

Case 2. $p_1=8n+7$, $p_2=8(n+s)+3$, where $n\geqq 0$ and $s\geqq 2$ are integers. By a similar argument as in Case 1, we have $S_k\neq\phi$, Q.E.D.

Proof of Proposition (A). For the case where $m=p$ is prime, by Lemma 2, by (1) and by Theorem 1 of [2], there exists at most one $m\geqq e^{16}$ with $S_k=\phi$. A similar argument as in Theorem 1 of [2] works for $m=p_1p_2$, where p_1 and p_2 are primes of the form $4n+3$, $n\geqq 0$, an integer and $p_1-p_2=\pm 4$ (cf. Lemma 3). To be more precise, in this case, the fundamental unit u of $\boldsymbol{Q}(\sqrt{m})$ is $u=(p_1+2+\sqrt{m})/2$, where we assumed that $p_1<p_2$.[4] By the Dirichlet formula, we have

$$h(m)=\frac{\sqrt{m}}{2\log u}L(1,\chi_k).$$

Assume that $m\geqq e^{16}$. By Theorem 2 of [4], we have

$$L(1,\chi_k)>(0.655)m^{-1/16}/16$$

with one possible exception of m.[5]

It is clear that $u<2\sqrt{m}$. Then we have

$$\begin{aligned}h(m)=\frac{\sqrt{m}}{2\log u}L(1,\chi_k)&>\frac{\sqrt{m}}{2\log 2\sqrt{m}}\frac{1}{16}(0.655)m^{-1/16}\\ &=\frac{1}{16}(0.655)\frac{m^{7/16}}{\log 4m}.\end{aligned}$$

Since $f(x)=(x^{7/16}/\log 4x)$ is increasing on $[e^{16},\infty)$, we have

$$\begin{aligned}h(m)&>\frac{1}{16}(0.655)\frac{(e^{16})^{7/16}}{\log 4e^{16}}=\frac{1}{16}(0.655)\frac{e^7}{\log 4+16}>\frac{1}{16}(0.655)\frac{e^7}{20}\\ &=2.244\cdots>2,\end{aligned}$$

which completes the proof of Proposition (A).

---

4) The verification of $uu'=1$ by using $p_2-p_1=4$ is amusing.

5) Put $k=m$ and $\varepsilon=1/16$ in Theorem 2 of [4].

References

[1] H. Heilbronn and E. H. Linfoot: On the imaginary quadratic corpora of class-number one. Quart. J. Math., V. 5, pp. 293–301 (1934).

[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] H. M. Stark: A complete determination of the complex quadratic fields of class-number one. Michigan Math. J., **14**, 1–27 (1967).

[4] T. Tatuzawa: On a theorem of Siegel. Japan. J. Math., **21**, 163–178 (1951).

[5] H. Yokoi: Class-number one problem for certain kind of real quadratic fields. Proc. International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields, June 24–28, 1986, Katata, Japan, pp. 125–137.