# 6. On Ono's Problem for Quadratic Fields

By Masaki KOBAYASHI

Department of Mathematics School of Science, Nagoya University

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1993)

For a quadratic number field $k$, we shall denote by $d_k$, $h_k$ and $\chi_k$, the discriminant, the class number and the Kronecker character of $k$, respectively. Let $M_k$ be the Minkowski constant of $k$:

$$M_k = \begin{cases} \dfrac{1}{2}\sqrt{d_k} & \text{if } k \text{ is real,} \\ \dfrac{2}{\pi}\sqrt{-d_k} & \text{if } k \text{ is imaginary.} \end{cases}$$

For the following finite sets of rational prime numbers:

$$S(k) = \{p, \text{ rational prime}; p \leq M_k\},$$
$$S_1(k) = \{p \in S(k)\ ;\ \chi_k(p) = -1\},$$
$$S_2(k) = \{p \in S(k)\ ;\ \chi_k(p) = 0\},$$
$$S_3(k) = \{p \in S(k)\ ;\ \chi_k(p) = 1\},$$

we shall define the following three families of quadratic fields by

$$K_i = \{k, \text{ quadratic field}; S(k) = S_i(k)\}\ (i = 1,2,3).$$

It follows from Minkowski's theorem that the ideal class group of $k$ is generated by the classes of prime ideals $\mathfrak{p}$ lying on $p$ in $S(k)$. Therefore if $S(k) = S_1(k)$ holds, then $h_k = 1$. When $k$ is imaginary, it is easy to prove that $h_k = 1$ holds if and only if $S(k) = S_1(k)$. In the relation with conjecture of Gauss on the class number of real quadratic fields, it is interesting to determine $K_1$. Leu and Ono determined $K_2$ and $K_3$ in [2], [5] as follows:

$$K_2 = \{Q(\sqrt{m})\ ;\ m = -1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 7, 13, 15, \pm 30\},$$
$$K_3 = \{Q(\sqrt{m})\ ;\ m = -1, \pm 2, \pm 3, 5, -7, 13, -15, 17, -23, 33, -47, -71, 73, 97, -119\}.$$

Moreover Leu determined $K_1$, with one possible exception in [1]:

$$K_1 = \{Q(\sqrt{m})\ ;\ m = -1, \pm 2, \pm 3, 5, -7, -11, 13, -19, 21, 29, -43, 53, -67, 77, -163, 173, 293, 437\}.$$

**Remark 1.** Under the assumption of GRH (the generalized Riemann Hypothesis), we can determine $K_1$ without any exception.

Consider the finite set of prime numbers such as

$$S_0(k) = \{p \in S(k),\ \chi_k(p) \neq 1\}.$$

If $h_k$ is odd and $S(k) = S_0(k)$, then $h_k = 1$ holds. The condition that $h_k$ is odd and $S(k) = S_0(k)$ is weaker than $S(k) = S_1(k)$. Our purpose is to determine the family $K$ of all fields $k$ satisfying that $h_k$ is odd and $S(k) = S_0(k)$ under the assumption of GRH.

**Theorem 1.** *If GRH holds, then there are exactly* 42 *belonging to* $K$:

$$K = \{Q(\sqrt{m})\ ;\ m = -1, \pm 2, \pm 3, 5, 6, \pm 7, \pm 11, 13, 14, -19, 21, 23, 29, 38, -43, 47, 53, 62, -67, 69, 77, 83, 93, -163,$$

167, 173, 213, 227, 237, 293, 398, 413, 437, 453, 717, 1077, 1133, 1253}.

For real $k = Q(\sqrt{m})$ belonging to $K$, by the genus theory, there are three different cases as follows:

$$m = \begin{cases} p_1, \\ 2p_1 & ; p_1 \equiv 3(\mathrm{mod}4), \\ p_1p_2 & ; p_1 \equiv p_2 \equiv 3(\mathrm{mod}4), \end{cases}$$

where $p_1$ and $p_2$ are primes and $p_1 < p_2$. Consider the following four families of fields:

$$A = \{\text{imaginary quadratic fields}\} \cap K,$$
$$B = \{Q(\sqrt{p_1})\} \cap K,$$
$$C = \{Q(\sqrt{2p_1})\ ;\ p_1 \equiv 3(\mathrm{mod}4)\} \cap K,$$
$$D = \{Q(\sqrt{p_1p_2})\ ;\ p_1 \equiv p_2 \equiv 3(\mathrm{mod}4)\} \cap K.$$

Then $K$ is classified into four disjoint classes: $A$, $B$, $C$ and $D$. When $k$ is imaginary, $k$ belongs to $A$ if and only if $h_k = 1$ holds. Therefore $A = \{Q(\sqrt{m})\ ; m = -1, -2, -3, -7, -11, -19, -43, -67, -163\}$. So it is sufficient to prove the following Theorems 2-4.

**Theorem 2.** *If GRH holds, there are exactly* 15 *fields belonging to* $B$:

$B = \{Q(\sqrt{m})\ ;\ m = 2, 3, 5, 7, 11, 13, 23, 29, 47, 53, 83, 167, 173, 227, 293\}$.

**Theorem 3.** *If GRH holds, then there are exactly* 5 *fields belonging to* $C$:

$C = \{Q(\sqrt{m})\ ;\ m = 6, 14, 38, 62, 398\}$.

**Theorem 4.** *If GRH holds, then there are exactly* 13 *fields belonging to* $D$:

$D = \{Q(\sqrt{m})\ ;\ m = 21, 69, 77, 93, 213, 237, 413, 437, 453, 717, 1077, 1133, 1253\}$.

In order to prove Theorems 2-4, we need the following two theorems.

**Theorem 5** (Mollin and Williams [3]). *If GRH holds, the squarefree positive integers* $m \equiv 2 \pmod 4$ *satisfying* $(m/p) = -1$ *for all odd primes* $p < \sqrt{m}/2$ *are* 6, 10, 14, 26, 38, 62, 122, 362, 398, *where* (/) *is the Legendre symbol.*

**Theorem 6** (Mollin and Williams [3]). *If GRH holds, the squarefree positive integers* $m \equiv 3 \pmod 4$ *which satisfy* $m \neq 2q^2 + 1$ *for any prime* $q$ *and* $(m/p) = -1$ *for all odd primes* $p < \sqrt{m-2}$ *are* 3, 7, 11, 15, 23, 35, 47, 83, 143, 167, 227.

*Proof of Theorem* 2. It is clear that the quadratic field $k = Q(\sqrt{2})$ satisfies the condition $S(k) = S_0(k)$. Consider the following families of fields:

$$B_1 = \{Q(\sqrt{p_1})\ ;\ p_1 \equiv 1(\mathrm{mod}\ 4)\} \cap K,$$
$$B_2 = \{Q(\sqrt{p_1})\ ;\ p_1 \equiv 3(\mathrm{mod}\ 4)\} \cap K.$$

Then $B$ is classified into three disjoint classes as follows:

$$B = \{Q(\sqrt{2})\} \cup B_1 \cup B_2.$$

Next, suppose that $k = Q(\sqrt{p_1})$ belongs to $B_2$. If there is a prime number $q$ satisfying $p_1 = 2q^2 + 1$, then $M_k = \sqrt{2q^2+1} > q$ and $(p_1/q) = 1$. From Theorem 6, it is necessary that $p_1$ belongs to {3, 7, 11, 15, 23, 35, 47, 83, 143, 167, 227}. So we see easily

$$B_2 = \{Q(\sqrt{m})\ ;\ m = 3, 7, 11, 23, 47, 83, 167, 227\}.$$

Therefore

$$B = \{Q(\sqrt{m})\ ;\ m = 2, 3, 5, 7, 11, 13, 23, 29, 47, 53, 83, 167, 173, 227, 293\}.$$

*Proof of Theorem* 3. Suppose that $k = Q(\sqrt{2p_1})$ belongs to $C$. Then, since $M_k = \sqrt{2p_1}$, the prime number $p$ such that $p < M_k$ and $\chi_k(p) = 0$ is 2 only. From Theorem 5, it is necessary that $2p_1$ belongs to $\{6, 10, 14, 26, 38, 62, 122, 362, 398\}$. So we see easily

$$C = \{Q(\sqrt{m})\ ;\ m = 6, 14, 38, 62, 398\}.$$

*Proof of Theorem* 4. Suppose that $k = Q(\sqrt{p_1p_2})$ belongs to $D$ and set $A(x) = \sum (p_1p_2/q)$, where the sum is taken over all primes $q \leq x$.

Let $\pi(x)$ be the number of primes $\leq x$. For all primes $\leq x$, we denote by $\pi_1(x)$ and $\pi_2(x)$ the number of primes $q$ such that $(p_1p_2/q) = 1$ and $(p_1p_2/q) = -1$, respectively. Then $A(x) = \pi_1(x) - \pi_2(x)$. By Oesterlé [4], if GRH holds, for $i = 1,2$,

$$\left| \pi_i(x) - \frac{1}{2}\int_2^x \frac{dt}{\log t} \right| \leq B(x),$$

where

$$B(x) = \frac{1}{2}\sqrt{x}\left\{\left(\frac{1}{\pi} + \frac{5.3}{\log x}\right)\log(p_1p_2) + 2\left(\frac{\log x}{2\pi} + 2\right)\right\}.$$

Therefore

$$|A(x)| \leq 2B(x).$$

On the other hand, since $k$ belongs to $D$, for $x \leq \frac{\sqrt{p_1p_2}}{2}$

$$|A(x)| \geq \pi(x) - 1$$

holds. By Roser-Schoenfeld [6], $x \geq 17$ implies $\frac{x}{\log x} \leq \pi(x)$. Put $t = \frac{1}{2}\sqrt{p_1p_2}$, then

$$B(t) = \frac{1}{2}\sqrt{t}\left\{\left(\frac{1}{\pi} + \frac{5.3}{\log t}\right)\log(4t^2) + 2\left(\frac{\log t}{2\pi} + 2\right)\right\}.$$

Assume $t \geq e^{12}$, then

$$|A(t)| > \frac{t}{\log t} - 1.$$

On the other hand, we have

$$\begin{aligned}
|A(t)| &\leq 2B(t) \\
&= \frac{3}{\pi}\sqrt{t}\log t + \left(\frac{2\log 2}{\pi} + 14.6\right)\sqrt{t} + \frac{10.6\sqrt{t}\log 2}{\log t} \\
&< \sqrt{t}\log t + 15.3\sqrt{t} + \frac{10.6\sqrt{t}}{\log t} \\
&< \left(1 + \frac{15.3}{12} + \frac{10.6}{12^2}\right)\sqrt{t}\log t \\
&< 2.35\sqrt{t}\log t \\
&< \frac{t}{\log t} - 1 \\
&\leq |A(t)|,
\end{aligned}$$

Table I

| $p$ | $n$ | $p$ | $n$ | $p$ | $n$ |
|---|---|---|---|---|---|
| 3 | 5 | 43 | 140213 | 101 | 261153653 |
| 5 | 5 | 47 | 156525 | 103 | 261153653 |
| 7 | 5 | 53 | 550205 | 107 | 416748717 |
| 11 | 77 | 59 | 550205 | 109 | 416748717 |
| 13 | 117 | 61 | 994565 | 113 | 416748717 |
| 17 | 605 | 67 | 1144293 | 127 | 1586592293 |
| 19 | 717 | 71 | 1878245 | 131 | 1586592293 |
| 23 | 1965 | 73 | 1878245 | 137 | 5702566397 |
| 29 | 10925 | 79 | 9903005 | 139 | 5702566397 |
| 31 | 10925 | 83 | 27005517 | 149 | 15933687413 |
| 37 | 26253 | 89 | 27082557 | 151 | 25777678685 |
| 41 | 26253 | 97 | 27082557 | 157 | 181315486677 |

Table II

| $m$ | $r$ | $m$ | $r$ | $m$ | $r$ | $m$ | $r$ | $m$ | $r$ |
|---|---|---|---|---|---|---|---|---|---|
| 21 | 5 | 597 | 7 | 1349 | 5 | 2021 | 5 | 2757 | 13 |
| 69 | 5 | 669 | 5 | 1357 | 3 | 2077 | 3 | 2773 | 3 |
| 77 | 13 | 717 | 23 | 1389 | 5 | 2101 | 3 | 2869 | 3 |
| 93 | 7 | 749 | 5 | 1397 | 7 | 2149 | 3 | 2893 | 3 |
| 133 | 3 | 781 | 3 | 1437 | 7 | 2157 | 7 | 2901 | 5 |
| 141 | 5 | 789 | 5 | 1461 | 5 | 2181 | 5 | 2933 | 17 |
| 213 | 11 | 813 | 7 | 1477 | 3 | 2189 | 5 | 2949 | 5 |
| 237 | 13 | 869 | 5 | 1501 | 3 | 2229 | 5 | 2973 | 11 |
| 253 | 3 | 893 | 7 | 1509 | 5 | 2253 | 11 | 2981 | 5 |
| 301 | 3 | 917 | 11 | 1541 | 5 | 2317 | 3 | 3013 | 3 |
| 309 | 5 | 933 | 7 | 1589 | 5 | 2413 | 3 | 3053 | 7 |
| 341 | 5 | 973 | 3 | 1661 | 5 | 2429 | 5 | 3093 | 13 |
| 381 | 5 | 989 | 5 | 1757 | 19 | 2453 | 13 | 3101 | 5 |
| 413 | 13 | 1077 | 29 | 1797 | 11 | 2461 | 3 | 3117 | 7 |
| 437 | 7 | 1101 | 5 | 1821 | 5 | 2469 | 5 | 3149 | 5 |
| 453 | 37 | 1133 | 23 | 1829 | 5 | 2517 | 7 | 3173 | 7 |
| 469 | 3 | 1141 | 3 | 1837 | 3 | 2573 | 7 | 3189 | 5 |
| 501 | 5 | 1149 | 5 | 1893 | 11 | 2589 | 5 | 3197 | 13 |
| 517 | 3 | 1253 | 29 | 1909 | 3 | 2629 | 3 | 3261 | 5 |
| 573 | 11 | 1293 | 17 | 1941 | 5 | 2653 | 3 | 3269 | 5 |
| 581 | 5 | 1317 | 7 | 1957 | 3 | 2661 | 5 | 3309 | 5 |
| 589 | 3 | 1333 | 3 | 1981 | 3 | 2733 | 11 | 3317 | 17 |

which is a contradiction. Therefore we have $p_1p_2 < 4e^{24}$. If $p_1p_2 \equiv 1 \pmod 8$, then $(p_1p_2/2) = 1$. Therefore we may consider $p_1p_2 \equiv 5 \pmod 8$ only. We owe Tables I, II to J. Muramatsu. In the Table I, $n$ is the minimal positive integer such that $n \equiv 5 \pmod 8$ and $(n/q) \neq 1$ for all primes $q \leq p$. From Table I, we see $p_1p_2 \leq 3364$. In Table II, $r$ is the minimal prime such that $(p_1p_2/r) = 1$ for $p_1p_2 \equiv 5 \pmod 8$. From the table II, we have

$$D = \{Q(\sqrt{m})\,;\, m = 21, 69, 77, 93, 213, 237, 413, 437, 453, 717, 1077, 1133, 1253\}.$$

## References


[1] M. G. Leu: On a conjecture of Ono on real quadratic fields. Proc. Japan Acad., **63**A, 323–326(1987).

[2] ——: On a problem of Ono and quadratic non-residue. Nagoya Math. J., **115**, 185–198 (1989).

[3] R. A. Mollin and H. C. Williams: Quadratic non-residue and prime-producing polynomials. Canada. Math. Bull., **32**, 474–478 (1989).

[4] Oesterlé: Versions effectives du théorèm de Chebotalev sous L'Hypothèse de Riemann Génèralisè. Soc. Math. France Astérisque, **61**, 165–167 (1979).

[5] T. Ono: A problem on quadratic fields. Proc. Japan Acad., **64**A, 78–79 (1988).

[6] J. B. Rosser and L. Schoenfeld: Approxiamate formulas for some functions of prime numbers. Illinois J. Math., **6**, 64–94 (1962).

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

[8] K. Yosidome and Y. Asaeda: On Ono's problem on quadratic fields. Proc. Japan Acad., **67**A, 348–352 (1991).