M.-G. Leu
Nagoya Math. J.
Vol. 115 (1989), 185–198

ON A PROBLEM OF ONO AND QUADRATIC NON-RESIDUES

MING-GUANG LEU

§ 0. Introduction

Let k be a quadratic field, Δ_k the discriminant and M_k the Minkowski constant:

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

Consider the finite set of prime numbers

$$\Pi_k = \{p, \text{ rational prime}; \ p \leq M_k\}.$$

There are exactly 8 fields for which $\Pi_k = \emptyset$. They make up an exceptional family:

$$E_8 = \{k = \boldsymbol{Q}(\sqrt{m}); \ m = -1, \ \pm 2, \ \pm 3, \ 5, \ -7, \ 13\}.$$

For any k, let χ_k denote the Kronecker character. The character splits Π_k into 3 disjoint parts:

$$\begin{aligned} \Pi_k^0 &= \{p \in \Pi_k; \ \chi_k(p) = 0\}, \\ \Pi_k^- &= \{p \in \Pi_k; \ \chi_k(p) = -1\}, \\ \Pi_k^+ &= \{p \in \Pi_k; \ \chi_k(p) = +1\}. \end{aligned}$$

We remind the reader that for a positive prime integer p

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

Consider, next, the 3 families of fields:

Received May 23, 1988.

$$K^0 = \{k;\ \Pi_k = \Pi_k^0\},$$
$$K^- = \{k;\ \Pi_k = \Pi_k^-\},$$
$$K^+ = \{k;\ \Pi_k = \Pi_k^+\}.$$

Ono's problem in [4] is to determine explicitly the 3 families. Since E_8 is common to all 3 families, it is enough to determine $K^0 - E_8$, $K^- - E_8$, $K^+ - E_8$, respectively. In the first case, the equality $K^0 - E_8 = \{k = \boldsymbol{Q}(\sqrt{m});\ m = -5, \pm 6, 7, 15, \pm 30\}$[1] is settled in [4]. In the second case, the equality $K^- - E_8 = \{k = \boldsymbol{Q}(\sqrt{m});\ m = -11, -19, -43, -67, -163, 21, 29, 53, 77, 173, 293, 437\}$ is almost settled by H.M. Stark [6] and M.-G. Leu [3]. (For more details, see [4].)

In this paper, we shall consider the third case and prove that

$$K^+ - E_8 = \{k = \boldsymbol{Q}(\sqrt{m});\ m = -15, -23, -47, -71, -119, 17, 33, 73, 97\}$$

which is the equality (5) in [4] hinted by the machine computations. Since $\chi_k(2) = 0$ for $m \equiv 2, 3 \pmod 4$, $\chi_k(2) = -1$ for $m \equiv 5 \pmod 8$, and $\chi_k(2) = 1$ for $m \equiv 1 \pmod 8$, we have $m \equiv 1 \pmod 8$ for $k = \boldsymbol{Q}(\sqrt{m})$ in $K^+ - E_8$. So the problem to determine $K^+ - E_8$ is reduced to prove that M_k is larger than the least quadratic non-residue modulo $|m|$ for certain numbers m of type $m \equiv 1 \pmod 8$. For $k = \boldsymbol{Q}(\sqrt{m})$, we define the following 3 disjoint classes:

$$C = \{n \in \boldsymbol{Z};\ \chi_k(n) = 0\},$$
$$C_1 = \{n \in \boldsymbol{Z};\ \chi_k(n) = -1\},$$
$$C_2 = \{n \in \boldsymbol{Z};\ \chi_k(n) = +1\}.$$

In the sequel, $\left(\frac{n}{Q}\right)$ will denote the Jacobi symbol, where Q denotes a positive odd integer and n is an integer such that $(n, Q) = 1$. Note that $\chi_k(n) = \left(\frac{n}{|\Delta_k|}\right)$ when $\Delta_k \equiv 1 \pmod 4$ and $(n, \Delta_k) = 1$. Furthermore, m will denote a square-free integer $\equiv 1 \pmod 8$, $[x]$ the integral part of a positive real number x, q the least positive integer belonging to C_1 and p, p_1, p_2 the positive prime numbers.

We shall divide our argument into two parts. In §1 we shall consider the case $m < 0$ and in §2 the case $m > 0$. Before the main argument, we prove the following lemma which enables us to consider

[1] In [4] Ono included erroneously $m=10$ in the set $K^0 - E_8$. This was pointed out by M. Ishibashi.

only the cases where either m is a prime number or a product of two prime numbers.

LEMMA 1. *If* $k = \boldsymbol{Q}(\sqrt{m}) \in K^+ - E_8$, *then*

(1) *for* $m > 0$, *either* $m = p$ *or* $m = p_1p_2$,

and

(2) *for* $m < 0$, *either* $m = -p$ *or* $m = -p_1p_2$.

Proof. Suppose that $m > 0$ and $m = p_1p_2p_3 \cdots p_n$, $n \geq 3$, where p_i is prime for $i = 1, 2, \cdots, n$. Without loss of generality, one can assume that $p_1 = \min\{p_1, p_2, \cdots, p_n\}$. Then we have $p_1^2 < p_1p_2 \cdots p_n/4$ which implies that $p_1 \leq M_k$. Since $\chi_k(p_1) = 0$, we have $\Pi_k \neq \Pi_k^+$ and so $k = \boldsymbol{Q}(\sqrt{m}) \notin K^+ - E_8$ which proves the assertion in the case (1). Similarly one proves the assertion in the case (2), Q.E.D.

§ 1. The case $m < 0$

Case 1. $m = -p_1p_2$, $p_1p_2 \equiv 7 \pmod 8$.

Without loss of generality, we can assume that $p_1 < p_2$. Since $p_1 > M_k = \dfrac{2}{\pi}\sqrt{p_1p_2}$ for $k = \boldsymbol{Q}(\sqrt{-p_1p_2}) \in K^+ - E_8$, we have $p_2 < \dfrac{\pi^2}{4}p_1$.

We first prove the following lemma.

LEMMA 2. *For* $k = \boldsymbol{Q}(\sqrt{-p_1p_2}) \in K^+ - E_8$, *we have* $q < \dfrac{p_1p_2}{8}$ *if* $p_1p_2 > 3000$.

Proof. Suppose, on the contrary, that $q \geq \dfrac{p_1p_2}{8}$ for some $p_1p_2 > 3000$, since $p_1 < p_2 < 3p_1$, we have $23 < p_1 < q$. So $\left(\dfrac{23}{p_1p_2}\right) = 1$ by the minimality of q. Since $\left[\dfrac{p_1p_2}{24}\right] = \dfrac{p_1p_2}{24} - s$ for some positive real number $s < 1$, we have

$$\begin{aligned}
\frac{7}{8}p_1p_2 + 1 < \frac{22}{24}p_1p_2 &< \frac{22}{24}p_1p_2 + \left(\frac{p_1p_2}{24} - 23s\right) \\
&= 23\left(\frac{p_1p_2}{24} - s\right) \\
&= 23\left[\frac{p_1p_2}{24}\right] < p_1p_2 \qquad \text{for } p_1p_2 > 3000.
\end{aligned}$$

So we have $23\left[\frac{p_1p_2}{24}\right] = p_1p_2 - x$ for some integer x, $1 \leq x < \frac{p_1p_2}{8}$. Since $\left[\frac{p_1p_2}{24}\right] = \frac{p_1p_2}{24} - s \neq ap_1$ or bp_2 for any integers a, b (otherwise, we have

$$24 > 24s = \begin{cases} p_1(p_2 - 24a) \\ \quad\text{or} \\ p_2(p_1 - 24b) \end{cases} > 24,$$

a contradiction), we have $(x, p_1p_2) = 1$. Furthermore, $\left[\frac{p_1p_2}{24}\right] < \frac{p_1p_2}{8} \leq q$. Hence, we have

$$\begin{aligned} 1 &= \left(\frac{23}{p_1p_2}\right)\left(\frac{[\frac{p_1p_2}{24}]}{p_1p_2}\right) \\ &= \left(\frac{23[\frac{p_1p_2}{24}]}{p_1p_2}\right) \\ &= \left(\frac{p_1p_2 - x}{p_1p_2}\right) \\ &= \left(\frac{-x}{p_1p_2}\right) \\ &= \left(\frac{-1}{p_1p_2}\right)\left(\frac{x}{p_1p_2}\right) \\ &= -1, \text{ a contradiction,} \end{aligned}$$

Q.E.D.

Now we can prove Theorem 1 after the model of the proof of the theorem in [2][2)]

THEOREM 1. *For $k = \boldsymbol{Q}(\sqrt{-p_1p_2}) \in K^+ - E_8$, we have $p_1p_2 \leq 360000$.*

Proof. Since $\sqrt{2}(p_1p_2)^{2/5} + 8(p_1p_2)^{1/5} + 18 < \frac{2}{\pi}\sqrt{p_1p_2} = M_k$ for $p_1p_2 > 360000$, it suffices to prove that

$$q < \sqrt{2}(p_1p_2)^{2/5} + 8(p_1p_2)^{1/5} + 18 \tag{1.1}$$

for $k = \boldsymbol{Q}(\sqrt{-p_1p_2}) \in K^+ - E_8$ and $p_1p_2 > 360000$.

[2)] In p. 108 of [2], there seems to be a gap of arguments in the choice of a and the choice of α there. So we make our argument slightly different from [2]. Our inequality (1.1) is weaker than that of Hudson and Williams in [2] (the inequality (2.1)), but our (1.1) is enough to prove our theorems.

Assume, on the contrary, that

(1.2) $$q \geq \sqrt{2}(p_1p_2)^{2/5} + 8(p_1p_2)^{1/5} + 18, \qquad \text{for some } p_1p_2 > 360000.$$

Since $p_1p_2 \equiv 7 \pmod 8$, we have $\left(\frac{8}{p_1p_2}\right) = 1$ and $\left(\frac{-1}{p_1p_2}\right) = -1 = \chi_k(-1)$. By Lemma 2, we have $q < \frac{p_1p_2}{8}$ and so the integers

(1.3) $$p_1p_2 - 8(q-1), \quad p_1p_2 - 8(q-2), \cdots, p_1p_2 - 8$$

are all positive and belong to C or C_1.

Let r be an odd positive integer of the form

(1.4) $$r = \left[\frac{1}{2}(p_1p_2)^{1/5}\right] + \alpha$$

where α is a positive integer ≤ 4 to be chosen later.

Since

(1.5) $$\frac{1}{2}(p_1p_2)^{1/5} < r \leq \frac{1}{2}(p_1p_2)^{1/5} + 4$$

and $p_1 > M_k = \frac{2}{\pi}\sqrt{p_1p_2}$ as $k = \boldsymbol{Q}(\sqrt{-p_1p_2}) \in K^+ - E_8$, we must have

(1.6) $$r < p_1 \quad \text{and} \quad r \leq q - 1.$$

Let h be the unique integer satisfying

(1.7) $$8h \equiv 8q - p_1p_2 \pmod r, \qquad 1 \leq h \leq r.$$

By (1.7), we may define an integer n by

(1.8) $$n = \frac{p_1p_2 - 8(q-h)}{r}.$$

From (1.6) and (1.7), we have $1 \leq h \leq q-1$ and $1 \leq h < p_1$, and so the numerator in (1.8) is one of the integers in (1.3), and hence n is positive.

Now, let $l = [2(p_1p_2)^{1/5}] + 8$ so that

(1.9) $$2(p_1p_2)^{1/5} + 7 < l < 2(p_1p_2)^{1/5} + 8.$$

Further, put

(1.10) $$a = [n^{1/2}] + 1.$$

Then $n^{1/2} < a \leq n^{1/2} + 1$ so that $(a-1)^2 \leq n < a^2$. Finally, choose α such that

$$\text{either} \quad r \equiv 1 \pmod 8 \quad \text{or} \quad r \equiv 5 \pmod 8.$$

Case (I) $r \equiv 1 \pmod 8$.

(1.11) (a) $a \equiv 0$ or $3 \pmod 4$.

As we verify it soon, we have

$$(n + 8l - 8)r \leq p_1p_2 - 8, \tag{1.12}$$

and so the integers $nr, (n + 8)r, \cdots, (n + 8l - 8)r$ appear in the sequence (1.3) (c.f. (1.8)) and the l integers

$$n, n + 8, \cdots, n + 8l - 8, \tag{1.13}$$

belong either to C or to C_1 because $\left(\frac{r}{p_1p_2}\right) = 1$. These integers are $\equiv 7 \pmod 8$. Now, the condition (1.12) is satisfied because by (1.2), (1.5), (1.7), (1.8) and (1.9), we have

$$\begin{aligned}(n + 8l - 8)r &< p_1p_2 - 8q + 8r + 8r(2(p_1p_2)^{1/5} + 8) - 8r \\ &< p_1p_2 - 8q + 8\left(\frac{1}{2}(p_1p_2)^{1/5} + 4\right)(2(p_1p_2)^{1/5} + 8) \\ &< p_1p_2 - 8\sqrt{2}(p_1p_2)^{2/5} - 64(p_1p_2)^{1/5} - 144 \\ &\qquad + 8(p_1p_2)^{2/5} + 96(p_1p_2)^{1/5} + 256 \\ &= p_1p_2 - 8(p_1p_2)^{2/5}(\sqrt{2} - 1) + 32(p_1p_2)^{1/5} + 112 < p_1p_2 - 8.\end{aligned}$$

If $a \equiv 0 \pmod 4$, we consider the sequence of integers

$$(a + 1)(a - 1), (a + 3)(a - 3), \cdots, (a + 2b - 1)(a - 2b + 1) \tag{1.14}$$

where b is the largest integer such that

$$(a + 2b - 1)(a - 2b + 1) > (a - 1)^2; \tag{1.15}$$

if $a \equiv 3 \pmod 4$, we consider the sequence of integers

$$(a + 2)a, (a + 4)(a - 2), \cdots, (a + 2c)(a - 2c + 2) \tag{1.16}$$

where c is the largest integer such that

$$(a + 2c)(a - 2c + 2) > (a - 1)^2. \tag{1.17}$$

Since the integers in (1.14) and in (1.16) are $\equiv 7 \pmod 8$, we see that the integers in (1.13) are in the same residue class modulo 8 as those in (1.14) and as those in (1.16).

Next, we have $(a-1)^2 \leq n < \frac{p_1 p_2}{r} < 2(p_1 p_2)^{4/5}$, so $a < \sqrt{2}\,(p_1 p_2)^{2/5} + 1 < p_1$. Then we have

$$\begin{aligned} a + 2b - 1 < a + \sqrt{2a-1} &< \sqrt{2}\,(p_1 p_2)^{2/5} + \sqrt{2\sqrt{2}}((p_1 p_2)^{1/5} + 1) + 1 \\ &< \min(p_1, q), \end{aligned}$$

by (1.2) and by the inequalities, $p_1 p_2 > 360000$, $p_1 > \frac{2}{\pi}\sqrt{p_1 p_2}$. Therefore the integers in (1.14) belong to C_2. Similarly the integers in (1.16) belong to C_2.

Thus, subdividing the integer interval

$$\begin{cases} [(a-1)^2, (a-1)^2 + 1, \cdots, a^2 - 2, a^2 - 1] & \text{if } a \equiv 0 \pmod 4, \\ [(a-1)^2, (a-1)^2 + 1, \cdots, a^2 + 2a - 1, a^2 + 2a] & \text{if } a \equiv 3 \pmod 4) \end{cases}$$

by the integers in (1.14) and (1.16), respectively, we see, by (1.13), that $8l - 8$ is less than the maximum difference between integers in the subdivided interval. This gives the required contradiction; we just give the details for $a \equiv 3 \pmod 4$. In this case, the difference between integers in (1.16) in the subdivided interval of $[(a-1)^2, (a-1)^2 + 1, \cdots, a^2 + 2a - 1, a^2 + 2a]$ is at most

$$\begin{aligned} (a + 2c)(a - 2c + 2) - (a + 2c + 2)(a - 2c) &= 8c \\ &< 4 + 8a^{1/2} \\ &< 4 + 8\sqrt[4]{2}((p_1 p_2)^{1/5} + 1) \\ &< 16(p_1 p_2)^{1/5} + 20 \\ &< 8l - 8\,. \end{aligned}$$

(b) $a \equiv 1$ or $2 \pmod 4$.

If $a \equiv 2 \pmod 4$, we consider the sequence of integers

(1.14)′ $(a+3)(a+1),\ (a+5)(a-1), \cdots, (a+2b+1)(a-2b+3),$

where b is the largest integer such that

(1.15)′ $$(a + 2b - 1)(a - 2b + 1) > (a-1)^2;$$

if $a \equiv 1 \pmod 4$, we consider the sequence of integers

(1.16)′ $(a+6)a,\ (a+8)(a-2), \cdots, (a+2c)(a-2c+6)$

where c is the largest integer such that

$$(1.17)\qquad (a+2c)(a-2c+2) > (a-1)^2 .$$

By a similar argument as in (a), we also get a contradiction.

Similarly one wlll get a contradiction for Case (II) where $r \equiv 5 \pmod 8$, Q.E.D.

Case 2. $m = -p$, $p \equiv 7 \pmod 8$.

By almost the same argument as in the proof of Theorem 1, we have the following theorem.

THEOREM 1′. *For* $k = \boldsymbol{Q}(\sqrt{-p}) \in K^+ - E_8$, *we have* $p \leq 360000$.

According to Case 1 and Case 2, for $m < 0$ and $k = \boldsymbol{Q}(\sqrt{m}) \in K^+ - E_8$, $-m$ must be ≤ 360000. By the help of a computer in our department, we obtain that $m = -15, -23, -47, -71, -119$. (See table).

§ 2. The case $m > 0$

Case 1. $m = p$, $p \equiv 1 \pmod 8$.

By applying a theorem of L. Rédei [5], we shall prove Proposition 1 below which will provide $\frac{\sqrt{p}}{2}$ as an upper bound for the least quadratic-nonresidue of a prime $p \equiv 1 \pmod 8$ for $p > 97$.

THEOREM (L. Rédei [5]). *For* $4 \mid p-1$, *the density* δ_2 *of the quadratic residues, and also the density* δ_1 *of the non-residues* (mod p) *in the interval* $[1, \sqrt{p}]$ *is grater than* $\frac{1}{4+2\sqrt{2}}$ *and less than* $1 - \frac{1}{4+2\sqrt{2}}$.

PROPOSITION 1. *For* $p \equiv 1 \pmod 8$ *and* $p > 240000$ *then* $q < M_k = \frac{\sqrt{p}}{2}$.

Proof. Suppose, on the contrary, that there exists a prime $p_0 \equiv 1 \pmod 8$, $p_0 > 240000$ such that $q > \frac{\sqrt{p_0}}{2}$.

Let $x = [\sqrt{p_0}]$, the integral part of $\sqrt{p_0}$. Then one observes the following four cases.

(i) There are at least $\frac{x-a}{2}$ integers $< \frac{\sqrt{p_0}}{2}$ which are quadratic residues (mod p_0), where a is an integer, $0 \leq a \leq 1$, such that $\frac{x-a}{2}$ is an integer.

(ii) There are at least $\left(x - \frac{x+a'}{2}\right)\Big/2$ even integers in the interval $\left(\left[\frac{\sqrt{p_0}}{2}\right], [\sqrt{p_0}]\right)$, which are quadratic residues (mod p_0), where a' is an integer, $0 \leq a' \leq 3$, such that $x - \frac{x+a'}{2}$ is an even integer. (Note that for an even integer $2b < \sqrt{p_0}$, we have $b < \frac{1}{2}\sqrt{p_0}$ and so b is a quadratic residue.)

(iii) There are at least $\left(\frac{x-b}{3} - \frac{x+b'}{6}\right)\Big/2$ odd integers with 3 as a factor in the interval $\left(\left[\frac{\sqrt{p_0}}{2}\right], [\sqrt{p_0}]\right)$, which are quadratic residues (mod p_0), where b, b' are integers, $0 \leq b$, $b' \leq 5$, such that $\frac{x-b}{3}$, $\frac{x+b'}{6}$ and $\left(\frac{x-b}{3} - \frac{x+b'}{6}\right)\Big/2$ are integers.

(iv) There are at least $\frac{1}{3}\left\{\left(\frac{x-c}{5} - \frac{x+c'}{10}\right) - d\right\}$ odd integers relatively prime to 3 with 5 as a prime factor in the interval $\left(\left[\frac{\sqrt{p_0}}{2}\right], [\sqrt{p_0}]\right)$, which are quadratic residues (mod p_0), where c, c' and d are integers, $0 \leq c$, $c' \leq 9$, $0 \leq d \leq 2$, such that

$$\frac{x-c}{5},\ \frac{x+c'}{10} \quad \text{and} \quad \frac{1}{3}\left\{\left(\frac{x-c}{5} - \frac{x+c'}{10}\right) - d\right\}$$

are integers.

From (i), (ii), (iii) and (iv), we see that there are at least

$$N = \frac{x-a}{2} + \left(x - \frac{x+a'}{2}\right)\Big/2 + \left(\frac{x-b}{3} - \frac{x+b'}{6}\right)\Big/2 + \frac{1}{3}\left\{\left(\frac{x-c}{5} - \frac{x+c'}{10}\right) - d\right\}$$

distinct integers in the interval $[1, \sqrt{p_0}]$, which are quadratic residues (mod p_0). We have

$$\begin{aligned} N &\geq \frac{x-1}{2} + \left(x - \frac{x+3}{2}\right)\Big/2 + \left(\frac{x-5}{3} - \frac{x+5}{6}\right)\Big/2 \\ &\quad + \frac{1}{3}\left\{\left(\frac{x-9}{5} - \frac{x+9}{10}\right) - 2\right\} \\ &= \frac{52x - 244}{60}. \end{aligned}$$

So the density δ_2 of quadratic residues in $[1, \sqrt{p_0}] > \frac{N}{x} \geq \frac{1}{60}\left(52 - \frac{244}{x}\right)$.

Since $\frac{1}{4 + 2\sqrt{2}} > \frac{1}{7}$, we have

$$1 = \delta_1 + \delta_2 > \frac{1}{7} + \frac{52 - \frac{244}{x}}{60} = \frac{424 - \frac{1708}{x}}{420} > 1 \qquad \text{for } p_0 > 240000,$$

a contradiction, Q.E.D.

Case 2. $m = p_1 p_2$, $p_1 p_2 \equiv 1 \pmod 8$.

Without loss of generality, one can assume that $p_1 < p_2$. Since $p_1 > M_k = \frac{\sqrt{p_1 p_2}}{2}$ for $k = \boldsymbol{Q}(\sqrt{p_1 p_2}) \in K^+ - E_8$, we have $p_2 < 4p_1$.

For $p_1 p_2 \equiv 1 \pmod 8$, $p_1 < p_2 < 4p_1$ and $p_1 p_2 > 300$, by a theorem of Thue [1], the congruence $x \equiv ny \pmod{p_1 p_2}$ has non-trivial solutions x, y for which $|x| \leq \sqrt{p_1 p_2}$ and $|y| \leq \sqrt{p_1 p_2}$. We can choose a positive integer n such that $n < p_1 p_2$, $(n, p_1 p_2) = 1$, $n \not\equiv +1 \pmod{p_2}$ and $\left(\frac{n}{p_1 p_2}\right) = -1$. By the choice of n, we see that one of the numbers x and y, say x, must belong to C_1. (Note that $p_1 < \sqrt{p_1 p_2} < 2p_1$, so neither $|x|$ nor $|y|$ equal to p_1, because otherwise $n \equiv +1$ or $-1 \pmod{p_2}$, which contradicts the choice of n.) Since $\left(\frac{x}{p_1 p_2}\right) = -1$, we have $\left(\frac{-x}{p_1 p_2}\right) = -1$. So there exists a positive integer $x < \sqrt{p_1 p_2}$ such that $\left(\frac{x}{p_1 p_2}\right) = -1$. Denote by v_i the number of elements in C_i, $i = 1, 2$, which lie in the interval $[1, \sqrt{p_1 p_2}]$. Furthermore, since $\left(\frac{2}{p_1 p_2}\right) = 1$, we see that $v_i \neq 0$, $i = 1, 2$, for $k = \boldsymbol{Q}(\sqrt{p_1 p_2}) \in K^+ - E_8$ and $p_1 p_2 > 300$. We have $v_1 + v_2 = [\sqrt{p_1 p_2}] - 1$ because $p_1 < \sqrt{p_1 p_2}$. Denote by $\delta_i = \frac{v_i}{[\sqrt{p_1 p_2}] - 1}$ the density of the class C_i in the interval $[1, \sqrt{p_1 p_2}]$, for $i = 1, 2$. Now we are ready to prove Theorem 2 which is similar to a theorem of Rédei [5].

THEOREM 2. *For* $k = \boldsymbol{Q}\sqrt{p_1 p_2})$, *if* $p_1 p_2 \equiv 1 \pmod 8$, $p_1 < p_2 < 4p_1$ *and* $p_1 > 265$, *then we have* $\frac{1}{7} < \delta_1, \delta_2 < 1 - \frac{1}{7}$.

Proof. Since $(p_1 - 1)(p_2 - 1)/2$ is the number of incongruent elements $\pmod{p_1 p_2}$ in C_d, $d = 1, 2$, for $\alpha \in C_1$ with $\alpha \not\equiv \pm 1 \pmod{p_2}$, there exist x,

y, $x \in C_i$, $y \in C_j$, $i \neq j$, $1 \leq x, y < \sqrt{p_1 p_2}$, such that $\alpha \equiv \frac{y}{x}$ or $-\frac{y}{x}$ (mod $p_1 p_2$). From this, we have

$$(2.1) \qquad 2(v_1 v_2 + v_2 v_1) \geq \frac{(p_1 - 1)(p_2 - 1)}{2} - 2p_1$$

where $2p_1$ is the number of elements in the set

$$\{n \in N;\ n < p_1 p_2,\ n \equiv +1 \text{ or } -1 \pmod{p_2}\}.$$

Then since $v_1 + v_2 = [\sqrt{p_1 p_2}] - 1$, one has, by (2.1),

$$(2.2) \qquad \delta_1 \delta_2 + \delta_2 \delta_1 \geq x \qquad \left(x = \frac{(p_1 - 1)(p_2 - 1) - 4p_1}{4([\sqrt{p_1 p_2}] - 1)^2}\right)$$

$$(2.3) \qquad \delta_1 + \delta_2 = 1.$$

Consider the equations:

$$(2.4) \qquad 2uv = x,$$

$$(2.5) \qquad u + v = 1.$$

One solution for (2.4), (2.5) is

$$(2.6) \qquad u = \frac{1 + \sqrt{1 - 2x}}{2}, \qquad v = \frac{1 - \sqrt{1 - 2x}}{2}$$

by which the square root may be chosen positive because $2x < 1$ for $p_1 > 265$.

We set

$$(2.7) \qquad \delta_1 = \frac{v_1}{[\sqrt{p_1 p_2}] - 1} = u + \alpha_1, \qquad \delta_2 = \frac{v_2}{[\sqrt{p_1 p_2}] - 1} = v + \alpha_2$$

where α_1, α_2 are real numbers. By (2.3), (2.5) we have

$$(2.8) \qquad \alpha_1 + \alpha_2 = 0.$$

Furthermore, it follows from (2.2) that

$$2\delta_1 \delta_2 \geq x,$$

i.e., by (2.3), $\delta_1^2 + \delta_2^2 \leq 1 - x$.

By (2.7) we have

$$u^2 + v^2 + 2u\alpha_1 + 2v\alpha_2 + (\alpha_1^2 + \alpha_2^2) \leq 1 - x.$$

Since $u^2+v^2=1-x$ by (2.6) and $\alpha_1^2+\alpha_2^2 \geq 0$, we have $2u\alpha_1+2v\alpha_2 \leq 0$. By (2.8), we also have $2u\alpha_1-2v\alpha_1 \leq 0$. On the other hand it follows from (2.6) that $u-v>0$, and so $\alpha_1 \leq 0$, i.e., by (2.7), $\delta_1 \leq u$. Because the conditions (2.2), (2.3) are symmetric in δ_1, δ_2, one has $\delta_i \leq u$, $i=1, 2$. Furthermore, we have $([\sqrt{p_1p_2}]-1)^2 \leq \frac{65}{64}[(p_1-1)(p_2-1)-4p_1]$ because $p_1>265$ and, by (2.2), we have $2x \geq \frac{32}{65}$. Therefore, by (2.6), we have

$$\begin{aligned}\delta_i \leq u &\leq \left(1+\sqrt{\frac{33}{65}}\right)\Big/2 \\ &\approx 0.8562\cdots \\ &\leq 1-\frac{1}{7} \approx 0.8571\cdots\end{aligned}$$

where $i=1, 2$, Q.E.D.

By the similar argument as the proof of Proposition 1, we have the following proposition:

PROPOSITION 2. *Assume that* $k=\boldsymbol{Q}(\sqrt{p_1p_2})$, $p_1p_2 \equiv 1 \pmod 8$, $p_1<p_2<4p_1$, $p_1>265$ *and* $p_1p_2>240000$. *Then* $q \leq M_k = \frac{\sqrt{p_1p_2}}{2}$.

According to Proposition 1 and Proposition 2, we see that for $m>0$ and $k=\boldsymbol{Q}(\sqrt{m}) \in K^+ - E_8$, m must be less than 290000. With the help of computer, we obtain that $m=17, 33, 73, 97$. (See table.)

Combining the results in § 1 and § 2, we have proved that

$$K^+ - E_8 = \{k=\boldsymbol{Q}(\sqrt{m});\ m=-15, -23, -47, -71, -119, 17, 33, 73, 97\}.$$

Table[3]

$m > 0$				$m < 0$			
$m = 0$	q	$m = p_1 p_2$	q	$-m = p$	q	$-m = p_1 p_2$	q
17	—	33	—	23	—	15	—
41	3	65	3	31	3	55	3
73	—	161	3	47	—	119	—
89	3	209	3	71	—	143	5
97	—	377	3	79	3	247	3
113	3	473	3	103	3	391	3
137	3	481	7	127	3	527	5
193	5	697	5	151	3	551	11
233	3	713	3	167	5	703	3
241	7	817	5	191	7	943	3
257	3	1073	3	199	3	1247	5
281	3	1081	7	223	3	1271	7
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
239641	7	239969	3	359311	3	356047	3
239689	11	240809	3	359327	5	356359	3
239713	5	241697	3	359407	3	356519	7
239737	5	243721	19	359479	3	356639	19
239753	3	244921	7	359599	3	357191	7
239849	3	251089	7	359663	5	357407	5
239857	5	254321	3	359719	3	358151	17
239873	3	258529	7	359767	3	358871	7
239929	11	259313	3	359783	5	359039	7
239977	5	260633	3	359911	3	359831	19
240017	3	271153	5	360007	3	359903	5
240041	3	273257	3	360023	5	359999	17

[3] In the column "q" of the table, the smallest odd prime $q \leq M_k$ such that $\chi_k(q) = -1$ is given. Since the complete table would occupy at least 20 pages long, we only show the beginning and the end of the original table.

References

[1] A. Brauer, Combinatorial Methods in the Distribution of k-th Power Residues, Combinatorial Mathematics and its Applications, Chapel Hill 1967, 14–37.

[2] R. H. Hudson and K. S. Williams, On the Least Quadratic Nonresidue of a prime $p \equiv 3 \pmod 4$, J. Reine Angew. Math., **318** (1980), 106–109.

[3] M.-G. Leu, On a Conjecture of Ono on Real Quadratic Fields, Proc. Japan Acad., **63**A (1987), 323–326.

[4] T. Ono, A Problem on Quadratic Fields, Proc. Japan Acad., **64**A (1988), 78–79.

[5] L. Rédei, Über die Anzahl der Potenzreste mod p im Intervall, 1, $\sqrt{p}$ Nieuw Arch. Wiskunde, (2) **23** (1950), 150–162.

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

Department of Mathematics
The Johns Hopkins University
Baltimore, MD 21218
U.S.A.

Permanent address:
Department of Mathematics
National Central University
Chung-Li, Taiwan 32054
R. O. C.