87. On Ono's Problem on Quadratic Fields

By Kakuzi YOSHIDOME and You ASAEDA
Department of Mathematics, Gakushuin University

(Communicated by Shokichi IYANAGA, M. J. A., Dec. 12, 1991)

1. Prof. T. Ono [1] posed the following problem on quadratic fields.

Let m be a square-free integer, $k=\boldsymbol{Q}(\sqrt{m})$, Δ_k the discriminant, χ_k the Kronecker character and M_k the Minkowski constant.

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

The problem is to determine the set K^+ of all k's such that $\chi_k(p)=+1$ for all rational primes $p\leq M_k$. Obviously $K^+\supset E_8=\{k=\boldsymbol{Q}(\sqrt{m})\,|\,m=-1, \pm 2, \pm 3, 5, -7, 13\}$ as there is no primes $\leq M_k$ for $k\in E_8$. We put $K^+\backslash E_8=S$. Our problem is to determine S.

In [1] it is conjectured that

(*) $S=\{k=\boldsymbol{Q}(\sqrt{m})\,|\,m=17, 33, 73, 97, -15, -23, -47, -71, -119\}$.

Our aim is to prove this conjecture. (*) is easily deduced from the following theorem, where $(n/|m|)$ is the Jacobi symbol.

Theorem. *Let $m=p$ or pq, where p, q are distinct prime numbers.*

(1) *If $m\equiv 1 \pmod 8$ and $7<\sqrt{m}/2<p, q$, then there exists an odd prime $p'<\sqrt{m}/2$ such that $(p'/m)=-1$.*

(2) *If $m\equiv 7 \pmod 8$ and $20<\sqrt{m}$, $2\sqrt{m}/\pi<p, q$, then there exists an odd prime $p'<2\sqrt{m}/\pi$ such that $(p'/m)=-1$.*

2. We shall prove this theorem in each of the two cases (1) and (2). To prove the case (1) we need the following Proposition.

Proposition. *Let $m=p$ or pq, where p, q are distinct prime numbers such that $\sqrt{m}/2<p, q$. If $m\equiv 1 \pmod 8$, then there exists an odd prime $p'<\sqrt{m}$ such that $(p'/m)=-1$.*

Proof. Let $m=p$. Assume $(p_i/m)=+1$ for every prime $p_i<\sqrt{p}$. Denote p_0 the minimal prime satisfying both conditions $\sqrt{p}<p_0<p$ and $(p_0/m)=-1$. There exists a positive integer $n<\sqrt{p}$ such that $0<p-np_0<p_0$. Then $1=((p-np_0)/p)=(-1/p)(n/p)(p_0/p)=-1$, which is a contradiction.

A similar proof is valid for the case $m=pq$.

3. *Proof of the case* (1). Assume $(p_i/m)=+1$ for every prime $p_i<\sqrt{m}/2$. Then we have $m\equiv 1 \pmod 8$ and $m\equiv 1 \pmod 3$ by the assumptions $7<\sqrt{m}/2$ and $(3/m)=+1$. Let p_0 be the minimal prime such that $\sqrt{m}/2<p_0<\sqrt{m}$ and $(p_0/m)=-1$. Such p_0 exists because of the above proposition.

Put

$$G=\{x\in N \mid \text{all prime components of } x<\sqrt{m}/2\}$$
$$G_{p_0}=\{x\in N \mid \text{all prime components of } x<p_0\}.$$

There exists a positive integer n such that $0<m-np_0<p_0$, where

$$n=\begin{cases} l & l\in G, \\ 2p_1 & \sqrt{m}/2<p_1<\sqrt{m}, \qquad p_1 \text{ is prime,} \\ 3p_2 & \sqrt{m}/2<p_2<2\sqrt{m}/3, \qquad p_2 \text{ is prime,} \\ p_3 & \sqrt{m}-1<p_3<2\sqrt{m}, \qquad p_3 \text{ is prime.} \end{cases}$$

If $n=l\in G$, then $(m-lp_0, m)=1$ and $((m-lp_0)/m)=1$ because $m-lp_0<p_0$, but $((m-lp_0)/m)=(-1/m)(l/m)(p_0/m)=-1$, a contradiction.

Let $n=2p_1$ or $3p_2$ or p_3. Put $m-np_0=r$. If we can choose a suitable integer a such that $|n-a|\in G$ and $|ap_0+r|\in G_{p_0}$, then $(n-a, m)=(ap_0+r, m)=1$ and $((n-a)/m)=((ap_0+r)/m)=+1$, hence $((m-(n-a)p_0)/m)=((ap_0+r)/m)=1$. On the other hand $((m-(n-a)p_0)/m)=(-1/m)((n-a)/m)(p_0/m)=-1$, which is a contradiction.

So we have only to find a such that $|a|\le 7$, $a\equiv n \pmod 5$ and that ap_0+r has a factor $>|a|$ and $\in G$. The following Table A shows how we can find it. This table is made as follows.

Table A

(a) $n=2p_1$

	$p_0\equiv5$ (6) $p_1\equiv5$ (6)	$p_0\equiv5$ (6) $p_1\equiv1$ (6)	$p_0\equiv1$ (6) $p_1\equiv5$ (6)	$p_0\equiv1$ (12) $p_1\equiv1$ (6)	$p_0\equiv7$ (12) $p_1\equiv1$ (6)
a	2	1 −3 3 −1	1 −3 3 −1	1 −3 −2 −1	1 7 −2 −1

(b) $n=3p_2$

	$p_0\equiv1$ (6)	$p_0\equiv5$ (6) $p_2\equiv1$ (4)	$p_0\equiv5$ (6) $p_2\equiv3$ (4)
a	−4 2 −2 −1	−1	1

(c) $n=p_3$

	$p_3\equiv5$ (6)	$p_3\equiv1$ (6)				
		$p_0\equiv5$ (6)	$p_0\equiv1$ (12) $p_3\equiv1$ (4)	$p_0\equiv1$ (12) $p_3\equiv3$ (4)	$p_0\equiv7$ (12) $p_3\equiv1$ (4)	$p_0\equiv7$ (12) $p_3\equiv3$ (4)
a	−1	−4 2 −2 −1	−4 −3 −2 −1	6 −3 −2 --1	6 −3 −2 −1	−4 −3 −2 −1

Three cases are considered, (a) $n=2p_1$, (b) $n=3p_2$, (c) $n=p_3$, and each case is further divided according to the nature of p_0 and p_i $(i=1,2,3)$. If, for example, $p_0\equiv 5 \pmod 6$, $p_1\equiv 5 \pmod 6$ in case (a), we can take $a=2$. In this case, the condition $a\equiv n \pmod 5$ is unnecessary, because a satisfies $a\equiv n \pmod 4$. If $p_0\equiv 5 \pmod 6$, $p_1\equiv 1 \pmod 6$, then we can take $a=1$, -3, 3, -1 according as $n\equiv 1,2,3,4 \pmod 5$. If $p_3\equiv 5 \pmod 6$ in case (c), we can take $a=-1$ which satisfies $a\equiv n \pmod 6$. Likewise in other cases.

4. *Proof of the case* (2). Assume $(p_i/m)=+1$ for every prime $p_i<2\sqrt{m}/\pi$. Put

$$M=\{x\in N \mid \text{all prime components of } x<2\sqrt{m}/\pi\}.$$

(I) If there exists an integer $a\in M$ such that $m-a\in M$, then (m,a) $(m,m-a)=1$ and $1=((m-a)/m)=(-1/m)(a/m)=-1$, which is a contradiction.

(II) If there exists an integer b such that $m-b^2\in M$, then $(m-b^2,m)=1$ and $1=((m-b^2)/m)=(-1/m)(b/m)^2=-1$, which is a contradiction.

Thus the proof will be done if we can show that there exists either (I) a with $a\in M$ and $m-a\in M$ or (II) b with $m-b^2\in M$.

Put now $a_0=[\sqrt{m}]$. If $m\equiv a_0^2 \pmod 5$, we have only to put $b=a_0$ to get b satisfying (II).

By the assumptions that $(p_i/m)=+1$ for every $p_i<2\sqrt{m}/\pi$ and $20<$

Table B

(a) $m\equiv 1 \pmod 5$

t_1 t_2 t_3		t_1 t_2 t_3		t_1 t_2 t_3		t_1 t_2 t_3		t_1 t_2 t_3	
0 1 0	(−2,2)	0 2 0	(−2,2)	1 0 0	(−3,3)	1 1 0	(−3,3)	1 2 0	(−8,−2)
0 1 2	(−6,4)	0 2 2	(−4,0)	1 0 2	(II,0,1)	1 1 2	(II,−2,3)	1 2 2	(−9,5)
0 1 3	(−1,0)	0 2 3	(*)	1 0 3	(−1,0)	1 1 3	(*)	1 2 3	(II,−2,3)

(*)

t_1 t_2 t_3 t_4	$m\equiv 3(7)$	$m\equiv 5(7)$	$m\equiv 6(7)$	t_1 t_2 t_3 t_4	$m\equiv 3(7)$	$m\equiv 5(7)$	$m\equiv 6(7)$
0 2 3 0	(−2,2)	(−2,1)	(−13,13)	1 1 3 0	(−4,1)	(−3,3)	(−1,1)
0 2 3 1	(−3,1)	(−2,1)	(−4,4)	1 1 3 1	(−3,1)	(−4,2)	(−3,3)
0 2 3 2	(−3,2)	(−6,2)	(−6,5)	1 1 3 2	(−1,1)	(−8,3)	(−4,2)
0 2 3 3	(−4,1)	(−2,2)	(−6,2)	1 1 3 3	(−4,1)	(−8,3)	(−9,−4)
0 2 3 4	(−2,1)	(−2,2)	(−3,2)	1 1 3 4	(−9,1)	(−5,5)	(−3,2)
0 2 3 5	(−10,9)	(−3,1)	(−4,1)	1 1 3 5	(−1,1)	(−3,1)	(−4,1)
0 2 3 6	(−3,2)	(−4,0)	(−4,4)	1 1 3 6	(−3,2)	(−7,3)	(−3,3)

(b) $m\equiv 4 \pmod 5$

t_1 t_2 t_3		t_1 t_2 t_3		t_1 t_2 t_3		t_1 t_2 t_3		t_1 t_2 t_3	
0 1 0	(−4,4)	0 2 0	(−4,4)	1 0 0	(−1,1)	1 1 0	(−1,1)	1 2 0	(−1,1)
0 1 1	(−2,0)	0 2 1	(−1,1)	1 0 1	(**)	1 1 1	(−5,3)	1 2 1	(**)
0 1 4	(−1,1)	0 2 4	(**)	1 0 4	(**)	1 1 4	(**)	1 2 4	(II,−2,3)

$\sqrt{m}$, we have $(m/3)=(m/7)=-1$, $(m/5)=1$, which means $m\equiv 2 \pmod 3$, $m\equiv 1, 4 \pmod 5$, $m\equiv 3, 5, 6 \pmod 7$.

We shall put $a_0\equiv t_1 \pmod 2$, $\equiv t_2 \pmod 3$, $\equiv t_3 \pmod 5$, $\equiv t_4 \pmod 7$, and consider the different cases according to the values of (t_1, t_2, t_3, t_4), $t_1\in\{0,1\}$, $t_2\in\{0,1,2\}$, $t_3\in\{0,1,2,3,4\}$, $t_4\in\{0,1,2,3,4,5,6\}$.

If $t_1=t_2=0$, i.e. $6\mid a_0$, then $a=(a_0-3)(a_0+3)$ satisfies obviously (I). If $m\equiv 1 \pmod 5$ and $t_3=1$ or 4, or if $m\equiv 4 \pmod 5$ and $t_3=2$ or 3, then $b=a_0$ satisfies (II) as noticed above.

The following Table B will show how we can get a satisfying (I) or b satisfying (II) in all other cases.

This Table B consists of two tables (a) for the case $m\equiv 1 \pmod 5$ and (b) for the case $m\equiv 4 \pmod 5$, and to (a) and (b) are attached (*) and (**) respectively.

If, for example, $t_1=0$, $t_2=1$, $t_3=0$ in case $m\equiv 1 \pmod 5$, we can take $a=(a_0-2)(a_0+2)$. Thus (s,t) in Table B means that we can take $a=(a_0+s)(a_0+t)$.

If $t_1=0$, $t_2=2$, $t_3=3$ in case $m\equiv 1 \pmod 5$, the table (a) refers to (*). Then we must consider different values of t_4 and further the different values of $m \bmod 7$. If, for example, $t_1=0$, $t_2=2$, $t_3=3$, $t_4=0$ and $m\equiv 3 \pmod 7$, we can take $a=(a_0-2)(a_0+2)$.

(**)

t_1	t_2	t_3	t_4	$m\equiv 3(7)$	$m\equiv 5(7)$	$m\equiv 6(7)$	t_1	t_2	t_3	t_4	$m\equiv 3(7)$	$m\equiv 5(7)$	$m\equiv 6(7)$
0	2	4	0	(-2,2)	(-4,4)	(-6,6)	1	1	4	0	(-5,5)	(-3,3)	(-1,1)
0	2	4	1	(-6,4)	(-2,1)	(-1,1)	1	1	4	1	(-3,1)	(-4,2)	(-3,3)
0	2	4	2	(-4,0)	(-5,1)	(-10,6)	1	1	4	2	(-1,1)	(II, -2,3)	(-4,2)
0	2	4	3	(-8,-5)	(-2,2)	(-6,2)	1	1	4	3	(II, -5,6)	(-5,5)	(II, -4,5)
0	2	4	4	(-2,1)	(-2,2)	(-10,2)	1	1	4	4	(-9,1)	(-3,1)	(-3,2)
0	2	4	5	(-10,7)	(-6,4)	(-8,0)	1	1	4	5	(-1,1)	(-3,1)	(-14,6)
0	2	4	6	(-10,2)	(-4,0)	(-4,4)	1	1	4	6	(-3,2)	(II, -5,6)	(-3,3)
1	0	1	0	(-12,5)	(-3,3)	(-1,1)	1	2	1	0	(-3,-1)	(-2,1)	(-1,1)
1	0	1	1	(-6,4)	(-5,3)	(-3,3)	1	2	1	1	(-13,-3)	(-2,1)	(-3,3)
1	0	1	2	(-6,6)	(-15,3)	(-6,0)	1	2	1	2	(-1,1)	(-15,3)	(-5,3)
1	0	1	3	(-7,5)	(-7,1)	(-1,0)	1	2	1	3	(-7,5)	(-5,5)	(II, -2,3)
1	0	1	4	(-9,1)	(-6,4)	(-6,0)	1	2	1	4	(-2,1)	(-5,5)	(II, -6,7)
1	0	1	5	(-1,1)	(-9,6)	(-1,0)	1	2	1	5	(-1,1)	(-6,4)	(-8,7)
1	0	1	6	(-7,5)	(-5,-1)	(-3,3)	1	2	1	6	(-7,5)	(-7,3)	(-3,3)
1	0	4	0	(-4,1)	(-3,3)	(-1,1)							
1	0	4	1	(-11,5)	(-3,0)	(-3,3)							
1	0	4	2	(-1,1)	(-3,0)	(-6,0)							
1	0	4	3	(-4,1)	(-7,1)	(-1,0)							
1	0	4	4	(-13,5)	(-1,0)	(-6,0)							
1	0	4	5	(-3,0)	(-7,3)	(-1,0)							
1	0	4	6	(-5,-3)	(-7,3)	(-3,3)							

In case $t_1=1$, $t_2=0$, $t_3=2$, $m\equiv 1 \pmod 5$, the table (a) gives (II, 0, 1). In general, (II, s, t) means that we should separate two cases according as, $\varepsilon<1/2$ or $\varepsilon>1/2$ where $\varepsilon=\sqrt{m}-a_0$, and $b=a_0$ satisfies (II) if $\varepsilon<1/2$, while $a=(a_0+s)(a_0+t)$ satisfies (I) if $\varepsilon>1/2$. Thus in the present case, we have $b=a_0$ or $a=a_0(a_0+1)$ in each case. Likewise in other cases.

Reference

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