H. Yokoi
Nagoya Math. J.
Vol. 134 (1994), 137–149

SOLVABILITY OF THE DIOPHANTINE EQUATION $x^2 - Dy^2 = \pm 2$ AND NEW INVARIANTS FOR REAL QUADRATIC FIELDS

HIDEO YOKOI

In our recent papers [3, 4, 5], we defined some new D-invariants for any square-free positive integer D and considered their properties and interrelations among them. Especially, as an application of it, we discussed in [5] the characterization of real quadratic field $\mathbf{Q}(\sqrt{D})$ of so-called *Richaud-Degert* type in terms of these new D-invariants.

Main purpose of this paper is to investigate the Diophantine equation $x^2 - Dy^2 = \pm 2$ and to discuss characterization of the solvability in terms of these new D-invariants. Namely, we consider the equation $x^2 - Dy^2 = \pm 2$ and first provide necessary conditions for the solvability by using an additive property and the multiplicative structure of D (Proposition 2). Next, we provide necessary and sufficient conditions for the solvability in terms of an unit of the real quadratic field $\mathbf{Q}(\sqrt{D})$ (Theorems 1,2). Finally, we provide sufficient conditions for the solvability in terms of new D-invariants (Theorems 3,4). It is conjectured with a great expectation for these conditions to be also necessary conditions.

Throughout this paper, for any square-free positive integer D we denote by $\varepsilon_D = (t_D + u_D\sqrt{D})/2$ (> 1) the fundamental unit of the real quadratic field $\mathbf{Q}(\sqrt{D})$ and by N the norm mapping from $\mathbf{Q}(\sqrt{D})$ to the rational number field $\mathbf{Q}$. Moreover, we denote $(\ /\ )$ the Legendre's symbol and by $[x]$ the greatest integer less than or equal to x.

On Pell's equation, we know already the following result by Perron (cf. [1], p. 106-109):

Proposition 1 (O. Perron). *For any positive square-free integer $D \neq 2$, at most only one of the following three equations is solvable in integers*:

Received April 19, 1993.

$$x^2 - Dy^2 = -1, \quad x^2 - Dy^2 = 2, \quad x^2 - Dy^2 = -2.$$

We may first provide the following necessary condition for solvability of the equation $x^2 - Dy^2 = \pm 2$:

PROPOSITION 2. *For any positive square-free integer D, if the Diophantine equation $x^2 - Dy^2 = \pm 2$ has an integral solution, then*

$$D \equiv 2 \text{ or } 3 \pmod 4 \quad \text{and} \quad N\varepsilon_D = 1$$

hold.

Moreover, if the equation $x^2 - Dy^2 = 2$ is solvable, then

$$p \equiv \pm 1 \pmod 8$$

holds for any odd prime factor p of D, and if the equation $x^2 - Dy^2 = -2$ is solvable, then

$$q \equiv 1 \text{ or } 3 \pmod 8$$

holds for any odd prime factor q of D.

Proof. When $x^2 - Dy^2 = \pm 2$ has an integral solution $(x, y) = (a, b)$, if we assume $D \equiv 1 \pmod 4$, then we get

$$a^2 - Db^2 \equiv a^2 - b^2 \equiv 0 \text{ or } \pm 1 \pmod 4,$$

which contradicts with $a^2 - Db^2 = \pm 2$.
Hence $D \equiv 2$ or $3 \pmod 4$ holds.

On the other hand, if we assume $N\varepsilon_D = -1$, then the equation $x^2 - Dy^2 = -1$ is solvable, which contradicts with solvability of $x^2 - Dy^2 = \pm 2$ by Proposition 1. Hence $N\varepsilon_D = 1$ holds.

Moreover, if the equation $x^2 - Dy^2 = 2$ is solvable, then for any odd prime factor p of D, we get $(2/p) = 1$, and so $p \equiv \pm 1 \pmod 8$ holds.

If the equation $x^2 - Dy^2 = -2$ is solvable, then for any odd prime factor q of D, we get $(-2/q) = 1$, and so $q \equiv 1$ or $\pmod 8$ holds.

Now we may provide the following necessary and sufficient conditions through an unit of the associated real quadratic field $\mathbf{Q}(\sqrt{D})$ with the equation $x^2 - Dy^2 = \pm 2$:

THEOREM 1. *For any positive square-free integer D, it is necessary and sufficient* *for the equation* $x^2 - Dy^2 = 2$ *to be solvable that there exists an unit* $\varepsilon = (t + u\sqrt{D})/2 > 1$ *of the real quadratic field* $\mathbf{Q}(\sqrt{D})$ *such that*

$$N\varepsilon = 1 \quad \text{and} \quad t = Dm + 2$$

for a positive integer m *satisfying* $m \equiv 2 \pmod 8$.

Proof. If the equation $x^2 - Dy^2 = 2$ has an integral positive solution

$$(x, y) = (n_1, n_2),$$

i.e. $n_1^2 - Dn_2^2 = 2$ holds, then

$$(t, u) = (2n_1^2 - 2, 2n_1n_2)$$

is an integral positive solution of the Diophantine equation $t^2 - Du^2 = 4$, and hence $\varepsilon = (t + u\sqrt{D})/2 > 1$ is an unit of $\mathbf{Q}(\sqrt{D})$ and satisfies $N\varepsilon = 1$.

Moreover, if we put $m = 2n_2^2$, then

$$t = 2n_1^2 - 2 = Dm + 2$$

holds, and from $n_2 \equiv 1 \pmod 4$ we get immediately

$$m = 2n_2^2 \equiv 2 \pmod 8.$$

Conversely, if there exists an unit $\varepsilon = (t + u\sqrt{D})/2 > 1$ of $\mathbf{Q}(\sqrt{D})$ such that $N\varepsilon = 1$ and $t = Dm + 2$ for a positive integer m satisfying $m \equiv 2 \pmod 8$, then from $N\varepsilon = 1$ we get

$$Du^2 = t^2 - 4 = D(Dm + 4)m, \quad \text{and so} \quad u^2 = (Dm + 4)\, m.$$

On the other hand, $m \equiv 2 \pmod 8$ implies $(Dm + 4, m) = 2$. Hence, there exist two positive integers n_1, n_2 such that

$$Dm + 4 = 2n_1^2,\ m = 2n_2^2, \quad ((n_1, n_2) = 1,\ u = 2n_1n_2),$$

and hence $n_1^2 - Dn_2^2 = 2$ holds.

Therefore, the equation $x^2 - Dy^2 = 2$ has an integral positive solution

$$(x, y) = (n_1, n_2).$$

For the equation $x^2 - Dy^2 = -2$, we can prove the following analogous theorem:

THEOREM 2. *For any positive square-free integer* D, *it is necessary and sufficient for the equation* $x^2 - Dy^2 = -2$ *to be solvable that there exists an unit* $\varepsilon = (t +$

$u\sqrt{D})/2>1$ *of the real quadratic field* $\mathbf{Q}(\sqrt{D})$ *such that*

$$N\varepsilon = 1 \quad \textit{and} \quad t = Dm - 2$$

for a positive integer m *satisfying* $m \equiv 2 \pmod 8$.

For any positive square-free integer D, we put

$$\mathbf{A}_D = \{a : 0 \leqq a < D,\ a^2 \equiv 4N\varepsilon_D \pmod D\},$$

and

$$(A, B)_D = \{(a, b) : a \in \mathbf{A}_D,\ a^2 - 4N\varepsilon_D = bD\}.$$

Then, we obtained in [5] the following result:

There are uniquely determined non-negative integer m_D and (a_D, b_D) in $(A, B)_D$ such that

$$\begin{cases} t_D = D\cdot m_D + a_D \\ u_D^{\ 2} = D\cdot m_D^{\ 2} + 2a_D\cdot m_D + b_D. \end{cases}$$

Now, we may prove first the following:

PROPOSITION 3. *Under the assumption* $D \neq 2,5$,

$$a_D = 2 \quad \textit{if and only if} \quad b_D = 0,$$

and

$$a_D = D - 2 \quad \textit{if and only if} \quad b_D = D - 4.$$

Proof. $a_D = 2$ implies $b_D D = a_D^{\ 2} - 4N\varepsilon_D = 4(1 - N\varepsilon_D)$, and hence from $D \neq 2$, we get $N\varepsilon_D = 1$ and $b_D = 0$.

Conversely, $b_D = 0$ implies

$$a_D^{\ 2} = b_D D + 4N\varepsilon_D = 4N\varepsilon_D,$$

and so we get

$$N\varepsilon_D = 1 \quad \text{and} \quad a_D = 2.$$

Moreover, $a_D = D - 2$ implies

$$b_D D = a_D^{\ 2} - 4N\varepsilon_D = (D-2)^2 - 4N\varepsilon_D = (D-4)D + 4(1 - N\varepsilon_D),$$

and hence from $D \neq 2$, we get

$$N\varepsilon_D = 1 \quad \text{and} \quad b_D = D - 4.$$

Conversely, $b_D = D - 4$ implies

$$a_D^2 = b_D D + 4N\varepsilon_D = (D-4)D + 4N\varepsilon_D = (D-2)^2 - 4(1 - N\varepsilon_D),$$

and hence from $D \neq 5$, we get

$$N\varepsilon_D = 1 \quad \text{and} \quad a_D = D - 2.$$

We can now provide the following sufficient conditions of the equation $x^2 - Dy^2 = \pm 2$ in terms of such invariants a_D, b_D and m_D :

THEOREM 3. *If* $(a_D, b_D) = (2,0)$ *holds, then we have the following*:

(1) $N\varepsilon_D = 1$,
(2) $m_D \equiv 2 (\mathrm{mod}\ 8)$,
(3) $x^2 - Dy^2 = 2$ *is solvable in integers.*

Proof. We assume $(a_D, b_D) = (2,0)$, i.e.

$$t_D = Dm_D + 2 \quad \text{and} \quad u_D^2 = Dm_D^2 + 4m_D.$$

Then, we can first get

$$4N\varepsilon_D = t_D^2 - Du_D^2 = 4,$$

and hence $N\varepsilon_D = 1$.

Next, we assert $(Dm_D + 4, m_D) = 2$.

If we assume $(Dm_D + 4, m_D) = 1$, then it follows from $u_D^2 = (Dm_D + 4)m_D$ that there exist two positive integers n_1, n_2 such that

$$Dm_D + 4 = n_1^2,\ m_D = n_2^2 \quad \text{with} \quad (n_1, n_2) = 1,\ u_D = n_1 n_2,$$

and hence $n_1^2 - Dn_2^2 = 4$ holds.
However, since $n_1 > 1$, $u_D = n_1 n_2$ is greater than n_2, which contradicts with minimum property of u_D.

If we assume $(Dm_D + 4, m_D) = 4$, then similarly there exist two positive integers n_1, n_2 such that

$$Dm_D + 4 = 4n_1^2,\ m_D = 4n_2^2 \quad \text{with} \quad (n_1, n_2) = 1,\ u_D = 4n_1 n_2,$$

and hence $n_1^2 - Dn_2^2 = 1$ holds. However, $u_D = 4n_1 n_2$ is greater than n_2, which contradicts with minimum property of u_D.
Therefore, we get

$$(Dm_D + 4,\ m_D) = 2,$$

and moreover it follows from $u_D^2 = (Dm_D + 4)m_D$ that there exist two positive integers n_1, n_2 such that

$$Dm_D + 4 = 2n_1^2,\ m_D = 2n_2^2 \quad \text{with} \quad (n_1, n_2) = 1,\ u_D = 2n_1n_2,$$

and hence we get $n_1^2 - Dn_2^2 = 2$.

Furthermore, since $n_2 \equiv 1 \pmod 2$, we get finally

$$m_D = 2n_2^2 \equiv 2 \pmod 8.$$

THEOREM 4. *If* $(a_D, b_D) = (D-2, D-4)$ *holds, then we have the following*:

(1) $N\varepsilon_D = 1$,
(2) $m_D \equiv 1 \pmod 8$,
(3) $x^2 - Dy^2 = -2$ *is solvable in integers.*

Proof. We assume $(a_D, b_D) = (D-2, D-4)$, i.e.

$$t_D = Dm_D + D - 2 \quad \text{and} \quad u_D^2 = Dm_D^2 + 2(D-2)m_D + D - 4$$

Then, we can first get

$$4N\varepsilon_D = t_D^2 - Du_D^2 = 4,$$

and hence we get $N\varepsilon_D = 1$. Moreover, we get immediately

$$u_D^2 = (Dm_D + D - 4)(m_D + 1).$$

Next, we assert $(Dm_D + D - 4,\ m_D + 1) = 2$.

If we assume $(Dm_D + D - 4,\ m_D + 1) = 1$, then it follows from $u_D^2 = (Dm_D + D - 4)(m_D + 1)$ that there exist two positive integers n_1, n_2 such that

$$Dm_D + D - 4 = n_1^2,\ m_D + 1 = n_2^2 \quad \text{with} \quad (n_1, n_2) = 1,\ u_D = n_1n_2,$$

and hence $n_1^2 - Dn_2^2 = -4$ holds, which contradicts with $N\varepsilon_D = 1$.

If we assume $(Dm_D + D - 4,\ m_D + 1) = 4$, then similarly there exist two positive integers n_1, n_2 such that

$$Dm_D + D - 4 = 4n_1^2,\ m_D + 1 = 4n_2^2 \quad \text{with} \quad (n_1, n_2) = 1,\ u_D = 4n_1n_2,$$

and hence $n_1^2 - Dn_2^2 = -1$ holds, which also contradicts with $N\varepsilon_D = 1$.

Therefore, we get

$$(Dm_D + D - 4,\ m_D + 1) = 2.$$

Moreover, it follows from $u_D^2 = (Dm_D + D - 4)(m_D + 1)$ that there exist two positive integers n_1, n_2 such that

$$Dm_D + D - 4 = 2n_1^2,\ m_D + 1 = 2n_2^2 \quad \text{with} \quad (n_1, n_2) = 1,\ u_D = 2n_1 n_2,$$

and hence $n_1^2 - Dn_2^2 = -2$ holds.

Furthermore, since $n_2 \equiv 1 \pmod 2$, we get finally

$$m_D = 2n_2^2 - 1 \equiv 1 \pmod 8.$$

COROLLARY 1. *In the case* $(a_D, b_D) = (2,0)$ (*resp.* $(D-2, D-4)$), *the integral solution* $(x, y) = (n_1, n_2)$ *of the equation* $x^2 - Dy^2 = 2$ (*resp.* $x^2 - Dy^2 = -2$) *induced from the fundamental unit* ε_D of $\mathbf{Q}(\sqrt{D})$ *in the proof of Theorem 3* (*resp.* 4) *is the minimal positive solution.*

Proof. In the case $(a_D, b_D) = (2,0)$, let $(x, y) = (n_1, n_2)$ be the integral solution induced from the fundamental unit ε_D of $\mathbf{Q}(\sqrt{D})$, and $(x, y) = (m_1, m_2)$ be the minimal positive integral solution of the equation $x^2 - Dy^2 = 2$. Then,

$$n_1 \geqq m_1,\ n_2 \geqq m_2 \quad \text{and} \quad u_D = 2n_1 n_2$$

hold, and hence we get immediately

$$u_D \geqq 2m_1 m_2.$$

On the other hand, from the proof of Theorem 1

$$(x, y) = (2m_1^2 - 2,\ 2m_1 m_2)$$

is a positive integral solution of the equation $x^2 - Dy^2 = 4$, and hence we get $u_D \leqq 2m_1 m_2$, by the minimum property of u_D. Therefore, we obtain $u_D = 2m_1 m_2$, which implies $n_1 = m_1$, $n_2 = m_2$.

In the case $(a_D, b_D) = (D-2, D-4)$, we can also prove Corollary 1 in analogous way to the case $(a_D, b_D) = (2,0)$.

COROLLARY 2. *If* $D = q$ *or* $2q$ *for a prime number* q *congruent to* $3 \pmod 4$, *then* $N\varepsilon_D = 1$ *holds.*

Moreover, if $q \equiv -1 \pmod 8$, *then* $a_D = 2$ *holds and* $x^2 - Dy^2 = 2$ *is solvable in integers.*

If $q \equiv 3 \pmod 8$, *then* $a_D = D - 2$ *holds and* $x^2 - Dy^2 = -2$ *is solvable in integers.*

Proof. If we assume $N\varepsilon_D = -1$, then Pell's equation $x^2 - Dy^2 = -4$ is solvable in integers, and so $q \equiv 1 \pmod 4$ holds for any prime factor q of D which contradicts with $q \equiv 3 \pmod 4$. Hence $N\varepsilon_D = 1$ holds.

Next, since $t_D = Dm_D + a_D$, $N\varepsilon_D = 1$ implies

$$Du^2 = t_D^2 - 4 = m_D(Dm_D + 2a_D)D + (a_D^2 - 4),$$

and hence

$$(a_D - 2)(a_D + 2) = a_D^2 - 4 \equiv 0 \pmod D.$$

Therefore, in the case $D = q$,

$$a_D \equiv 2 \text{ or } -2 \pmod D,$$

and hence

$$a_D = 2 \text{ or } D - 2.$$

In the case $D = 2q$, $t_D \equiv 0 \pmod 2$ implies $a_D \equiv 0 \pmod 2$, and so

$$a_D - 2 \equiv a_D + 2 \equiv 0, \quad \text{i.e.} \quad a_D \equiv \pm 2 \pmod 2.$$

On the other hand, $a_D \equiv 2$ or $-2 \pmod q$ holds, and so we get

$$a_D \equiv 2 \text{ or } -2 \pmod D,$$

which implies directly

$$a_D = 2 \text{ or } D - 2.$$

Consequently, Corollary 2 is follows from Propositions 2,3 and Theorems 3.4.

With regard to insolubility of $x^2 - Dy^2 = \pm 2$, we obtain easily the following:

COROLLARY 3. *If we assume*

$$D = p \quad \textit{for a prime } p \textit{ congruent to } 1 \bmod 4,$$

or

$$D = 2p \quad \textit{for a prime } p \textit{ congruent to } 5 \bmod 8,$$

then

$$N\varepsilon_D = -1$$

holds and

$$x^2 - Dy^2 = \pm 2$$

is insoluble.

Proof. If $D = p$ $(p \equiv 1 \mod 4)$, or $D = 2p$ $(p \equiv 5 \mod 8)$, then we get $N\varepsilon_D = -1$ (cf. for instance [2]).

Hence by Proposition 2 $x^2 - Dy^2 = \pm 2$ is insoluble.

$$(a_D, b_D) = (2,0)$$

$t_D = Dm_D + a_D$

${u_D}^2 = D{m_D}^2 + 2a_Dm_D + b_D$

${a_D}^2 - 4 = b_DD$

$n_1 = \sqrt{D \cdot m_D/2 + 2}$

$n_2 = \sqrt{m_D/2}$

$t_D = Dm_D + 2$

$u_D = 2n_1 \cdot n_2$

$$m_D = [t_D/D] = 2{n_2}^2 \equiv 2 \pmod 8 \qquad {n_1}^2 - D{n_2}^2 \equiv 2$$

D	type	h_D	r	m_D	n_1	n_2
7	q	1	-2	2	3	1
14	$2q$	1	-2	2	4	1
23	q	1	-2	2	5	1
31	q	1		98	39	7
34	$2p$	2	-2	2	6	1
46	$2q$	1		1058	156	23
47	q	1	-2	2	7	1
62	$2q$	1	-2	2	8	1
71	q	1		98	59	7
79	q	3	-2	2	9	1
94	$2q$	1		45602	1464	151
103	q	1		4418	477	47
119	pq	2	-2	2	11	1
127	q	1		74498	2175	193
142	$2q$	3	-2	2	12	1
151	q	1		22889378	41571	3383
158	$2q$	1		98	88	7
167	q	1	-2	2	13	1

D	type	h_D	r	m_D	n_1	n_2
191	q	1		94178	2999	217
194	$2p$	2	-2	2	14	1
199	q	1		163479362	127539	9041
206	$2q$	1		578	244	17
223	q	3	-2	2	15	1
238	$2pq$	2		98	108	7
239	q	1		51842	2489	161
254	$2q$	3	-2	2	16	1
263	q	1		1058	373	23
287	pq	2	-2	2	17	1
302	$2q$	1		28322	2068	119
311	q	1		108578	4109	233
322	$2q_1q_2$	4	-2	2	18	1
359	q	3	-2	2	19	1
383	q	1		98	137	7
386	$2p$	2		578	334	17
391	pq	2		37538	2709	137
398	$2q$	1	-2	2	20	1
431	q	1		703298	12311	593
439	q	5	-2	2	21	1
446	$2q$	1		494018	10496	497
479	q	1		12482	1729	79
482	$2p$	2	-2	2	22	1

Prime p is congruent to 1 mod 8 ; $p \equiv 1 \pmod 8$.
Prime q is congruent to -1 mod 8 ; $q \equiv -1 \pmod 8$.
$h_D = -n$ means that $N\varepsilon_D = -1$ and $h_D = n$.
r represents the integer such that $D = k^2 + r$, $-k < r \leqq k$ and $4k \equiv 0 \pmod r$ for real quadratic field $\mathbf{Q}(\sqrt{D})$ of **R-D** type.

$$(a_D,\ b_D) = (D-2,\ D-4)$$

$t_D = Dm_D + a_D$

${u_D}^2 = D{m_D}^2 + 2a_Dm_D + b_D$

${a_D}^2 - 4 = b_DD$

$n_1 = \sqrt{D(m_D+1)/2-2}$

$n_2 = \sqrt{(m_D+1)/2}$

$t_D = D(m_D+1) - 2$

$u_D = 2n_1 \cdot n_2$

$$m_D = [t_D/D] = 2{n_2}^2 - 1 \equiv 1 \pmod 8 \qquad {n_1}^2 - D{n_2}^2 = -2$$

D	type	h_D	r	m_D	n_1	n_2
2	2	-1	-2	1		1
3	q	1	-2	1	1	1
6	$2q$	1	2	1	2	1
11	q	1	2	1	3	1
19	q	1		17	13	3
22	$2q$	1		17	14	3
38	$2q$	1	2	1	6	1
43	q	1		161	59	9
51	pq	2	2	1	7	1
59	q	1		17	23	3
66	$2q_1q_2$	2	2	1	8	1
67	q	1		1457	221	27
83	$2q$	1	2	1	9	1
86	$2q$	1		241	102	11
102	$2pq$	2	2	1	10	1
107	q	1		17	31	3
114	$2q_1q_2$	2		17	32	3
118	$2q$	1		5201	554	51
123	pq	1		1	11	1
131	q	1		161	103	9
134	$2q$	1		2177	382	33
139	q	1		1116017	8807	747
146	$2p$	2	2	1	12	1
163	q	1		786257	8005	627
178	$2p$	2		17	40	3
179	q	1		46817	2047	153
187	pq	2		17	41	3
211	q	1				

D	type	h_D	r	m_D	n_1	n_2
214	$2q$	1				
227	q	1	2	1	15	1
246	$2pq$	2		721	298	19
251	q	1		29281	1917	121
258	$2pq$	2		1	16	1
262	$2q$	1		801377	10246	633
267	pq	2		17	49	3
278	$2q$	1		17	50	3
283	q	1		977201	11759	699
291	pq	4	2	1	17	1
307	q	1		576737	9409	537
326	$2q$	3		1	18	1
339	pq	2		577	313	17
347	q	1		3697	801	43
354	$2q_1q_2$	2		1457	508	27
358	$2q$	1				
374	$2pq$	2		17	58	3
402	$2q_1q_2$	2		1	20	1
411	pq	2		241	223	11
418	$2q_1q_2$	2		161	184	9
419	q	1		1289617	16437	803
422	$2q$	1		33281	2650	129
443	q	3	2	1	21	1
451	pq	2		206081	6817	321
454	$2q$	1				
467	q	1		6961	1275	59
498	$2q_1q_2$	2		721	424	19
499	q	5		17	67	3

Prime p is congruent to 1 mod 8 ; $p \equiv 1 \pmod 8$)
Prime q is congruent to 3 mod 8 ; $q \equiv 3 \pmod 8$.

REFERENCES

[1] O. Perron, Die Lehre von den Kettenbruchen, Chelsea Publ. Comp., 1929.
[2] T. Takagi, Syoto-sesuron-kogi (Japanese), Kyoritu Publ. Comp., 1953.
[3] H. Yokoi, Some relations among new invariants of prime number p congruent to 1 mod 4, Advances in Pure Math.,**13** (1988), 493–501.

[4] ——, The fundamental unit and bounds for class numbers of real quadratic fields, Nagoya Math. J., **124** (1991), 181–197.

[5] ——, New invariants and class number problem in quadratic fields, Nagoya Math. J., **132** (1993), 175–197.

Graduate School of Human Informatics
Nagoya University
Chikusa-ku, Nagoya 464-01
Japan