F. Halter-Koch
Nagoya Math. J.
Vol. 123 (1991), 141-151

ON A CLASS OF INSOLUBLE BINARY QUADRATIC DIOPHANTINE EQUATIONS

FRANZ HALTER-KOCH

§ 0. Introduction

The binary quadratic diophantine equation

$$|x^2 - ny^2| = t$$

is of interest in the class number problem for real quadratic number fields and was studied in recent years by several authors (see [4], [5], [2] and the literature cited there).

To be precise, for a positive square-free integer n, we set

$$\sigma_n = \begin{cases} 1, & \text{if } n \not\equiv 1 \bmod 4, \\ 2, & \text{if } n \equiv 1 \bmod 4; \end{cases}$$

a solution $(x, y) \in \mathbf{Z}$ of the diophantine equation

$$|x^2 - ny^2| = \sigma_n^2 t$$

is called *primitive*, if $(x, y) | \sigma_n$, where (x, y) denotes the g.c.d. of x and y. The reason for this terminology will become clear from the theory of quadratic orders, to be explained in § 1.

R. A. Mollin [4] proved, generalizing previous results by Yokoi [5] and others, the following criterion.

PROPOSITION 0. *Let s, t, r be integers such that $n = (st)^2 + r > 5$ is squarefree and the following conditions are satisfied:*

(1) $s \geq 1$, $t \geq 2$ *and* $(t, r) = 1$;
(2) $r | 4s$, *and* $-st < r \leq st$;
(3) *If* $n \equiv 1 \bmod 4$, *then* $|r| \in \{1, 4\}$.
(4) *If* $|r| = 4$, *then* $s \geq 2$.
(5) *If* $r = 1$, *then* $s \geq 3$ *and* $2 | st$.

Then the diophantine equation $|x^2 - ny^2| = \sigma_n^2 t$ *has a primitive solution if*

Received November 13, 1990.

and only if $n = 7$, $t = 3$.

Actually, the result as given in [4], is formally stronger than Proposition 0; there it is asserted, that the diophantine equation has no non-trivial solutions (in a sense precised there). To obtain Mollin's result, we must apply Proposition 0 for all $t' > 1$ such that $t = t'u^2$ for some $u \in \mathbf{N}$.

In [2], we derived a general method to handle such equations using continued fractions, and we claimed [2, p. 92] that an application of these techniques would lead to a simple proof and a generalization of Proposition 0. J. B. Leicht (Heidelberg) pointed out to me that this is not quite correct: The techniques of [2] do only work if $\sigma_n t < \sqrt{n}$, and there are two cases of Proposition 0 in which this condition is violated:

$$s = 1, \quad r = -1, \quad n = t^2 - 1;$$
$$s = 1, \quad r = -2, \quad n = t^2 - 2.$$

In this paper, we develop different techniques which, among others, also cover these cases. We consider the diophantine equation as a norm equation, and then the ideal theory of quadratic orders becomes available for the problem (§ 1). In § 2 we prove a criterion for certain ideals to be reduced (Theorem 1) and a general reduction statement (Theorem 2). In § 3 we reformulate these Theorems for diophantine equations. Finally, in § 4, we give some applications for discriminants of Richaud-Degert-type; thereby we restrict ourselves to those cases, which cannot be settled with the methods of [2].

§ 1. Preliminaries on quadratic orders

In this section we recall some well-known facts about quadratic orders and formulate them in a manner which will be useful later on; for proofs see [1] or [3] (but note that the notions of [3] are slightly different from ours).

A positive integer D is called a *discriminant*, if D is not a square and $D \equiv 0$ or $1 \bmod 4$; in this paper, D always denotes a discriminant. We set

$$\omega_D = \begin{cases} \dfrac{1}{2}\sqrt{D}\,, & \text{if } D \equiv 0 \bmod 4\,, \\[2ex] \dfrac{1}{2}(1 + \sqrt{D})\,, & \text{if } D \equiv 1 \bmod 4\,, \end{cases}$$

and

$$\mathscr{R}_D = \mathbf{Z} \oplus \mathbf{Z}\omega_D .$$

$\mathscr{R}_D$ is an order in the quadratic number field $\mathbf{Q}(\sqrt{D})$. If D_0 is the discriminant of $\mathbf{Q}(\sqrt{D})$, then

$$D = D_0 f_D^2$$

for some $f_D \in \mathbf{N}$; f_D is called the *conductor* associated with D.

Every $\xi \in \mathscr{R}_D$ has a unique representation in the form

$$\xi = \frac{b + e\sqrt{D}}{2},$$

where $b, e \in \mathbf{Z}$ and $b \equiv eD \bmod 2$; we call

$$\mathscr{N}(\xi) = \frac{b^2 - e^2 D}{4} \in \mathbf{Z}$$

the *norm* of ξ. An element $\xi \in \mathscr{R}_D$ is called *primitive*, if $m^{-1}\xi \notin \mathscr{R}_D$ for all integers $m \geq 2$. Obviously, $\xi \in \mathscr{R}_D$ is primitive if and only if either

$$D \equiv 0 \bmod 4, \quad \xi = x + y\sqrt{\frac{D}{4}}, \quad x, y \in \mathbf{Z}, \quad (x, y) = 1$$

or

$$D \equiv 1 \bmod 4, \quad \xi = \frac{x + y\sqrt{D}}{2}, \quad x, y \in \mathbf{Z}, \quad x \equiv y \bmod 2, \ (x, y) \mid 2 .$$

For an ideal $(0) \neq J \lhd \mathscr{R}_D$ we call

$$\mathscr{N}(J) = (\mathscr{R}_D : J) \in \mathbf{N}$$

the *norm* of J; J is called *primitive*, if $m^{-1}J \not\subset \mathscr{R}_D$ for all integers $m \geq 2$. If $J = \xi\mathscr{R}_D$ is a principal ideal, then $\mathscr{N}(J) = |\mathscr{N}(\xi)|$, and J is primitive if and only if ξ is primitive. Let $\Omega(D)$ be the set of all norms of primitive principal ideals of $\mathscr{R}_D$. Using this terminology, we rephrase the question about the solubility of the diophantine equations under consideration as follows.

PROPOSITION 1. *If D is a discriminant and t is a positive integer, then the following two assertions are equivalent*:

a) $t \in \Omega(D)$

b) *The diophantine equation*

$$\begin{cases} \left| x^2 - \dfrac{D}{4} y^2 \right| = t\,, & \text{if } D \equiv 0 \bmod 4\,, \\ |x^2 - Dy^2| = 4t\,, & \text{if } D \equiv 1 \bmod 4 \end{cases}$$

has a solution $(x, y) \in \mathbf{Z}^2$ *satisfying*

$$\begin{cases} (x, y) = 1\,, & \text{if } D \equiv 0 \bmod 4\,, \\ (x, y) \mid 2\,, & \text{if } D \equiv 1 \bmod 4\,. \end{cases}$$

An ideal $(0) \neq J \triangleleft \mathscr{R}_D$ is called *regular*, if $\mathscr{R}_D = \{x \in \mathbf{Q}(\sqrt{D}) \mid xJ \subset J\}$. Any regular ideal is invertible. Any principal ideal and any ideal J of $\mathscr{R}_D$ such that $(\mathscr{N}(J), f_D) = 1$ is regular. In this paper we shall mainly be concerned with ideals J such that $(\mathscr{N}(J), f_D) = 1$.

The primitive ideals of $\mathscr{R}_D$ are precisely the $\mathbf{Z}$-modules of the form

$$J = \mathbf{Z}a \oplus \mathbf{Z}\frac{b + \sqrt{D}}{2}$$

where $a, b \in \mathbf{Z}$, $a > 0$ and $4a \mid b^2 - D$. In this representation, $a = \mathscr{N}(J)$ is uniquely determined by J, while b is only determined modulo $2a$. If J is as above, then J is regular if and only if $(a, b, (b^2 - D)/4a) = 1$.

For lack of a suitable reference, we give a proof of the following simple result concerning ideals whose norm divides the discriminant.

LEMMA 1. *Let D be a discriminant and r a positive integer such that $r \mid D$ and $4 \nmid r$. Then there exists exactly one primitive ideal $J \triangleleft \mathscr{R}_D$ such that $\mathscr{N}(J) = r$.*

Proof. Since $4 \nmid r$, we have either $4r \mid D$ or $4r \mid r^2 - D$, and we set

$$J = \begin{cases} \mathbf{Z}r \oplus \mathbf{Z}\dfrac{\sqrt{D}}{2}\,, & \text{if } 4r \mid D\,, \\[2ex] \mathbf{Z}r \oplus \mathbf{Z}\dfrac{r + \sqrt{D}}{2}\,, & \text{if } 4r \nmid D\,. \end{cases}$$

Then J is a primitive ideal of $\mathscr{R}_D$, and $\mathscr{N}(J) = r$.

If $I = \mathbf{Z}r \oplus \mathbf{Z}(b + \sqrt{D})/2$ is a primitive ideal of $\mathscr{R}_D$, where $0 \leq b < 2r$, $4r \mid b^2 - D$, then $r \mid D$ implies $r \mid b$ and therefore $b = 0$ or $b = r$. If there were two primitive ideals in $\mathscr{R}_D$ with norm r, then $I_1 = \mathbf{Z}r \oplus \mathbf{Z}(\sqrt{D}/2)$ and $I_2 = \mathbf{Z}r \oplus \mathbf{Z}(r + \sqrt{D})/2$ both were ideals, whence $4r \mid D$ and $4r \mid r^2 - D$; this implies $4r \mid r^2$ and hence $4 \mid r$, contradicting the assumption that r is square-free. $\square$

https://doi.org/10.1017/S002776300000369X Published online by Cambridge University Press

An ideal $(0) \neq J \lhd \mathscr{R}_D$ is called *reduced*, if it is primitive, regular, and has a representation of the form

$$J = \mathbf{Z}a \oplus \mathbf{Z}\frac{b + \sqrt{D}}{2}$$

such that

$$0 < \sqrt{D} - b < 2a < \sqrt{D} + b\,;$$

note that these conditions also determine b uniquely. If J is a reduced ideal of $\mathscr{R}_D$, then $\mathscr{N}(J) < \sqrt{D}$. If J is a primitive regular ideal of $\mathscr{R}_D$ and $\mathscr{N}(J) < \frac{1}{2}\sqrt{D}$, then J is reduced.

Two ideals $J_1, J_2 \lhd \mathscr{R}_D$ are called *equivalent*, if there exist elements $\beta_1, \beta_2 \in \mathscr{R}_D \backslash \{0\}$ such that $\beta_1 J_1 = \beta_2 J_2$.

If $J = \mathbf{Z}a \oplus \mathbf{Z}(b + \sqrt{D})/2$ is a primitive ideal of $\mathscr{R}_D$ ($a, b \in \mathbf{Z}$, $a > 0$, $4a \mid b^2 - D$), then its *Lagrange neighbour* J^+ is defined by

$$J^+ = \mathbf{Z}a^+ \oplus \mathbf{Z}\frac{b^+ + \sqrt{D}}{2}\,,$$

where

$$b^+ = -b + 2a\left[\frac{b + \sqrt{D}}{2a}\right] \quad \text{and} \quad a^+ = \frac{D - b^{+2}}{4a}\,.$$

J^+ is an ideal of $\mathscr{R}_D$, equivalent to J, and if J is regular (reduced), then J^+ is also regular (reduced). Let $(J_n)_{n\geq 0}$ be defined by $J_0 = J$ and $J_{n+1} = J_n^+$. The sequence $(J_n)_{n\geq 0}$ becomes ultimately periodic, and if J is regular, it contains all reduced ideals equivalent to J. The sequence $(J_n)_{n\geq 0}$ can be calculated by means of the continued fraction algorithm as follows: If

$$\xi = \frac{b + \sqrt{D}}{2a} = [b_0, b_1, b_2, \cdots]$$

is the simple continued fraction expansion of ξ and, for $\nu \geq 0$,

$$\xi_\nu = [b_\nu, b_{\nu+1}, \cdots] = \frac{P_\nu + \sqrt{D}}{2Q_\nu}\,,$$

where $P_\nu \in \mathbf{Z}$ and $Q_\nu \in \mathbf{N}$, then

$$J_\nu = \mathbf{Z}Q_\nu \oplus \mathbf{Z}\frac{P_\nu + \sqrt{D}}{2}\,.$$

The case $J_0 = \mathscr{R}_D$ is of particular interest: If

$$\omega_D = [b_0, \overline{b_1, \cdots, b_l}]\,,$$

l is the length of a primitive period and if, for $\nu \in \{1, \cdots, l\}$,

$$\xi_\nu = [\overline{b_\nu, b_{\nu+1}, \cdots, b_l, b_1, \cdots, b_{\nu-1}}] = \frac{P_\nu + \sqrt{D}}{2Q_\nu}\,,$$

then the set

$$\Omega^*(D) = \{Q_1, \cdots, Q_l\}$$

is precisely the set of norms of reduced principal ideals of $\mathscr{R}_D$.

§ 2. Reduced ideals

THEOREM 1. *Let $D = 4t^2 + m$ be a discriminant, where t and m are integers such that $t > 0$, $4t \nmid m$ and either*

$$m \geq -4t + 2$$

or

$$m \geq -8t + 5\,, \qquad m \not\equiv 1 \bmod 4t\,.$$

Then any primitive regular ideal J of $\mathscr{R}_D$ with $\mathscr{N}(J) = t$ is reduced.

Proof. If $m > 0$, then $t < \frac{1}{2}\sqrt{D}$, and therefore any primitive regular ideal of $\mathscr{R}_D$ with norm t is reduced.

Thus we may suppose that $m < 0$. Let $J \lhd \mathscr{R}_D$ be a primitive regular ideal with $\mathscr{N}(J) = t$, and set

$$J = \mathbf{Z}t \oplus \mathbf{Z}\frac{x + \sqrt{D}}{2}\,,$$

where $1 \leq x \leq 2t$ and $x^2 \equiv D \equiv m \bmod 4t$. Since $4t \nmid m$, we have $x < 2t$, and we must prove that

$$0 < \sqrt{D} - x < 2t < \sqrt{D} + x\,,$$

i.e.,

$$x^2 < D < (2t + x)^2 \quad \text{and} \quad (2t - x)^2 < D\,.$$

Since $m < 0$, we always have $D < 4t^2 < (2t + x)^2$. If $m \geq -4t + 2$, then $x^2 \leq (2t - 1)^2$, $(2t - x)^2 \leq (2t - 1)^2$, and $(2t - 1)^2 < 4t^2 + m = D$.

If $m \not\equiv 1 \bmod 4t$ and $m \geq -8t + 5$, then $2 \leq x \leq 2t - 2$, $x^2 \leq (2t - 2)^2$, $(2t - x)^2 \leq (2t - 2)^2$ and $(2t - 2)^2 < 4t^2 + m = D$. □

THEOREM 2. *Let $D = t^2 + m$ be a discriminant, where $t > 1$ and m are integers such that either*

$$-2t + 1 < m < 2t + 1$$

or

$$-4t + 4 < m < 4t + 4, \qquad m \not\equiv 1 \bmod t.$$

Let $J \lhd \mathscr{R}_D$ be a primitive regular ideal such that $\mathscr{N}(J) = t$, let J^+ be the Lagrange neighbour of J, and $Q = \mathscr{N}(J^+)$.

Then $Q < \frac{1}{2}\sqrt{D}$, and $D - 4tQ \in \mathbf{Z}$ is a perfect square. In particular, J^+ is reduced.

Proof. Suppose that $J = \mathbf{Z}t \oplus \mathbf{Z}(y + \sqrt{D})/2$ where $y \in \mathbf{Z}$, $y^2 \equiv D \bmod 4t$ and $t < y \leq 3t$; we consider first the case $m \neq 4t$. Then we have $y \neq 3t$ and therefore $t + 1 \leq y \leq 3t - 1$. Moreover, if $m \not\equiv 1 \bmod t$, then $y^2 \not\equiv 1 \bmod t$, and therefore $t + 2 \leq y \leq 3t - 2$. Since

$$t - 1 < \sqrt{D} < t + 1, \qquad \text{if } -2t + 1 < m < 2t + 1,$$
$$t - 2 < \sqrt{D} < t + 2, \qquad \text{if } -4t + 4 < m < 4t + 4,$$

we obtain in any case

$$1 < \frac{y + \sqrt{D}}{2t} < 2$$

and therefore

$$J^+ = \mathbf{Z}Q \oplus \mathbf{Z}\frac{P + \sqrt{D}}{2},$$

where $P = 2t - y$ and $Q = (D - P^2)/4t$. We set $y^2 = D + 4tz$, where $z \in \mathbf{Z}$, and obtain

$$Q = y - t - z.$$

If $m = 4t$, then $y = 3t$ and $J^+ = \mathscr{R}_D$, so that in this case $Q = 1$, $z = 2t - 1$ and again

$$Q = y - t - z.$$

In any case we obtain

$$y^2 = D + 4t(y - t - Q) = 4ty + D - 4t^2 - 4tQ,$$

and therefore

$$y = 2t \pm \sqrt{D - 4tQ},$$

whence $D - 4tQ$ must be a perfect square.

Suppose that $Q > \frac{1}{2}\sqrt{D}$; then we obtain

$$z = y - t - Q < y - t - \frac{1}{2}\sqrt{D},$$

and therefore

$$y^2 = D + 4tz < t^2 + m + 4ty - 4t^2 - 2t\sqrt{D},$$

whence

$$y^2 - 4ty + (3t^2 + 2t\sqrt{D} - m) < 0.$$

This however can only occur when

$$(2t)^2 - (3t^2 + 2t\sqrt{D} - m) = t^2 - 2t\sqrt{D} + m > 0,$$

i.e., when $2t\sqrt{D} < t^2 + m$. Squaring this inequality gives

$$4t^2D = 4t^4 + 4t^2m < t^4 + 2t^2m + m^2,$$

and therefore

$$0 > 3t^4 + 2t^2m - m^2 = (3t^2 - m)(t^2 + m),$$

contradicting our assumptions on m and t. □

§ 3. Diophantine equations

In this section we reformulate Theorems 1 and 2 for diophantine equations. We do this using the set $\Omega(D)$; the final translation into the language of diophantine equations is given by Proposition 1.

THEOREM 1A. *Let $D = 4t^2 + m$ be a discriminant as in Theorem 1, and suppose that $(t, f_D) = 1$. Then we have $t \in \Omega(D)$ if and only if $t \in \Omega^*(D)$.*

Proof. Since $(t, f_D) = 1$, any ideal J of $\mathscr{R}_D$ satisfying $\mathscr{N}(J) = t$ is regular. Therefore the assertion follows from Theorem 1. □

THEOREM 2A. *Let $D = t^2 + m$ be a discriminant as in Theorem 2, and suppose that $(t, f_D) = 1$.*

i) *If $t \in \Omega(D)$, then there exists some $Q \in \Omega^*(D)$ such that $Q < \frac{1}{2}\sqrt{D}$, and the integer $D - 4tQ$ is a perfect square.*

https://doi.org/10.1017/S002776300000369X Published online by Cambridge University Press

ii) *If* $Q \in \Omega(D)$ *is such that the integer* $D - 4tQ$ *is a perfect square and all primitive ideals* $J \lhd \mathscr{R}_D$ *with* $\mathscr{N}(J) = Q$ *are principal ideals, then* $t \in \Omega(D)$.

iii) *If* $D - 4t$ *is a perfect square, then* $t \in \Omega(D)$.

Proof. i) Let $J \lhd \mathscr{R}_D$ be a primitive principal ideal such that $\mathscr{N}(J) = t$; since $(t, f_D) = 1$, J is regular. By Theorem 2, $Q = \mathscr{N}(J^+) < \frac{1}{2}\sqrt{D}$, and $D - 4tQ$ is a perfect square.

ii) If $D - 4tQ = P^2$ for some $P \in \mathbf{N}$, then the primitive ideals $J_1 = \mathbf{Z}Q \oplus \mathbf{Z}(P + \sqrt{D})/2$ and $J_2 = \mathbf{Z}t \oplus \mathbf{Z}(-P + \sqrt{D})/2$ are equivalent by [3, Cor. 2]. By assumption, J_1 is principal, whence J_2 is principal, too, and therefore $t \in \Omega(D)$.

iii) follows from ii) with $Q = 1$. □

§ 4. Discriminants of Richaud-Degert-type

PROPOSITION 2. *Let* $D = 4a^2 + r$ *be a discriminant, where* a *and* r *are integers such that* $1 \leq |r| < a$, $r \mid a$, r *is square-free and* $r \equiv 1 \bmod 4$.

i) *If* $r \neq 1$, *then* $a \notin \Omega(D)$.

ii) $2a \in \Omega(D)$ *if and only if either* $4a^2 - 8a + r$ *or* $4a^2 - 8a|r| + r$ *is a perfect square.*

iii) $2a \in \Omega(4a^2 + 1)$ *if and only if* $a = 2$.

Proof. Since r is square-free, $(r, f_D) = 1$. From [2] we obtain $\Omega^*(D) = \{1, r, a \pm (r-1)/4\}$ if $r > 0$, and $\Omega^*(D) = \{1, |r|, a + (r-1)/4\}$ if $r < 0$.

i) follows from Theorem 1A with $t = a$, $m = r$.

ii) We apply Theorem 2A with $t = 2a$, $m = r$. If $2a \in \Omega(D)$, then $D - 4tQ$ is a perfect square for one of the numbers $Q = 1, |r|, a \pm (r-1)/4$. If $Q = a \pm (r-1)/4$, then $D - 4tQ < 0$, and therefore it cannot be a perfect square. If $Q = |r|$, then $D - 4tQ = 4a^2 - 8a|r| + r$, and if $Q = 1$, then $D - 4tQ = 4a^2 - 8a + r$.

For tbe converse suppose that, for $Q = 1$ or $Q = |r|$, $D - 4tQ$ is a perfect square. By Lemma 1, there eixsts exactly one primitive ideal J of $\mathscr{R}_D$ such that $\mathscr{N}(J) = Q$, and since $\{1, |r|\} \subset \Omega^*(D)$, J is principal. Now the assertion follow from Theorem 2A, ii).

iii) By ii), $2a \in \Omega(4a^2 + 1)$ if and only if $4a^2 - 8a + 1 = (2a - 2)^2 - 3$ is a perfect square, which is equivalent with $a = 2$. □

PROPOSITION 3. *Let* $D = a^2 + 4r$ *be a discriminant, where* a *and* r *are integers such that* $a \equiv 1 \bmod 2$, $a > 1$, $r \mid a$, $r \neq -a$, *and* r *is square-free.*

i) *$a \in \Omega(D)$ if and only if either $a^2 - 4a + 4r$ or $a^2 - 4a|r| + 4r$ is a perfect square.*

ii) *$a \in \Omega(a^2 - 4)$ if and only if $a = 5$.*

Proof. From $-a = \mathcal{N}(\frac{1}{2}(a + \sqrt{a^2 + 4a}))$ we obtain $a \in \Omega(a^2 + 4a)$, and therefore we may suppose that $|r| < a$, and consequently $|r| \leq a/3$. Since r is square-free, $(r, f_D) = 1$. From [2] we obtain $\Omega^*(D) = \{1, r\}$ if $r > 0$, and $\Omega^*(D) = \{1, |r|, a + r - 1\}$ if $r < 0$.

We apply Theorem 2A with $t = a$, $m = 4r$. If $a \in \Omega(D)$, then $D - 4tQ$ is a perfect square for one of the numbers $Q = 1, |r|, a + r - 1$. If $Q = a + r - 1$, then $D - 4tQ = -a(3a + 4r) + 4(a + r) < 0$ cannot be a perfect square. If $Q = |r|$, then $D - 4tQ = a^2 - 4a|r| + 4r$, and if $Q = 1$, then $D - 4tQ = a^2 - 4a + 4r$.

The converse is proved exactly as in Proposition 2.

ii) follows from i) with $r = -1$, observing that $a^2 - 4a - 4 = (a - 1)^2 - 8$ is a perfect square if and only if $a = 5$. □

PROPOSITION 4. *Let $D = 4(a^2 + r)$ be a discriminant, where a and r are integers such that $a \geq 3$, $r | 2a$, $r > -a$, and r is square-free.*

i) *Suppose that either $2 \nmid a$ or $a^2 + r$ is not a discriminant. Then $a \in \Omega(D)$ if and only if $a = r$.*

ii) *Suppose that $a^2 + r$ is not a discriminant. Then $2a \in \Omega(D)$ if and only if either $a^2 - 2a + r$ or $a^2 - 2a|r| + r$ is a perfect square. In particular:*

If $r = 1$, then $2a \in \Omega(D)$;

if $r \in \{-1, 2\}$, then $2a \notin \Omega(D)$;

if $r = -2$, then $2a \in \Omega(D)$ if and only if $a = 3$.

Proof. From [2] we obtain $\Omega^*(D) = \{1, r\}$, if $r > 0$, and $\Omega^*(D) = \{1, 2a + r - 1, |r|\}$, if $r < 0$. Since r is square-free, no odd prime divides (a, f_D). Since $2 | f_D$ if and only if $a^2 + r$ is a discriminant, we obtain $(a, f_D) = 1$ in i) and $(2a, f_D) = 1$ in ii).

Now we proceed as in the proof of Proposition 2: We infer i) from Theorem 1A with $t = a$, $m = 4r$, and ii) from Theorem 2A with $t = 2a$, $m = 4r$. □

§ 5. An application

We finish with an amusing application of the preceding theory, part of which was posed as a problem (cf. Bulletin dell' Association des

Professeurs de Mathématiques no. 374, 1990, Problem no. 177).

PROPOSITION 5. *If x and y are positive integers such that, for some choice of the sign,*

$$c = \frac{x^2 + y^2}{xy \pm 1}$$

is an integer, then c is either a perfect square, or $c = 5$.

Proof. We suppose that $c = (x^2 + y^2)/(xy \pm 1)$ is an integer and not a perfect square; since $c = 2$ implies $(x - y)^2 = \pm 2$, we obtain $c > 2$. Dividing by (x, y), we obtain an equation

$$u^2 - cuv + v^2 = \pm c_0,$$

where $u, v \in \mathbf{Z}$, $(u, v) = 1$, $c_0 > 1$ and $c = c_0 q^2$ for some $q \in \mathbf{N}$. If $D = c^2 - 4$, then D is a discriminant, and

$$\pm c_0 = \mathcal{N}\left(\frac{2u - cv + v\sqrt{D}}{2}\right),$$

whence $c_0 \in \Omega(D)$. If $4 | c_0$, then we obtain $u^2 + v^2 \equiv 0 \bmod 4$, contradicting $(u, v) = 1$; therefore we have $4 \nmid c_0$ and thus $(c_0, f_D) = 1$.

If $c_0 \neq c$, then $c_0 \leq c/4 < \frac{1}{2}\sqrt{D}$ and therefore $c_0 \in \Omega^*(D)$. By [2], we have $\Omega^*(D) = \{1, c - 2\}$ and therefore $c_0 = 1$, a contradiction.

If $c_0 = c$ is odd, then Proposition 3, ii) implies $c = 5$. If $c_0 = c$ is even, then $c \equiv 2 \bmod 4$, since $4 \nmid c_0$, and therefore $u^2 - cuv + v^2 \equiv (u - v)^2 \equiv 2 \bmod 4$, a contradiction. □

REFERENCES

[1] P. G. L. Dirichlet, Vorlesungen über Zahlentheorie, Braunschweig 1893, Chelsea Reprint 1968.

[2] F. Halter-Koch, Quadratische Ordnungen mit großer Klassenzahl, J. Number Theory, **34** (1990), 82–94.

[3] P. Kaplan, K. S. Williams, The distance between ideals in the orders of a real quadratic field, L'Enseig. Math., **36** (1990), 321–358.

[4] R. A. Mollin, On the insolubility of a class of Diophantine equations and the non-triviality of the class numbers of related real quadratic fields of Richaud-Degert-type, Nagoya Math. J., **105** (1987), 39–47.

[5] H. Yokoi, On the diophantine equation $x^2 - py^2 = \pm 4q$ and the class number of real subfields of a cyclotomic field, Nagoya Math. J., **91** (1983), 151–161.

Institut für Mathematik
Karl-Franzens-Universität
Halbärthgasse 1/I
A-8010 Graz, Österreich