



**CHARACTERIZATION OF  $D = P^2 + Q^2$  WHEN  
 $\gcd(P, Q) = 1$  AND  $x^2 - Dy^2 = -1$  HAS NO INTEGER  
SOLUTIONS**

**R. A. MOLLIN**

Department of Mathematics and Statistics  
University of Calgary  
Calgary, Alberta, Canada, T2N 1N4  
e-mail: ramollin@math.ucalgary.ca

**Abstract**

We settle the open problem of characterizing those nonsquare integers  $D > 1$  which are a sum of two relatively prime squares when  $x^2 - Dy^2 = -1$  has no solution in integers  $x, y$ .

**1. Introduction**

In the recent paper [5], interesting in its own right, it is stated at the end of the paper: “An apparently open problem is to characterize those  $D$  that are a sum of two relatively prime squares but for which  $x^2 - Dy^2$  does not represent  $-1$ . Such  $D$  include 34, 146, 178, 194, 205, 221, 305, 377, 386 and 410.” It is the purpose of this work to provide that characterization. We do so in terms of ambiguous classes of forms related to that of ideals in quadratic orders.

It should be noted that this is a necessary and sufficient condition for the problem cited in the abstract, but we have not addressed and have no

2000 Mathematics Subject Classification: **Please provide.**

Keywords and phrases: Pell’s equation, sums of two squares, quadratic fields, cycles of ideals, ambiguous ideals.

Received November 27, 2008

input into the computational problem of *efficiently* deciding whether  $x^2 - Dy^2 = -1$  is solvable. We consider this to be a computational complexity issue in which we have no interest herein. Our solution involves the purely mathematical issues involving the intimate connection between the topics of binary quadratic forms, classes of ideals, and the ambiguous classes in both. This has, as a nice feature, an explanation of the distinction between the wide and narrow ideal class groups, when they differ, which is exactly when the question surrounding the sums of squares problem, which we solve, comes into play. Moreover, since the form class group is essentially the narrow ideal class group, we exploit this connection to help explain the mathematical architecture underlying this perspective. The reader interested in the complexity issue can read the still definitive article by Jeff Lagarias [1].

## 2. Preliminaries

Let  $\mathfrak{O}_F$  be the ring of integers in a quadratic field  $F$  of discriminant  $\Delta_F$ . Then the *wide* ideal class group is denoted by  $C_{\mathfrak{O}_F}$ , meaning  $I_F/P_F$ , where  $I_F$  is the group of fractional ideals and  $P_F$  is the group of principal fractional ideals. Equivalence of representative  $\mathfrak{O}_F$ -ideals  $I, J$  from classes in  $C_{\mathfrak{O}_F}$  is denoted by  $I \sim J$ . The *narrow* ideal class group is denoted by  $C_{\mathfrak{O}_F}^+$ , meaning  $I_F/P_F^+$ , where  $P_F^+$  is the group of principal ideals  $(\alpha)$  for  $\alpha \in \mathfrak{O}_F$ , where  $N_F(\alpha) > 0$ , namely the norm  $N_F(\alpha) = \alpha\alpha'$  is positive where  $\alpha'$  is the algebraic conjugate of  $\alpha$ . Equivalence of representatives in this group is denoted by  $I \approx J$ . The cardinality of  $C_{\mathfrak{O}_F}$  is denoted by  $h_{\mathfrak{O}_F}$  called the *wide* class number, and the cardinality of  $C_{\mathfrak{O}_F}^+$  is denoted by  $h_{\mathfrak{O}_F}^+$ , called the *narrow* class number.

### **Theorem 2.1 (Narrow and Wide Class Numbers and Ideals).**

*With notation as defined above,*

CHARACTERIZATION OF  $D = P^2 + Q^2$  WHEN  $\gcd(P, Q) = 1 \dots^3$

$$h_{\mathfrak{D}_F}^+ = \begin{cases} h_{\mathfrak{D}_F} & \text{if } \Delta_F < 0, \\ h_{\mathfrak{D}_F} & \text{if } \Delta_F > 0 \text{ and there exists a } u \in \mathfrak{U}_F \\ & \text{with } N_F(u) = -1, \\ 2h_{\mathfrak{D}_F} & \text{if } \Delta_F > 0 \text{ and there is no } u \in \mathfrak{U}_F \\ & \text{with } N_F(u) = -1. \end{cases}$$

**Proof.** See [2].

We now need to introduce the notion that is the bedrock of our characterization.

**Definition 2.1 (Ambiguous Ideals).**

If  $\mathfrak{D}_F$  is an order of discriminant  $\Delta_F$  in a quadratic field  $F$  and  $I$  is an  $\mathfrak{D}_F$ -ideal, then  $I$  is called *ambiguous* if  $I = I'$ , where  $I'$  is the conjugate ideal of  $I$ . An ambiguous class of ideals in  $C_{\mathfrak{D}_F}$ , respectively  $C_{\mathfrak{D}_F}^+$ , is one that contains an ideal  $I$  such that  $I \sim I'$ , respectively,  $I \approx I'$ .

**Definition 2.2 (Conjugates and Norms of Ideals).**

Suppose that  $F$  is a quadratic field of discriminant  $\Delta_F$ . If

$$I = \left( a, \frac{-b + \sqrt{\Delta_F}}{2} \right) = a\mathbb{Z} + \frac{-b + \sqrt{\Delta_F}}{2}\mathbb{Z}, \quad (2.1)$$

is an  $\mathfrak{D}_F$ -ideal, then

$$I' = \left( a, \frac{b + \sqrt{\Delta_F}}{2} \right) = a\mathbb{Z} \oplus \frac{b + \sqrt{\Delta_F}}{2}\mathbb{Z},$$

is called the *conjugate ideal* of  $I$ . The representation of  $I$  given in (2.1) is called the *Hermite normal form* of  $I$ , and similarly for its conjugate. The value  $a > 0$  is called the *norm* of  $I$  (and of  $I'$ ) denoted by

$$a = N(I) = N(I'),$$

the smallest positive integer in the ideal. Also,  $N(IJ) = N(I)N(J)$  for  $\mathfrak{D}_F$ -ideals  $I, J$ .

**Remark 2.1.** It can be shown, see [2], that for an  $\mathfrak{D}_F$ -ideal  $I$ ,  $I = I'$  if and only if  $N(I) | \Delta_F$ .

The next result gives us conditions on strict equivalence, namely equivalence in  $C_{\mathfrak{D}_F}^+$ , not explicit in the literature.

**Lemma 2.1.** *If  $I$  is a primitive  $\mathfrak{D}_F$ -ideal of  $C_{\mathfrak{D}_F}$ , then the following are equivalent.*

- (a)  $I \approx I'$ .
- (b) *There exists an  $\mathfrak{D}_F$ -ideal  $J$  such that  $N(J) | \Delta_F$  and  $I \sim J$ .*
- (c) *There exists a primitive  $\mathfrak{D}_F$ -ideal  $J$  such that  $I \sim J$  and  $J = J'$ .*

**Proof.** If  $I \approx I'$ , then there exist  $\alpha, \beta \in \mathfrak{D}_F$  such that  $(\alpha)I = (\beta)I'$ , where  $N_F(\alpha) > 0$  and  $N_F(\beta) > 0$ . Thus,  $N_F(\alpha/\beta) = 1$ , so by Hilbert's Theorem 90, we know there exists  $\sigma \in \mathfrak{D}_F$  such that

$$\frac{\alpha}{\beta} = \frac{\sigma}{\sigma'},$$

so

$$(\sigma)I = (\sigma')I'. \tag{2.2}$$

Suppose now that  $n \in \mathbb{N}$  is the largest value such that  $(\sigma)I = (n)J$ , where  $J$  is a primitive  $\mathfrak{D}_F$ -ideal. Then from (2.2),  $J = J'$ . Hence, from Remark 2.1,  $N(J) | \Delta_F$  and from (2.2),  $I \sim J$ . Thus, (a) implies (b).

If (b) holds, then (c) holds by Remark 2.1. If (c) holds, then  $I$  is in an ambiguous class of  $C_{\mathfrak{D}_F}$  having an ambiguous ideal  $J$ , so there exist  $\alpha, \beta \in \mathfrak{D}_F$  such that

$$(\alpha)I = (\beta)J.$$

Hence, since  $J = J'$ , it follows that

$$(\beta\alpha')I' = (\beta'\alpha)I.$$

CHARACTERIZATION OF  $D = P^2 + Q^2$  WHEN  $\gcd(P, Q) = 1$  ...<sup>5</sup>

Since

$$N_F(\beta\alpha') = N_F(\beta'\alpha),$$

$N(\beta\alpha'\beta'\alpha) > 0$ , so  $I \approx I'$ . Thus, (c) implies (a) and this completes the logical circle.

For our characterization, need the following concept.

**Definition 2.3 (Radicands of Quadratic Fields).**

If  $\Delta_F$  is the discriminant of a quadratic field  $F$ , then the *radicand* is given by

$$D_F = \begin{cases} \Delta_F/4 & \text{if } \Delta_F \equiv 0 \pmod{4}, \\ \Delta_F & \text{if } \Delta_F \equiv 1 \pmod{4}. \end{cases}$$

**3. The Characterization**

We begin with the maximal order and radicands of quadratic fields.

**Theorem 3.1 (Ambiguity and Sums of Squares).**

*Let  $D_F$  be the radicand of a quadratic field  $F$ . Then the following are equivalent.*

(a) *There is an element of order 2 in  $C_{\mathfrak{D}_F}$  that is not the image of an ambiguous class under the natural mapping  $\rho : C_{\mathfrak{D}_F}^+ \mapsto C_{\mathfrak{D}_F}$ .*

(b)  *$D_F$  is a sum of two (relatively prime) squares and there is no unit  $u \in \mathfrak{D}_F$  such that  $N_F(u) = -1$ .*

**Proof.** If (a) holds, then by Lemma 2.1, there is an  $\mathfrak{D}_F$ -ideal  $I$  such that  $I \neq I'$  and  $\rho(I)$  is an element of order 2 in  $C_{\mathfrak{D}_F}$ . Therefore,

$$C_{\mathfrak{D}_F} \not\cong C_{\mathfrak{D}_F}^+,$$

so by Theorem 2.1,  $\Delta_F > 0$  and there is no unit  $u \in \mathfrak{D}_F$  such that  $N_F(u) = -1$ . Thus, we need only show that there is no prime  $p \mid \Delta_F$  with  $p \equiv 3 \pmod{4}$  since, once established,  $\Delta_F$  is a sum of two relatively

prime squares, a well-known fact from elementary number theory – see [4, Theorem 6.3, p. 247], for instance. If such a prime  $p$  exists, then there exists

$$\gamma = (x + y\sqrt{\Delta_F})/(2z) \in \mathbb{Q}(\sqrt{\Delta_F})$$

such that

$$I = (\gamma)I', \text{ where } N_F(\gamma) = -1,$$

since  $I \sim I'$ , but  $I \not\approx I'$ . We may assume without loss of generality that  $\gcd(z, p) = 1$  given that  $D_F$  is squarefree. Since

$$\frac{x^2 - y^2\Delta_F}{4z^2} = -1, \quad x^2 \equiv -4z^2 \pmod{p}, \text{ so } (x \cdot (2z)^{-1})^2 \equiv -1 \pmod{p}.$$

However, this is a contradiction since we know  $-1$  is not a quadratic residue of such primes. We have shown that (a) implies (b). Now assume that (b) holds. Thus, there are  $a, b \in \mathbb{Z}$ ,

$$D_F = 4a^2 + b^2, \text{ for some } a, b \in \mathbb{N}. \quad (3.3)$$

By (3.3),

$$I = (a, (-b + \sqrt{\Delta_F})/2)$$

is an  $\mathfrak{D}_F$ -ideal, so

$$II' = (a) \quad (3.4)$$

and  $I^2 = ((b + \sqrt{\Delta_F})/2)$ . Assume that  $I \approx I'$ , so by Lemma 2.1,  $I \sim J = J'$ . Therefore,  $I'J \sim (1)$  so there exists  $\alpha \in \mathfrak{D}_F$  such that  $(\alpha) = I'J$ . Hence,

$$(\alpha)I = II'J = (a)J, \quad (3.5)$$

where the last equality comes from (3.4). Taking conjugates in (3.5), we get  $(\alpha')I' = (a)J' = (a)J = (\alpha)I$ .

Thus,  $(\alpha')II = (\alpha)I^2$ , which implies that  $(\alpha')(\alpha) = (\alpha)((b + \sqrt{\Delta_F})/2)$ . Hence,

CHARACTERIZATION OF  $D = P^2 + Q^2$  WHEN  $\gcd(P, Q) = 1 \dots^7$

$$\frac{\alpha'}{\alpha} = u \left( \frac{b + \sqrt{\Delta_F}}{2a} \right), \quad (3.6)$$

for some unit  $u \in \mathfrak{O}_F$ . However, by the hypothesis in (b),  $N_F(u) = 1$ , so (3.6) implies

$$1 = N_F \left( \frac{\alpha'}{\alpha} \right) = N_F \left( \frac{b + \sqrt{\Delta_F}}{2a} \right) = \frac{b^2 - \Delta_F}{4a^2} = -1,$$

a contradiction that proves  $I \neq I'$ , so  $I$  is not the image under  $\rho$  of an ambiguous class. Hence, we have (a) holds, so the result is secured.

**Example 3.1.** If  $D_F = 34 = 2^3 \cdot 17 = 3^2 + 5^2$ , then Theorem 3.2 tells us there should be an  $\mathfrak{O}_F$ -ideal of order 2 that is not the image of an ideal in an ambiguous class in  $C_{\Delta_F}^+$ . This is given, as the proof of Theorem 3.2 suggests, by  $I = (3, -5 + \sqrt{34})$ . This is of order 2 in  $C_{\mathfrak{O}_F}$ . Indeed,  $h_{\mathfrak{O}_F} = 2$ , but it is not the image of an ideal in an ambiguous class of  $C_{\mathfrak{O}_F}^+$  since  $I$  has order 4 in the narrow class group. In fact,  $h_{\mathfrak{O}_F}^+ = 4$ , and

$$(\alpha)I = \left( \frac{5 + \sqrt{34}}{3} \right) (3, -5 + \sqrt{34}) = (3, 5 + \sqrt{34}) = I'$$

but  $N_F(\alpha) = -1$ , so  $I \sim I'$  but  $I \neq I'$ .

**Example 3.2.** If  $D_F = \Delta_F = 221 = 10^2 + 11^2$ , then

$$I = \left( 5, \frac{-11 + \sqrt{221}}{2} \right),$$

has order 2 in  $C_{\mathfrak{O}_F} = C_{\mathbb{Z}[(1+\sqrt{221})/2]}$ , but  $I$  has order 4 in  $C_{\mathfrak{O}_F}^+$ .

We now show that Theorem 3.2 fails if  $\Delta_F$  is not squarefree. In other words, this criterion only works in the maximal order.

**Example 3.3.** Let  $\Delta_F = 306 = 2 \cdot 3^2 \cdot 17$ . Then in the (non-maximal) order  $\mathfrak{O}_F = \mathbb{Z}[\sqrt{306}]$ , the  $\mathfrak{O}_F$ -ideal,  $I = (9, 15 + \sqrt{306})$  is in an ambiguous class of  $C_{\mathfrak{O}_F}$ , so of order 2, but is not the image of an element in an ambiguous class of  $C_{\Delta_F}^+$ . The reason is that  $I$  has order 4 therein. Indeed,

$$(\alpha)I = \left( \frac{-15 + \sqrt{306}}{9} \right) (9, 15 + \sqrt{306}) = (9, -15 + \sqrt{306}) = I',$$

where  $N_F(\alpha) = -1$ . Thus,  $I \neq I'$ . Moreover,  $I^2$  has order 2 in  $C_{\mathfrak{O}_F}^+$  but its image is in the principal class in  $C_{\mathfrak{O}_F}$ . Yet,  $306 = 9^2 + 15^2$ , and has no other representations as a sum of two squares. Thus, this is a counterexample to the possibility of extending the criterion Theorem 3.2 to non-squarefree  $\Delta_F$ .

In view of Example 3.3, we would like to have a criterion for non-maximal orders. Thus, we need to add to the criterion given in Theorem 3.2. We refer the reader to [2] for background material on general quadratic orders. We set up the basics for the following result.

Suppose we have a quadratic field  $F$  of discriminant  $\Delta_F$  and radicand  $D_F$ . Let  $\sigma_0 = 1$  if  $\Delta_F \equiv 0 \pmod{4}$ ,  $\sigma_2 = 2$  if  $\Delta_F \equiv 1 \pmod{4}$ ,  $g = \gcd(\sigma_0, f_{\Delta_F})$ , and  $\sigma = \sigma_0/g$ . Suppose that  $\mathfrak{O}$  is an order in  $\mathfrak{O}_F$ . Then the discriminant of  $\mathfrak{O}$  is given by  $\Delta = 4D/\sigma^2$ , where  $D = (f_{\Delta_F}/g)^2 D_F$  is the *radicand of the order*  $\mathfrak{O}$ . If  $\mathfrak{O} \neq \mathfrak{O}_F$ , then  $f_{\Delta_F} > 1$ , which is the case in which we are now interested.

**Theorem 3.2 (Sums of Squares in Non-Maximal Orders).**

*Let  $D$  be the radicand of a non-maximal order  $\mathfrak{O}$  in the quadratic field  $F$ . Then the following are equivalent.*

- (a) *There is an element of order 2 in  $C_{\mathfrak{O}}$  that is not the image of an ambiguous class under the natural mapping  $\rho : C_{\mathfrak{O}}^+ \mapsto C_{\mathfrak{O}}$ , and  $-1$  is a*

CHARACTERIZATION OF  $D = P^2 + Q^2$  WHEN  $\gcd(P, Q) = 1$  ...<sup>9</sup>  
*quadratic residue modulo  $D$ .*

(b)  $D$  is a sum of two (relatively prime) squares, and there is no unit  $u \in \mathfrak{O}_F$  such that  $N_F(u) = -1$ .

**Proof.** Now that we have the condition in part (a) that  $-1$  is a quadratic residue modulo  $D$ , then we do not need the squarefreeness in the proof of Theorem 3.2 of the radicand. The rest of the proof follows similarly.

**Example 3.4.** Let  $D = 143650 = 2 \cdot 13^2 \cdot 5^2 \cdot 17$ . Then  $D = 379^2 + 3^2$ , where  $\gcd(379, 3) = 1$ . Indeed the ideal  $I = [3, 379 + \sqrt{D}]$  has order 2 in  $C_{\mathfrak{O}}$ . However,  $I$  has order 4 in  $C_{\mathfrak{O}}^+$ .

The characterization given is important not only because it classifies those  $D > 1$  which are a sum of two relatively prime squares when there is no unit of norm  $-1$  in the order, but also because it provides a mechanism for generating the elementary abelian 2-part of the ideal class group of  $C_{\mathfrak{O}_F}$  via classes of ideals with of order 2 that are not images of an ideal in an ambiguous class in the narrow class group. This fact is explored in depth in [2, Remark 6.1.1, p. 190] and the material developed therein in Chapter Six as well as in [3, Theorem 3.70, p. 162].

We conclude with a comment on the connection with binary quadratic forms. Since the narrow ideal class group is isomorphic to the class group of binary quadratic forms in a given quadratic field, then the above says that the correspondence between ideals in the wide ideal class group and the form group when the radicand is a sum of two relatively prime integers occurs when a form in a class of order 4 in the form class group corresponds to a wide ideal class of order 2. For instance, in Example 3.1, the ideal  $I = (3, -5 + \sqrt{34})$  corresponds to the form  $f(x, y) = 3x^2 + 10xy - 3y^2$ , denoted by  $(3, 10, 3)$  which is of order 4 in the form class group of discriminant  $4 \cdot 34 = 136$ . Also, in Example 3.2,  $I = (5, (-11 + \sqrt{221})/2)$  corresponds to the form  $(5, 11, -5)$ , which is of order 4 in the form class group. These examples involving forms are emblematic of a general phenomenon which we now describe.

All form classes of type  $(a, b, -a)$  are of order 4 in the form class group and their correspondence with the wide ideal class group yields an ideal of order 2. These ideal classes are exactly the classes of ideas in the wide ideal class group that are ambiguous but have no ambiguous ideal in the class. This phenomenon is discussed in depth in [2, Chapter 6].

### Acknowledgements

The author's research is supported by NSERC Canada grant # A8484.

### References

- [1] J. C. Lagarias, On the computational complexity of determining the solvability or unsolvability of the equation  $x^2 - Dy^2 = -1$ , Trans. A.M.S. 260 (1980), 485-508.
- [2] R. A. Mollin, Quadratics, CRC Press, Boca Raton, London, New York, Tokyo, 1996.
- [3] R. A. Mollin, Algebraic Number Theory, Chapman and Hall/CRC, Boca Raton, London, New York, Tokyo, 1999.
- [4] R. A. Mollin, Fundamental Number Theory with Applications, 2nd ed., Chapman and Hall/CRC, Taylor and Francis Group, Boca Raton, London, New York, 2008.
- [5] J. P. Robertson and K. R. Matthews, A Continued Fraction Approach to a Result of Feit, American Math. Monthly 115 (2008), 346-349.

<p>Paper # 1081146-MS224</p> <p>Kindly return the proof after correction to:</p> <p style="text-align: center;"><i>The Publication Manager Pushpa Publishing House Vijaya Niwas 198, Mumfordganj Allahabad-211002 (India)</i></p> <p>along with the print charges* by the <u>fastest mail</u></p> <p><b>*Invoice attached</b></p>	<p>Proof read by: .....</p> <p>Copyright transferred to the Pushpa Publishing House</p> <p>Signature: .....</p> <p>Date: .....</p> <p>Tel: .....</p> <p>Fax: .....</p> <p>e-mail: .....</p> <p>Number of additional reprints required .....</p> <p>Cost of a set of 25 copies of additional reprints @ U.S. Dollars 15.00 per page. (25 copies of reprints are provided to the corresponding author ex-gratis)</p>
---	--