SOME DIOPHANTINE EQUATIONS
OF THE FORM $x^2 - py^2 = z$

WALTER FEIT

(Communicated by David Rohrlich)

Abstract. Let $p = a^2 + (2b)^2$ be a prime. It is shown that each of the two
Diophantine equations $x^2 - py^2 = a$ or $4b$ has integral solutions.

If $p \equiv 1 \pmod{4}$ is a prime, then $p = a^2 + (2b)^2$ with $a, b \in \mathbb{Z}$. The following
theorem answers a question of Kaplansky. While part (I) is implicit in Legendre
[1] pp. 70-71 and both parts are implicit in Gauss [G, Section 265], the explicit
statement does not seem to be in the literature.

Theorem. Let $d = a^2 + (2b)^2$, with $a, b \in \mathbb{Z}$. If $d$ is a prime, the following hold:

(I) There exist relatively prime integers $x, y$ so that $x^2 - dy^2 = a$.

(II) There exist relatively prime integers $x, y$ so that $x^2 - dy^2 = 4b$.

Note that in general the equation $x^2 - dy^2 = 2b$ need not have an integral
solution. Indeed if $d \equiv 5 \pmod{8}$, then there are no solutions mod 4. On the other
hand, if $d \equiv 1 \pmod{8}$, then there may or may not be an integral solution. For
instance a solution exists if $d = 17, 41, 73, 89, 97, \ldots$, but according to the following
result pointed out to me by Serre, not if $d = 401, 577, 1601, \ldots$.

Proposition. Let $d$ be a square-free integer of the form $d = (2b)^2 + 1$, where $b$
is a positive integer such that $2b$ is not a square. Then $2b$ is not a norm from $\mathbb{Q}(\sqrt{d})$.

If $d$ is not prime, then both (I) and (II) can fail. For instance $221 = 10^2 + 11^2 = \overline{5^2 + 14^2}$, but for $a = \pm 5$ or $\pm 11$ the equation $x^2 - 221y^2 = a$ has no solution mod 13, while for $b = \pm 5$ or $\pm 7$ the equation $x^2 - 221y^2 = 4b$ has no solution mod 17.

The proof of the Theorem uses the following well-known results: If $p \equiv 1 \pmod{4}$ is a prime and $K = \mathbb{Q}(\sqrt{p})$, then $K$ has odd class number and $-1$ is the norm
of a unit in $K$.

Proof of the Theorem. Take $d = p$, a prime congruent to 1 (mod 4), and put $K = \mathbb{Q}(\sqrt{p})$. Write $R$ for the ring of integers of $K$ and $U$ for the group of units of $R$, and put $U_0 = U \cap \mathbb{Z}[\sqrt{p}]$. We denote the conjugate of an element $\alpha \in K$ by $\overline{\alpha}$, whence the norm of $\alpha$ is $N(\alpha) = \alpha\overline{\alpha}$.

Lemma 1. (i) If $p \equiv 1 \pmod{8}$, then $U = U_0$.

(ii) In any case $U = U_0$ or $\vert U : U_0 \vert = 3$.

(iii) $U_0$ contains a unit of norm $-1$. \hfill $\Box$

Received by the editors January 20, 2000.
2000 Mathematics Subject Classification. Primary 11D09, 11R11.
Key words and phrases. Quadratic field, prime.

\c 2000 American Mathematical Society
To begin with assume only that

\[ \text{Proof of the Proposition.} \]

(i) Suppose that \( u \in U \) but \( u \notin U_0 \). Then \( u = (s + t\sqrt{p})/2 \) with \( s, t \) odd integers. Hence \( (s^2 - t^2)/2 = \pm 4 \). Reading modulo 8 yields \( 1 - p \equiv 4 \pmod{8} \), contrary to assumption.

(ii) By (i) we may assume that \( p \equiv 5 \pmod{8} \). Let \( u = (s + t\sqrt{p})/2 \) with \( s, t \) odd integers. Then \( u^3 = ((s^3 + 3st^2p) + n\sqrt{p})/8 \) for some integer \( n \). However \( s^3 + 3st^2p \equiv s(1 + 3p) \equiv 0 \pmod{8} \). Therefore \( u = m + n\sqrt{p}/8 \) for \( m, n \) integers. As \( u \) is an algebraic integer it follows that \( n = 0 \pmod{8} \).

(iii) This follows from (ii), because \( p \equiv 1 \pmod{4} \) and therefore \( -1 \in N(U) \).

To prove part (I) of the Theorem, write \( (a^2) = AA' \), where \( A \) is the ideal \( (2b - \sqrt{p}) \) in \( R \). A prime divisor \( P \) of \( A \) and \( A' \) must divide \( a^2 \) and \( 2\sqrt{p} = (2b + \sqrt{p}) - (2b - \sqrt{p}) \). As \( (a, 2p) = 1 \), this implies that \( A \) and \( A' \) are relatively prime. Hence \( A = C^2 \) for some ideal \( C \). Since the class number of \( K \) is odd, \( C = (\gamma) \) is principal and \( N(\gamma) = \pm a \). Furthermore, \( \gamma^2 = (2b - \sqrt{p})u \) for some unit \( u \). Thus if \( \gamma_1 = \gamma_2u \), then \( N(\gamma_1) = \pm a \) and \( \gamma_1 = (2b - \sqrt{p})u^3 \). As \( u^3 \in U_0 \) it follows from Lemma 1 that \( \gamma_1 = x + y\sqrt{p} \) with \( x, y \in \mathbb{Z} \). Multiplying by a unit in \( U_0 \) of norm \( -1 \) if necessary we may assume that \( N(\gamma_1) = a \) as required. If \( n = (x, y) \), then \( n \) divides \( \gamma_1 \), hence \( n^2 \) divides \( \gamma_2 \) and also \( (2b - \sqrt{p})) \). Thus \( n = 1 \).

To prove (II), write \( (b^2) = BB' \), where \( B \) is the ideal \( (a - \sqrt{p})/2 \) in \( R \). A prime divisor \( P \) of \( B \) and \( B' \) must divide \( b^2 \) and \( \sqrt{p} = (a + \sqrt{p})/2 - (a - \sqrt{p})/2 \). As \( (b, p) = 1 \), this implies that \( B \) and \( B' \) are relatively prime and so \( B = D^2 \) for some ideal \( D \). The rest of the argument is the same as in part (I).

**Proof of the Proposition.** To begin with assume only that \( d \) is a square-free integer \( > 1 \). Put \( K = \mathbb{Q}(\sqrt{d}) \), and let \( \tau \) be the nonidentity automorphism of \( K \) and \( N \) the norm. Write \( R \) for the ring of integers of \( K \) and \( U \) for the group of units of \( R \).

**Lemma 2.** Fix \( u \in U \) and let \( n \) be the norm of an element in \( R \). Then there exists \( \alpha \in R \) such that \( 1 < \alpha \leq u \) and \( |N(\alpha)| = |n| \). Furthermore, if we write \( \alpha = (x + y\sqrt{d})/2 \) with \( x, y \in \mathbb{Z} \), then

\[ |y| < (u + |n|)/\sqrt{d}. \]

**Proof.** Let \( n = N(\alpha_0) \). Replacing \( \alpha_0 \) by \( -\alpha_0 \) if necessary we may assume that \( \alpha_0 > 0 \). Thus there exists an integer \( k \) with \( \alpha^k < \alpha_0 \leq \alpha^{k+1} \). Then \( \alpha = \alpha_0 u^{-k} \) satisfies the first condition. Since \( 1 < \alpha \) and \( |\alpha\alpha'| = |n| \) it follows that \( |\alpha'| < |n| \) and so

\[ |y|\sqrt{d} = |\alpha - \alpha'| \leq |\alpha| + |\alpha'| < u + |n| \]

as required.

Now let \( d \) be as in the Proposition and put \( u = 2b + \sqrt{d} > 1 \), so that \( u \in U \). If \( 2b = N(\alpha) \) for some \( \alpha \in R \), then \( |y| < (2b + \sqrt{d}) + 2b)/\sqrt{d} = 1 + 4b/\sqrt{d} < 3 \) by Lemma 2. If \( y = 0 \), then \( 2b = x^2 \), so \( y \neq 0 \). Then \( y^2 = 1 \) or \( 4 \). As \( x^2 - y^2d = 2b\varepsilon \) with \( \varepsilon = \pm 1 \) we have \( (2xy)^2 - (4y^2b + \varepsilon)^2 = 4y^4 - 1 \). Thus \( |2xy| = |4y^2b + \varepsilon| \) are \( c_1, c_2 \) respectively for some \( c_1, c_2 \) with \( 4y^4 - 1 = c_1c_2 \). Consequently \( 4|xy|, |8y^2b + 2\varepsilon| \) are \( c_1 \pm c_2 \) respectively. If \( y^2 = 1 \), this yields that \( \{c_1, c_2\} = \{1, 3\} \) and so \( 4|x| = 4 \) and \( |8b + 2\varepsilon| = 2 \). Hence \( b = 0 \), a contradiction. If \( y^2 = 4 \), then \( 4y^4 - 1 = 63 \) and so \( \{c_1, c_2\} = \{1, 63\}, \{3, 21\} \) or \( \{7, 9\} \). Hence \( |32b + 2\varepsilon| = 62 \) or \( 2 \). The only possibility is \( b = 2 \), so \( 2b \) is a square, a contradiction.
SOME DIOPHANTINE EQUATIONS OF THE FORM $x^2 - py^2 = z$

REFERENCES


Department of Mathematics, Yale University, Box 208283, New Haven, Connecticut 06520-8283

E-mail address: feit@math.yale.edu