THE SOLVABILITY OF THE EQUATION $ax^2+by^2=c$ IN QUADRATIC FIELDS

NEAL PLOTKIN

Abstract. In a recent paper, L. J. Mordell gave necessary and sufficient conditions for the equation $ax^2+by^2=c$ to have algebraic integer solutions in the quadratic field $Q(\sqrt{(-n)})$. In this paper we drop the requirement that the solutions be algebraic integers. In particular, we prove that $ax^2+by^2=c$ has solutions in $Q(\sqrt{(-n)})$ if and only if the quadratic form $abt^2-bcu^2-acv^2-nw^2$ represents 0 over $Q$.

I. Theorem 1. Let $a$, $b$, $c$ be nonzero rational numbers, and $n$ an integer. Then solutions of the equation $ax^2+by^2=c$ exist in the quadratic field $Q(\sqrt{(-n)})$ if and only if solutions of $abt^2-bcu^2-acv^2=n$ exist in the field of rationals, $Q$.

We remark that rational solutions of $abt^2-bcu^2-acv^2=n$ exist if and only if the quadratic form $abt^2-bcu^2-acv^2-nw^2$ represents 0 in $Q$. The latter representation is a classical problem with a known solution—see [2, p. 75], noting that by a simple change of variables, we may assume the coefficients of $abt^2-bcu^2-acv^2-nw^2$ are square-free integers, no three having a factor in common.

Proof of Theorem 1. ($\Leftarrow$) Suppose there exist $t_0$, $u_0$, $v_0 \in Q$ with $abt^2_0-bcu^2_0-acv^2_0=n$.

Case I. Suppose $bu_0+av_0=0$. Then $abt^2_0=n$.

Let $x=((b-c)/2abt_0)\sqrt{(-n)}$, $y=(b+c)/2b$.

Case II. Suppose $bu_0+av_0\neq 0$.

Let $x=(1/d)(bt_0u_0+v_0\sqrt{(-n)})$, $y=((-d)(at_0v_0-u_0\sqrt{(-n)}))$, where $d=bu_0^2+av_0^2$.

In either case, an easy calculation shows that $ax^2+by^2=c$.

($\Rightarrow$) Suppose $ax^2_0+by^2_0=c$, where $x_0=r+s\sqrt{(-n)}$, $y_0=p+q\sqrt{(-n)}$.
\[ p, q, r, s \in \mathbb{Q}. \] Then

\[
c = a(r + s\sqrt{(-n)})^2 + b(p + q\sqrt{(-n)})^2
= (ar^2 - ans^2 + bp^2 - bnq^2) + (2ars + 2bpq)s\sqrt{(-n)}.
\]

Therefore \( ars + bpq = 0. \)

**Case I.** Suppose \( q = 0. \) Then \( c = ar^2 - ans^2 + bp^2, \) and also \( ars = 0, \) so either \( r \) or \( s = 0. \) If \( s = 0, \) we have \( c = ar^2 + bp^2. \) Upon multiplying by \( abc, \) this yields \( abc^2 = bca^2r^2 + a^2b^2q^2, \) which may be rewritten \( ab(c)^2 - bc(ar)^2 - ac(bp)^2 = 0; \) i.e. the quadratic form \( abt^2 - bcu^2 - acv^2 \) represents \( 0 \) in \( \mathbb{Q}. \)

By a well-known result [2, p. 41], \( abt^2 - bcu^2 - acv^2 \) also represents \( n \) in \( \mathbb{Q}. \)

If \( r = 0, s \neq 0, \) then \( c = bp^2 - ans^2, \) so \( n = (bp^2 - c)/as^2, \) which may be rewritten in the form \( n = ab(p/as)^2 - ac(1/as)^2 - bc(0)^2, \) which is a rational solution of \( n = abt^2 - bcu^2 - acv^2. \)

**Case II.** Suppose \( q \neq 0. \) Then \( p = -ars/bq. \) Therefore

\[
(*) \quad c = ar^2 - ans^2 + b(ar/bq)^2 - bnq^2.
\]

Solving for \( n, \) we get

\[
n = \frac{1}{xs^2 + bq^2} \left( ar^2 + \frac{a^2rs^2}{bq^2} - c \right) = \frac{ar^2}{bq^2} - \frac{c}{xs^2 + bq^2}
= ab \left( \frac{r}{bq} \right)^2 - ac \left( \frac{s}{xs^2 + bq^2} \right)^2 - bc \left( \frac{q}{xs^2 + bq^2} \right)^2,
\]

a rational solution of \( n = abt^2 - bcu^2 - acv^2. \)

Note that \( c \neq 0 \Rightarrow as^2 + bq^2 \neq 0 \) (from \( *) \). This completes the proof.

As an interesting special case, we get the following result of Fein and Gordon [1, Theorem 7].

**Corollary 1.** \( x^2 + y^2 = -1 \) may be solved in \( \mathbb{Q}(\sqrt{(-n)}), \) \( n \) a square-free integer, if and only if \( n > 0 \) and \( n \equiv 7 \pmod{8}. \)

**Proof.** Take \( a = b = -c = 1 \) in the theorem. We find that there are solutions in \( \mathbb{Q}(\sqrt{(-n)}), \) if and only if \( n \) is the sum of three squares, \( r^2 + u^2 + v^2, \) in \( \mathbb{Q}. \) By clearing denominators, we see that this occurs if and only if \( nw^2 = t_1^2 + u_1^2 + v_1^2, \) where \( t_1, u_1, v_1, w \) are integers. But it is well known that this is true if and only if \( nw^2 \) is not of the form \( 4^i(8j + 7), \) i.e. if and only if \( n \) (being square-free) is not congruent to 7 \( \pmod{8}. \)

II. In [3, p. 118], L. J. Mordell showed that \( ax^2 + by^2 = c \) has algebraic integer solutions in precisely the quadratic fields:

\[ A : \mathbb{Q}(\sqrt{(-abd^2/d_1^2 - c|d)}), \]

where \( d|abc, p \) and \( q \) are integers such that \( ap^2 + bq^2 = d, (ap, bq) = d_1, \) and
k is any integer making the radicand an integer, and

\[ B: \mathbb{Q}(\sqrt{-(abk^2/d_1^2 - 4c/d)}) \]

where \( d \mid abc \), \( p \), \( q \), and \( d_1 \) are as above, and \( k \) is any integer such that \( k = (abk^2/4d_1^2) - c/d \) is an integer.

In this section we show that the result of Theorem 1 is distinct from that of Mordell, i.e. there exists a field \( \mathbb{Q}(\sqrt{-(n)}) \) in which \( x^2 + y^2 = -1 \) has solutions but no algebraic integer solutions.

We have \( a = b = -c = 1 \). In case A, \( d = 1 \), so \( p = 0 \) or 1, \( q = 1 \) or 0, and \( d_1 = 1 \). Therefore there are algebraic integer solutions in the field \( \mathbb{Q}(\sqrt{-(k^2+1)}) \), any integer \( k \). In case B, \( d = 2 \), \( p = q = d_1 = 1 \), and so there are algebraic integer solutions in any field \( \mathbb{Q}(\sqrt{-(k^2+2)}) \), \( k \) odd. These are all.

In the field \( \mathbb{Q}(\sqrt{-(6)}) \), \( x = (2 + \sqrt{-(6)})/2 \), \( y = (2 - \sqrt{-(6)})/2 \) is a solution of \( x^2 + y^2 = -1 \). However, \( \mathbb{Q}(\sqrt{-(6)}) \) is neither of the form \( \mathbb{Q}(\sqrt{-(k^2+1)}) \), \( k \) an integer, nor \( \mathbb{Q}(\sqrt{-(k^2+2)}) \), \( k \) odd. For suppose \( \mathbb{Q}(\sqrt{-(6)}) = \mathbb{Q}(\sqrt{-(k^2+1)}) \). Then \( k^2 + 1 = 6j^2 \), some integer \( j \). It is easy to see there are no such \( k \), \( j \) by considering the equation mod 8. Now suppose \( \mathbb{Q}(\sqrt{-(6)}) = \mathbb{Q}(\sqrt{-(k^2+2)}) \), \( k \) odd. Therefore \( k^2 + 2 = 6j^2 \). Since \( k \) is odd, we again get a contradiction mod 8.

**Bibliography**