An Equation of Mordell

By Andrew Bremner

Abstract. All integer solutions of the Diophantine equation \(6y^2 = (x + 1)(x^2 - x + 6)\) are found.

1. Mordell [1] asks if all the integer solutions of the Diophantine equation \(6y^2 = (x + 1)(x^2 - x + 6)\) are given by \(x = -1, 0, 2, 7, 15, 74\). It is shown that there are precisely seven integer solutions, the seventh with \(x = 767\).

Consideration of factorization gives, for some integers \(a, b,\)

\[
\begin{align*}
&x^2 - x + 6 = 6b^2 \quad \text{or} \quad x^2 - x + 6 = 3b^2 \\
&x + 1 = a^2 \\
&x^2 - x + 6 = 2b^2 \quad \text{or} \quad x^2 - x + 6 = b^2 \\
&x + 1 = 3a^2 \\
&x^2 - x + 6 = 2b^2 \quad \text{or} \quad x^2 - x + 6 = b^2 \\
&x + 1 = 6a^2
\end{align*}
\]

and the latter case is impossible modulo 3. We thus obtain, on eliminating \(x,\) the three quartic equations,

(i) \(a^4 - 3a^2 + 8 = 6b^2,\)
(ii) \(4a^4 - 6a^2 + 8 = 3b^2,\)
(iii) \(9a^4 - 9a^2 + 8 = 2b^2.\)

The standard technique in dealing with equations of this type is to factorize in the appropriate quadratic extension of the integers, which here is \(\mathbb{Z}[(1 + \sqrt{-23})/2],\) to obtain a finite set of equations of the form,

\[a^2 = f(v, w), \quad 1 = g(v, w),\]

where \(f, g\) are homogeneous quadratic forms.

We need to know some details of the quadratic field \(\mathbb{Q}(\sqrt{-23}).\) The class-number of the ring of integers is 3; and we denote the ideal factorizations of 2 and 3 by

\((2) = p_2\overline{p}_2, \quad (3) = p_3\overline{p}_3\) where a bar denotes conjugacy, and \(p_2 p_3 = ((1 + \sqrt{-23})/2).\)

Thus in Eq. (i), \((2a^2 - 3)^2 + 23 = 24b^2\) implies the ideal equation

\[
\left(\frac{2a^2 - 3 \pm \sqrt{-23}}{2}\right) = q\overline{q} \quad \text{where} \quad q = (6) \quad \text{and} \quad b \quad \text{is some integral ideal.}
\]

There are essentially two possibilities, \(q = p_2 p_3\) and \(q = \overline{p}_2 p_3.\) In the former instance, \(b\) is principal, and in the latter, \(b\overline{p}_2\) is principal.

Since \(p_3\overline{p}_2^{-1} = ((1 + \sqrt{-23})/4)\) we have, respectively,
\[\pm \left( \frac{2a^2 - 3 \pm \sqrt{-23}}{2} \right) = \left( \frac{1 + \sqrt{-23}}{2} \right) \left( \frac{u + v\sqrt{-23}}{2} \right)^2\]

and

\[\pm \left( \frac{2a^2 - 3 \pm \sqrt{-23}}{2} \right) = \left( \frac{1 + \sqrt{-23}}{4} \right) \left( \frac{u + v\sqrt{-23}}{2} \right)^2\]

for some integers \(u, v\) satisfying \(u \equiv v \mod 2\). Thus we have, respectively,

\[
\begin{align*}
-(2a^2 - 3) &= \frac{u^2 - 46uv - 23v^2}{4} \\
1 &= \frac{u^2 + 2uv - 23v^2}{4}
\end{align*}
\]

and

\[
\begin{align*}
(2a^2 - 3) &= \frac{u^2 - 46uv - 23v^2}{8} \\
-1 &= \frac{u^2 + 2uv - 23v^2}{8}
\end{align*}
\]

where the signs in each equation have been determined by a congruence modulo 3.

In the former case, putting \(u + v = 2w\), we obtain

I: \[
\begin{align*}
a^2 &= w^2 + 12wv - 12v^2 \\
1 &= w^2 - 6v^2.
\end{align*}
\]

In the latter case, \(u^2 + 2uv + v^2 \equiv 0 \mod 8\), so \(u + v = 4w\) say; then

II: \[
\begin{align*}
a^2 &= 6u^2 - 12uv - 2w^2 \\
1 &= 3u^2 - 2w^2.
\end{align*}
\]

In similar manner (ii) gives rise to

III: \[
\begin{align*}
a^2 &= -2w^2 + 12wv - 6v^2 \\
1 &= 4w^2 - 3v^2
\end{align*}
\]

and (iii) to the three pairs

IV: \[
\begin{align*}
a^2 &= u(9v + 16w) \\
1 &= 9v^2 - 8w^2
\end{align*}
\]

and

V: \[
\begin{align*}
a^2 &= u(v + 8w) \\
1 &= v^2 - 18w^2
\end{align*}
\]

and

VI: \[
\begin{align*}
a^2 &= 32w(v - 9w) \\
1 &= v^2 - 288w^2.
\end{align*}
\]

Of these six pairs of equations, V and VI may be treated by simple descent arguments. For instance, in VI, we have that \(w = m^2\) or \(2m^2\) after change of sign if necessary: so it suffices to determine all integer solutions of the equations \(1 = v^2 - 18m^4\) and \(1 = v^2 - 72m^4\), respectively. This is readily achieved by means of a classical descent argument; but we can quote Ljunggren [2] to say that the only integer solutions of the former are \((\pm r, \pm m) = (1, 0)\) and \((17, 1)\), and of the latter \((\pm r, \pm m) = (1, 0)\). These give the solutions \(a = 0\) and \(a = 16\) of Eq. (iii) whence solutions \(x = -1, 767\) of the original equation.
Each of the four remaining pairs of equations represents the intersection of two quadrics in three-dimensional space; the method of solution, as exploited by Cassels [3], is to consider the singular elements in the pencil of the quadrics. Such singular quadrics are given by \( f - \lambda g \), where \( \det(f - \lambda g) = 0 \): that is, a linear combination of \( f \) and \( g \) which is a perfect square. In general, of course, \( \lambda \) is a quadratic irrational. We can thus rewrite each pair of equations in the form \( a^2 - \mu L(u, w)^2 = \lambda \) for some \( \mu \in \mathbb{Q}(\lambda) \), where \( L(u, w) \) is a homogeneous linear form with coefficients in \( \mathbb{Q}(\lambda) \). We now work over \( \mathbb{Q}(\delta) \) where \( \delta^2 = \mu \) and equate \( (a + L\delta) \) and \( (a - L\delta) \) as ideals, to two ideal factors of \( \lambda \) in \( \mathbb{Q}(\delta) \), noting that the two factors must be conjugate over \( \mathbb{Q}(\mu) \). All the ideals are principal, so using the appropriate arithmetical details of the field \( \mathbb{Q}(\delta) \), we can equate coefficients of elements of an integer base; in particular, it is clear that the coefficient of \( \delta^2 \) in \( a + L\delta \) is zero, and the resulting equation is completely solved by congruence considerations.

As an illustration, consider Eq. II. The singular quadrics in this pencil are obtained by taking a linear combination which is a perfect square: so let

\[
3(2 + \lambda)v^2 - 12wv - 2(1 + \lambda)w^2 \text{ be a perfect square.}
\]

Then \( 36 = -6(1 + \lambda)(2 + \lambda) \) or \( \lambda^2 + 3\lambda + 8 = 0 \). Taking \( \lambda = (-3 - \sqrt{-23})/2 \) we obtain

\[
a^2 - \left(1 + \frac{\sqrt{-23}}{2}\right)\left[w - \frac{1 - \sqrt{-23}}{4}v\right] = \frac{3 + \sqrt{-23}}{2},
\]

and accordingly work in \( \mathbb{Q}(\delta) \) where \( \delta^2 = 1 + \sqrt{-23} \). We need some arithmetical details of this field; certainly \( \tau = (\delta^3 - 2\delta^2 + 2\delta + 4)/8 \) is an algebraic integer, since \( \tau^2 - \tau((1 - \sqrt{-23})/2) + 1 = 0 \). The discriminant of \( R = \mathbb{Z}[1, \delta, \delta^2/2, \tau] \) is \( 2^3 \cdot 3 \cdot 23^2 \), whence \( R \) is indeed the ring of integers of the field (for 23 certainly ramifies, so \( 23^2 \) divides the discriminant, and Stickelberger’s criterion says that the discriminant is congruent to 0 or 1 modulo 4). It is also readily calculated by standard techniques that \( \delta \) is a fundamental unit for the field, and that we have the factorization,

\[
(2) = \mathfrak{q}_2(q^2)^2,
\]

where \( \mathfrak{q}_2 = \mathfrak{p}_2, (q^2)^2 = \overline{\mathfrak{p}_2} \), with \( \mathfrak{p}_2 = (2, (1 + \sqrt{-23})/2) \).

The equation now becomes in terms of ideals,

\[
(a + \delta\left(w - \frac{v}{2}\right) + \frac{\delta^3}{4}v)\left(a - \delta\left(w - \frac{v}{2}\right) - \frac{\delta^3}{4}v\right) = (q^2)^6,
\]

and since the two ideals on the left are conjugate over \( \mathbb{Z}[(1 + \sqrt{-23})/2] \) we must have

\[
(a + \delta\left(w - \frac{v}{2}\right) + \frac{\delta^3}{4}v)^3 = (q^2)^6 = \left(\frac{\delta^3 - 6\delta + 16}{4}\right).
\]

Because there are no nontrivial roots of unity in \( \mathbb{Q}(\delta) \) we now obtain \( a + \delta(w - v/2) + (\delta^3/4)v = \pm((\delta^3 - 6\delta + 16)/4)r^n \) for some integer \( n \). This exponential equation is solved by first comparing coefficients of \( \delta^2 \), using the fact that \( \tau^5 \equiv -1 \mod 7 \); a congruence modulo a suitable power of 7 then shows that the only solutions are given by \( n = 0 \) or \( -3 \). These give \( a = 4 \) as solution of (i), and \( x = 15 \) as a solution of the original equation.

The complete details of the proof are to appear in my Ph.D. Thesis. I gratefully thank Professors Swinnerton-Dyer and Cassels for their advice and encouragement.
Emmanuel College
Cambridge, England