Mordell’s Equation: An Introduction

1 Introduction

Fix $d \in \mathbb{Z}$. The diophantine equation $y^2 = x^3 + d$ for integer values $(x, y)$ is known as the Bachet-Mordell (hereafter shortened to Mordell’s) equation. Bachet created a method to generate infinitely many rational solutions, provided at least one such solution exists. Mordell indeed proved thus was the case when $d \neq -1, -432$ and $d$ is sixth power-free. On the other hand, he demonstrated that this equation finitely many integer solutions (provided they do exist).

Here, we will describe all of the integer solutions to the Mordell’s equation for a large family of values of $d$. This exposition is inspired by Keith Conrad’s Examples of Mordell’s Equations and Franz Lemmermeyer’s Algebraic Number Theory notes, both of which may be found online.

2 An example without solutions

In order to show a diophantine equation has no integer solutions, it is often useful to use congruences modulo an integer which is cunningly chosen. Here’s one such example.

**Theorem 2.1** $y^2 = x^3 - 3$ has no integer solutions.

*Proof:* Suppose that such an integer solution $(x, y)$ exists. We first narrow down the values which $x$ can equal: $x$ can not be even, because this would imply that $y^2 \equiv -3 \equiv 5 \mod 8$. This is impossible, since the squares modulo 8 are 0, 1, or 4. Moreover, $x \not\equiv 1 \mod 4$, because this would imply that $y^2 \equiv 2 \mod 4$, which is also impossible. Therefore, $x \equiv 3 \mod 4$ for a solution to exist.

To eliminate this possibility, we first rewrite the equation as $y^2 + 4 = x^3 + 1 = (x + 1)(x^2 - x + 1)$. Observe that $x^2 - x + 1 \geq 3$ for $x > 1$, and $x \equiv 3 \mod 4$ implies that $x^2 - x + 1 \equiv 3 \mod 4$. Thus, $x^2 - x + 1$ has a prime factor $p \equiv 3 \mod 4$. (Otherwise, $x^2 - x + 1$ would only have prime factors which are 1 mod 4. Then, their product $x^2 - x + 1 \equiv 1 \mod 4$, which is a contradiction.). Hence, we conclude that $p \mid (y^2 + 4)$, or equivalently $y^2 \equiv -4 \mod p$. Since 4 is a perfect square, we conclude that $-1$ is a square modulo $p$. This is a contradiction, because the Legendre symbol $\left( \frac{-1}{p} \right) = -1$ when $x \equiv 3 \mod 4$. ■

Many other equations of the Mordell type may be solved in this manner. However, at this point, we will turn to the methods of algebraic number theory (more specifically, the arithmetic in the number ring of $\mathbb{Q}(\sqrt{-d})$) to see what we may further deduce.
3 Using Algebraic Number Theory

First, let’s rewrite the Mordell equation as \( y^2 + d = x^3 \). We will see what conditions to impose on \( d \) as we go along in the derivation that ensues. Factoring this equation in the number ring \( \mathcal{O} \) of \( \mathbb{Q}(\sqrt{-d}) \), we obtain

\[
(y + \sqrt{-d})(y - \sqrt{-d}) = x^3.
\]

Let \( a = (y + \sqrt{-d}) \) and \( a' = (y - \sqrt{-d}) \). The first question we ask is what is the gcd of \( a \) and \( a' \)? We ultimately would like these ideals to be relatively prime. Suppose that \( p \) is a common prime divisor (with \( p \mid (\rho) \) for some prime \( p \in \mathbb{N} \)). It is clear that \( p \mid ((y + \sqrt{-d}) - (y - \sqrt{-d})) = (2\sqrt{-d}) \).

1. If \( p \neq 2 \), then we have \( p \mid (\sqrt{-d}) \). Hence \( p \mid d \), which in turn implies \( p \mid y \), \( p \mid x \), and thus \( p^2 \mid d \). We will exclude this by insisting that \( d \) is squarefree.

2. Now, we suppose that \( p \mid (2) \).

   (a) If \( d \equiv 2 \mod 4 \), then \( p = (2, \sqrt{-d}) \mid (\sqrt{-d}) \). This implies that \( p \mid (y) \), and hence \( p \mid y \). In this case, \( x^3 \equiv y^2 + d \equiv 0 + 2 = 2 \mod 4 \), which can’t occur.

   (b) If \( d \equiv 1 \mod 4 \), then \( p = (2, 1 + \sqrt{-d}) \mid (y + \sqrt{-d}) \) is true iff \( y \) is odd. In this case, \( x^3 \equiv y^2 + d \equiv 1 + 1 = 2 \mod 4 \), which can’t occur.

   (c) If \( d \equiv 3 \mod 4 \), then \( y + \sqrt{-d} \) is divisible by \( p \) if \( y \) is odd. This implies that \( x \) is even and thus \( d = -y^2 \equiv -1 \mod 8 \). So, if we assume that \( d \not\equiv 7 \mod 8 \), then no \( p \mid (2) \) can be a common divisor of \( a \) and \( a' \).

Under the above underlined conditions, we may assume that \( a \) and \( a' \) are relatively prime. Since their product is a cube, there exists an ideal \( b \) such that \( a = b^3 \). Conjugation shows that there exists an ideal \( b' \) such that \( a' = b'^3 \).

Now, let \( h \) be the class number of \( \mathbb{Q}(\sqrt{-d}) \). Since both \( b^3 \) and \( b'^h \) are principal, we can conclude that \( b \) is also principal if we insist that \( 3 \nmid h \).

Thus, \( b = \langle \frac{r + s\sqrt{-d}}{2} \rangle \) for some \( r \equiv s \mod 2 \).

If we insist that \( d > 0 \), then we have no fundamental units. Moreover, let’s insist that \( d \neq 3 \) (this imaginary quadratic ring has the most units; fortunately we showed this equation has no solutions in the previous section). Otherwise, the units are \( \pm 1 \) for \( d \neq 1 \) and \( \pm 1, \pm i \) for \( d = 1 \). Either way, the ideal equation yields the equation of numbers

\[
y + \sqrt{-d} = \left( \frac{r + s\sqrt{-d}}{2} \right)^3,
\]

where we have subsumed the units into the cube. Comparing coefficients, we see that \( 1 = \frac{1}{2}(3r^2s - ds^3) \), or \( 8 = s(3r^2 - ds^2) \). This implies that \( s \mid 8 \). Hence, \( s = \pm 1 \) or both \( r \) and \( s \) are even. In the first case, we get \( \pm 8 = 3r^2 - d \) or
\[d = 3r^2 \mp 8.\] In the second case, writing \(r = 2t\) and \(s = 2u\), we find that \(d = 3t^2 \mp 1\).

In summary, under the underlined conditions for \(d\), if \(d\) is not of the form \(3t^2 \pm 1\) or \(3t^2 \pm 8\), then the diophantine equation \(y^2 = x^3 - d\) has no integer solution. (Note that we may remove the restriction \(d \neq 3\), since 3 is of neither of the two forms quoted above).

What happens if \(d\) has this form? Straightforward algebra yields the following theorem:

**Theorem 3.1** Let \(d\) be a squarefree positive integer satisfying \(d \neq 7 \mod 8\). If the class number of \(\mathbb{Q}[\sqrt{-d}]\) is not divisible by 3, then the diophantine equation \(y^2 = x^3 - d\) has

1. Exactly two pairs of integral solutions \((3, \pm 4)\) and \((15, \pm 58)\) for \(d = 11\).
2. Exactly one pair of integral solutions if \(d \neq 11\) has the form \(d = 3t^2 \pm 1\) or \(d = 3t^2 \pm 8\) for some \(t \in \mathbb{Z}\), namely

\[
(x, y) = \begin{cases} 
(4t^2 + 1, \pm t(8t^2 + 3)) & \text{if } d = 3t^2 + 1 \\
(4t^2 - 1, \pm t(8t^2 - 3)) & \text{if } d = 3t^2 - 1 \\
(t^2 + 2, \pm t(t^2 + 3)) & \text{if } d = 3t^2 + 8 \\
(t^2 - 2, \pm t(t^2 - 3)) & \text{if } d = 3t^2 - 8.
\end{cases}
\]

3. No integral solutions otherwise. \(\blacksquare\)

**Remark:** \(d = 11\) is the only integer that has a representation \(3r^2 + 8\) and \(3t^2 - 1\). (Any other combination of representations are actually impossible; this is easy to check.)

Suppose you have not calculated \textit{a priori} the class number of the imaginary quadratic ring, and you find \textit{extra} integer solutions. For instance, \(y^2 = x^3 - 26\) has the predicted solution \((207, \pm 42849)\) as well as \((3, \pm 1)\). Congratulations; you have indirectly shown that the class number of \(\mathbb{Q}[\sqrt{-26}]\) must be divisible by 3! (In fact \(h = 6\) for this example.)

**Theorem 3.2** Let \(u\) be an odd integer and set \(d = 27u^6 - 1\). If \(d\) is squarefree, then \(\mathbb{Q}[\sqrt{-d}]\) has class number divisible by 3.

**Proof:** Note that \(d = 3t^2 - 1\) for \(t = 3u^3\). Besides the predicted solution \((4t^2 - 1, \pm t(8t^2 - 3))\), we also have the solution \((3u^2, 1)\). So, one of the conditions of Theorem 3.1 is not satisfied. In this case, we find that only the class number condition is not satisfied. \(\blacksquare\)

This is a good place to stop. I’ll refer you to the literature for what happens in the real quadratic case.