1

What Is the Mordell Conjecture (Faltings's Theorem)?

Diophantine geometry is the field of mathematics that concerns integer solutions and rational solutions of polynomial equations. It is named after *Diophantus of Alexandria* from around the third century who wrote a series of books called *Arithmetica*. Diophantine geometry is one of the oldest fields of mathematics, and it continues to be a major field in number theory and arithmetic geometry. If integer solutions and rational solutions are put aside, then polynomial equations determine an algebraic variety. Since around the start of the twentieth century, algebro-geometric methods have played an important role in the study of Diophantine geometry.

In 1922, Mordell (Figure 1.1) made a surprising conjecture in a paper where he proved the so-called Mordell–Weil theorem for elliptic curves (see Theorem 3.42). This conjecture, called the Mordell conjecture before Faltings's proof appeared, states that the number of rational points is finite on any geometrically irreducible algebraic curve of genus at least 2 defined over a number field. It is not certain on what grounds Mordell made this conjecture, but it was audacious at the time, and attracted the attention of many mathematicians. While some partial results were obtained, the Mordell conjecture stood as an unclimbed mountain before the proof by Faltings. Thus, when Faltings (Figure 1.2) proved the Mordell conjecture in a paper published in 1983, the news was circulated around the globe with much enthusiasm. Faltings's proof was momentous, using sophisticated and profound theories of arithmetic geometry. He proved the Shafarevich conjecture, the Tate conjecture, and the Mordell conjecture concurrently, and he was awarded the Fields Medal in 1986. Nevertheless, first-year students at universities can understand the statement of the Mordell conjecture, except for the notion of genus.

Let $f(X, Y)$ be a two-variable polynomial with coefficients in a number field K (e.g., the field $\mathbb{Q}$ of rational numbers). We assume the following:

Figure 1.1 Louis J. Mordell.
Source: Archives of the Mathematisches Forschungsinstitut Oberwolfach.

Figure 1.2 Gerd Faltings.
Source: Archives of the Mathematisches Forschungsinstitut Oberwolfach.

1. $f(X,Y)$ is irreducible as a polynomial in $\mathbb{C}[X,Y]$. Namely, if $f(X,Y) = g(X,Y)h(X,Y)$ with $g(X,Y), h(X,Y) \in \mathbb{C}[X,Y]$, then $g(X,Y)$ or $h(X,Y)$ is a constant.
2. The algebraic curve C defined by $f(X,Y) = 0$, extended to the projective plane, is smooth. In other words, let $F(X,Y,Z) \in \mathbb{C}[X,Y,Z]$ be the homogeneous polynomial with

$$F(X,Y,1) = f(X,Y) \quad \text{and} \quad \deg F(X,Y,Z) = \deg f(X,Y).$$

Then the only solution in $\mathbb{C}^3$ of

$$\begin{aligned} F(X,Y,Z) &= (\partial F/\partial X)(X,Y,Z) = (\partial F/\partial Y)(X,Y,Z) \\ &= (\partial F/\partial Z)(X,Y,Z) = 0 \end{aligned}$$

is $(0,0,0)$.

In this setting, the algebraic curve C has genus at least 2 if and only if the degree of f is at least 4. Thus, the Mordell conjecture states that if the degree of f is at least 4, then the number of points $(a,b) \in K^2$ with $f(a,b) = 0$ is finite. Here, the assumption that f is irreducible is essential. Indeed, for

any polynomial $h(X,Y) \in K[X,Y]$, we set $f(X,Y) = Xh(X,Y)$. Then $f(X,Y) = 0$ has infinitely many solutions $\{(0,b) \mid b \in K\}$. On the other hand, the assumption that C is smooth is not essential. This assumption is made only to avoid the notion of genus.

Let us look at some examples. For simplicity, we assume for the moment that K is the field $\mathbb{Q}$ of rational numbers.

The quadratic polynomial $f(X,Y) = X^2 + Y^2 - 1$ satisfies assumptions 1 and 2, and the set of all rational solutions of $f(X,Y) = 0$ (i.e., points $(a,b) \in \mathbb{Q}^2$ with $f(a,b) = 0$) is equal to

$$\left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) \;\middle|\; t \in \mathbb{Q} \right\} \cup \{(-1,0)\}.$$

Indeed, we associate a point $(a,b) \neq (-1,0)$ with $f(a,b) = 0$ to the slope t of the line $Y = t(X+1)$ that passes $(-1,0)$ and (a,b). Then the set of rational solutions of $f(X,Y) = 0$ other than $(-1,0)$ is in bijective correspondence with $\mathbb{Q}$. In this case, there are infinitely many rational points on the curve C defined by $f(X,Y) = 0$.

Next, we consider the quadratic polynomial $f(X,Y) = X^2 + Y^2 + 1$. It satisfies assumptions 1 and 2, but there are no rational solutions of $f(X,Y) = 0$. In general, if $f(X,Y)$ is a quadratic polynomial satisfying assumptions 1 and 2, then either there are infinitely many rational solutions of $f(X,Y) = 0$ or there are none. In other words, either there are infinitely many rational points on the curve C defined by $f(X,Y) = 0$ or there are none.

What about cubic polynomials? First we consider the cubic polynomial $f(X,Y) = X^3 + Y^3 - 1$. It satisfies assumptions 1 and 2. According to Euler (the cubic case of Fermat's last theorem), there are exactly four rational solutions $(\pm 1, 0), (0, \pm 1)$ for $f(X,Y) = 0$.

Next, we consider the cubic polynomial $f(X,Y) = Y^2 - X^3 - 877X$. It is easy to see that $f(X,Y)$ satisfies assumptions 1 and 2, and $(0,0)$ is a rational solution of $f(X,Y) = 0$. On the other hand, it is difficult to find a rational solution of $f(X,Y) = 0$ other than $(0,0)$. Perhaps surprisingly, there are in fact infinitely many rational solutions of $f(X,Y) = 0$, and the x-coordinate of the next "simple" rational solution (to be precise, the x-coordinate of a rational point with the next smallest Weil height in Chapter 3) is

$$\left(\frac{612776083187947368101}{78841535860683900210} \right)^2,$$

a result due to Bremner and Cassels. In general, the algebraic curve C defined by a cubic polynomial satisfying assumptions 1 and 2, extended to the projective plane, is equipped with the structure of an abelian group. Thus,

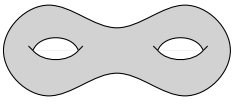

Figure 1.3 A curve of genus 2.

the set of rational points on C (on the projective plane) is also equipped with the structure of an abelian group, and the Mordell–Weil theorem (see Theorem 3.42) states that this group is finitely generated. In summary, if $f(X,Y)$ is a cubic polynomial satisfying assumptions 1 and 2, then there may be infinitely many rational points on the curve C defined by $f(X,Y)=0$, but they are finitely generated as an abelian group.

What about polynomials of degree 4 or higher? This is where the Mordell conjecture comes in. It states that under assumptions 1 and 2, there are only finitely many rational points on the curve defined by the polynomial.

For any polynomial $\phi(X)$ in X of degree 4 or higher with coefficients in $\mathbb{Q}$, we put $f(X,Y)=Y-\phi(X)$. Then $\{(a,\phi(a)) \mid a\in\mathbb{Q}\}$ are rational points on the curve C defined by $f(X,Y)=0$, and the curve C is smooth (on the affine plane). This may look strange at first glance, but in fact C has a singular point at the point $(0:1:0)$ at infinity on the projective plane, so assumption 2 is not satisfied.

Let $f(X,Y)$ be a polynomial of degree d satisfying assumptions 1 and 2, and let C be the curve defined by $f(X,Y)=0$ (extended on the projective plane). The *genus* of C, which we have not explained so far, is equal to the number $(d-1)(d-2)/2$. Thus, the genus is 0 if $d=1,2$, 1 if $d=3$, and at least 3 if $d\geq 4$. The genus of the curve defined by $Y-\phi(X)=0$ is 0. Now the meaning of the Mordell conjecture becomes clearer. It states that the distribution of rational points is determined by the genus of the curve (Figure 1.3). Further, the genus of a curve is a topological invariant, realized geometrically as the number of "holes" of the curve. Thus, the Mordell conjecture states that a topological invariant controls rational points.

With its generality and innovativeness, no one thought that the Mordell conjecture would be solved before the turn of the century. The solution by Faltings was a monumental achievement in twentieth-century mathematics. In this book, we will call the Mordell conjecture "Faltings's theorem."

Perhaps Faltings's success lifted a mental block associated with the Mordell conjecture. Subsequently, Vojta and Bombieri found a relatively elementary proof in line with classical Diophantine geometry [5, 29]. The purpose of the present book is to give a self-contained proof of Faltings's theorem by

following [5, 29], giving detailed accounts for some of the computations. Because the proof uses important results and techniques from Diophantine geometry, such as the theory of heights, the Mordell–Weil theorem, Siegel's lemma, and Roth's lemma, this book also serves as an introduction to Diophantine geometry. In this book, the reader will find the names of many great mathematicians who have contributed to the advancement of the field. In some sense, the path to Faltings's theorem ran alongside the advancement of mathematics more generally.

Lastly, we remark on some recent developments. In [9], Faltings proved that, if a subvariety X of an abelian variety defined over a number field does not contain a translation of a positive dimensional abelian subvariety, then the number of rational points on X is finite. A smooth projective curve of genus at least 2 is regarded as a subvariety of an abelian variety via the Jacobian embedding, and it does not contain a translation of a positive dimensional abelian subvariety. Thus, this result, often called Faltings's big theorem, generalizes Faltings's theorem on the Mordell conjecture. In this direction, the next big challenge will certainly be Lang's conjecture: if (the analytification of) a smooth projective variety X defined over a number field is a hyperbolic manifold, then the number of rational points on X should be finite. A smooth projective curve of genus at least 2 is a hyperbolic manifold, and thus, Lang's conjecture is a generalization of the Mordell conjecture. Very recently, Lawrence and Venkatesh [16] gave another proof of Faltings's theorem based on a detailed analysis of the variation of p-adic Galois representations, which does not use abelian varieties. Still the proofs of the Mordell conjecture that are known so far do not directly use hyperbolicity, and thus, are not applicable to Lang's conjecture. For example, the proof by Vojta and Bombieri in this book does not use the geometry of hyperbolic manifolds directly but instead uses some properties that are derived from the assumption that the genus g of the curve be at least 2 (e.g., $g > \sqrt{g}$, ampleness of a canonical bundle, and an embedding into the Jacobian variety). New ideas are needed for a direct proof of the Mordell conjecture that contributes to Lang's conjecture.