Chapter 1
Why Quadratic Diophantine Equations?

In order to motivate the study of quadratic type equations, in this chapter we present several problems from various mathematical disciplines leading to such equations. The diversity of the arguments to follow underlines the importance of this subject.

1.1 Thue's Theorem

Since ancient times mathematicians tried to solve equations over the integers. Pythagoras for instance described all integers as side lengths of rectangular triangles. After Diophantus from Alexandria such equations are called *Diophantine equations*. Since that time, many mathematicians worked on this topic, such as Fermat, Euler, Kummer, Siegel, and Wiles.

In 1909, A. Thue (see [62]) proved the following important theorem:

Let $f = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ *be an irreducible polynomial of degree* ≥ 3 *with integral coefficients. Consider the corresponding homogeneous polynomial*

$$F(x, y) = a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_1 x y^{n-1} + a_0 y^n.$$

If m is a nonzero integer, then the equation

$$F(x, y) = m$$

has either no solution or only a finite number of solutions in integers.

This result is in contrast to the situation when the degree of F is $n = 2$. In this case, if $F(x, y) = x^2 - Dy^2$, where D is a nonsquare positive integer, then for all nonzero integers m, the general Pell's equation

$$x^2 - Dy^2 = m$$

has either no solution or it has infinitely many integral solutions.

T. Andreescu, D. Andrica, *Quadratic Diophantine Equations*,
Developments in Mathematics 40, DOI 10.1007/978-0-387-54109-9_1

1.2 Hilbert's Tenth Problem

In 1900, at the International Congress of Mathematicians in Paris, David Hilbert, looking forward to the coming century, proposed 23 problems with which twentieth century mathematicians would have to contend. The tenth on the list, commonly simply termed "Hilbert's Tenth Problem," called for a general method to determine the solvability or unsolvability in integers of Diophantine equations. With our current knowledge of the unsolvability of this problem, it would be interesting to know why Hilbert felt it had a positive solution. Did it look like the Gaussian theory could extend indefinitely to more and more variables and higher and higher degrees? Did he think one could cut through all the details and give an abstract proof, in the way he finished off the theory of invariants? Or was it just a manifestation of his faith in the mathematician's ability to solve all problems he posed for himself—a faith on which he was quite explicit? The actual statement of Hilbert's Tenth Problem is rather brief and uninformative:

Given a Diophantine equation with any number of unknown quantities and with integral numerical coefficients, devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in integers.

To solve the Diophantine equation

$$f(x_1, x_2, \ldots, x_n) = 0,$$

where $f \in \mathbb{Q}[X_1, X_2, \ldots, X_n]$, amounts to determine the integer points on the corresponding hypersurface of the affine space. Hilbert's tenth problem is to give an algorithm which tells whether such a given Diophantine equation has a solution or not.

The final answers to Hilbert original tenth problem were given in 1970 by Yu. Matiyasevich, after the works of M. Davis, H. Putnam, and J. Robinson. This was the culminating stage of a rich and beautiful theory (see [59, 124, 130, 131], and [132]). The solution is negative: there is no hope nowadays to achieve a complete theory of the subject. But one may still hope that there is a positive answer if one restricts Hilbert's initial question to equations in few variables, say $n = 2$, which amounts to considering integer points on a plane curve. In this case deep results have been achieved during the twentieth century and many results are known, but much more remains unveiled.

The logical assault on Hilbert's Tenth Problem began around 1950, the first tentative papers appearing in the ensuing decade, the first major breakthrough appearing in print in 1961, and the ultimate solution being published in 1970. The first contributions were made by Julia Robinson and Martin Davis.

Robinson defined a relation R on natural numbers to be *Diophantine* if it could be written in the form

$$R(x_0, \ldots, x_{n-1}) : \exists y_0 \ldots y_{m-1} P(x_0, \ldots, x_{n-1}, y_0, \ldots, y_{m-1}) = 0,$$

where P is a polynomial with integral coefficients and $y_0, \ldots, y_{m-1}$ range over *natural* numbers. (Logicians prefer their Diophantine equations to have nonnegative integral solutions, an inessential reformulation of the usual Fermatian Diophantine problem.) Finding she could not exhibit many demonstrably Diophantine relations, she allowed exponentiation to enter into P to form *exponential Diophantine* relations. She was able to show several interesting relations to be exponential Diophantine, and she reduced the general problem of showing all exponential Diophantine relations to be Diophantine to that of showing any relation of roughly exponential growth to have a Diophantine graph. In this reduction, she used the sequence of solutions to the special Pell's equations

$$x^2 - (a^2 - 1)y^2 = 1, \quad a \geq 2.$$

Davis took a more logical approach. The theory of algorithms recognizes two basic types of sets of natural numbers, namely: *recursive* sets, for which an algorithm determining membership exists, and *recursively enumerable* sets, for which an algorithmic enumeration exists. There are recursively enumerable sets which are not recursive. If every recursively enumerable set could be shown to be Diophantine, then Hilbert's Tenth Problem would have no effective solution. The techniques Gödel developed in proving his famous Incompleteness Theorems readily show that every recursively enumerable set can be written in the form

$$\exists y_0 Q_1 y_1 \ldots Q_{m-1} y_{m-1} P(x, y_0, \ldots, y_{m-1}) = 0,$$

where each Q_i is either an existential quantifier or a *bounded* universal quantifier, i.e., a quantifier of the form $\forall y_i \leq y_0$. Davis simplified this representation to the *Davis Normal Form*

$$\exists y \forall\, z \leq y\, \exists\, w_0 \ldots w_{m-1} \leq y P(x, y, z, w_0, \ldots, w_{m-1}) = 0.$$

Within a few years, Robinson's husband Raphael showed one could take $m = 4$.

Towards the end of the 1950s, Hilary Putnam joined Davis. Together they proved—modulo the unproved assumption of the existence of arbitrarily long arithmetic progressions of prime numbers—the unsolvability of the exponential Diophantine problem over the natural numbers. With Julia Robinson's help, the unproven conjecture was bypassed. Together, Davis, Putnam, and Robinson applied Robinson's exponential Diophantine relations to eliminate the single bounded universal quantifier from the Davis Normal Form. Their proof was published in 1961.

With the Davis–Putnam–Robinson Theorem, Robinson's reduction of the problem of representing exponential Diophantine relations as Diophantine relations to the special problem of giving a Diophantine representation of a single relation of roughly exponential growth assumed a greater importance. The 1960s saw no progress in the construction of such a relation, merely a profusion of further reductions based on it; for example, on the eve of the final solution, Robinson

showed it sufficient to prove the Diophantine nature of any infinite set of prime numbers. In March 1970 the world of logic learned that the then twenty-two-year-old Yuri Matiyasevich has shown the relation

$$y = F_{2x}$$

to be Diophantine, where $F_0, F_1, \ldots$ is the Fibonacci sequence. Very quickly, a number of researchers adapted Matiyasevich's proof to give a direct proof of the Diophantiness of the sequences of solutions to the special Pell's equations

$$x^2 - (a^2 - 1)y^2 = 1, \quad a \geq 2,$$

cited earlier.

Interestingly, the corresponding problems when real solutions are looked for has a positive answer. The decision problem over the reals: *is there an algorithm deciding the existence of real solutions to a set of polynomial equation with integer coefficients?* was solved with a yes answer by Tarski [211] and Seidenberg [197].

1.3 Euler's Concordant Forms

In 1780, Euler asked for a classification of those pairs of distinct nonzero integers M and N for which there are integer solutions (x, y, z, t) with $xy \neq 0$ to

$$x^2 + My^2 = t^2 \quad \text{and} \quad x^2 + Ny^2 = z^2.$$

This is known as Euler's concordant forms problem. When $M = -N$, Euler's problem is the celebrated congruent number problem to which Tunnell gave a conditional solution using the theory of elliptic curves and modular forms. More precisely, let $E_{M,N}$ be the elliptic curve

$$y^2 = x(x + M)(x + N).$$

If the group of $\mathbb{Q}$-rational points of $E_{M,N}$ has positive rank, then there are infinitely many primitive integer solutions to Euler's concordant forms problem. But if the rank is zero, there is a solution if and only if the $\mathbb{Q}$-torsion subgroup of rational points of $E_{M,N}$ is $\mathbb{Z}_2 \times \mathbb{Z}_8$ or $\mathbb{Z}_2 \times \mathbb{Z}_6$. All the curves $E_{M,N}$ having such torsion subgroups are classified as follows. The torsion subgroup of $E_{M,N}(\mathbb{Q})$ is $\mathbb{Z}_2 \times \mathbb{Z}_8$ if there is a nonzero integer d such that $(M, N) = (d^2u^4, d^2v^4)$ or $(-d^2v^4, d^2(u^4 - v^4))$ or $(d^2(u^4 - v^4, -d^2v^4)$, where (u, v, w) is a Pythagorean triple. The torsion subgroup of $E_{M,N}(\mathbb{Q})$ is $\mathbb{Z}_2 \times \mathbb{Z}_6$ if there exist integers a and b such

that $\frac{a}{b} \notin \left\{-2, -1, -\frac{1}{2}, 0, 1\right\}$ and $(M, N) = (a^4 + 2a^3b, 2a^3b + b^4)$. Thus Euler's problem is reduced to a question of $\mathbb{Q}$-ranks of the Mordell–Weil groups of Frey curves. In proving the above results (see [166]) the study of the simultaneous Pell's equations

$$a^2 - Mb^2 = 1 \quad \text{and} \quad c^2 - Nb^2 = 1$$

played an important role.

1.4 Trace of Hecke Operators for Maass Forms

The trace of the Hecke operator $T(n)$ acting on a Hilbert space of functions spanned by the eigenfunctions of the Laplace–Beltrami operator Δ with a positive eigenvalue can be viewed as an analogue of Eichler–Selberg trace formula for nonholomorphic cusp forms of weight zero. For $\mathrm{Re}\ \sigma > 1$, let

$$L_n(\sigma) = \sum_{d \in \Omega} \sum_{u} \frac{h_d \ln \varepsilon_d}{(du^2)^\sigma},$$

where the summation on u is taken over all the positive integers u which together with t are the integral solution of the equation $t^2 - du^2 = 4n$, h_d is the class number of indefinite rational quadratic forms with discriminant d, and $\varepsilon_d = \frac{1}{2}(u_0 + v_0\sqrt{d})$, with (u_0, v_0) being the fundamental solution to the general Pell's equation

$$u^2 - dv^2 = 4.$$

Here Ω is the set of all positive integers d such that $d \equiv 0$ or $1 \pmod 4$ and d is not a perfect square. For more details we refer to [113].

1.5 Diophantine Approximation and Numerical Integration

Consider the quadrature formula over the s-dimensional unit cube of the form

$$\int_0^1 \cdots \int_0^1 f(x_1, \ldots, x_s) dx_1 \ldots dx_s = q^{-1} \sum_{t=1}^{q} f\left(\frac{a_1 t}{q}, \ldots, \frac{a_s t}{q}\right) + R,$$

where q and $a_1, \ldots, a_s$ are positive integers and f is supposed periodic of period 1 in each variable. Choose q to be a prime and seek to determine $a_1, \ldots a_s$ so as to minimize R for a class of functions f whose multiple Fourier coefficients are small.

One of the main methods is based on units of algebraic fields (see [94]). In this method the field is $R(\sqrt{p_1},\ldots,\sqrt{p_t})$, where $p_1,\ldots,p_t$ are distinct primes and the units are the fundamental solutions to the general Pell's equations

$$x^2 - Dy^2 = \pm 4,$$

where D runs over the $2^t - 1$ proper divisors of $p_1 p_2 \ldots p_t$.

1.6 Threshold Phenomena in Random Lattices and Reduction Algorithms

By a lattice is meant here the set of all linear combinations of a finite collection of vectors in $\mathbb{R}^n$ taken with integer coefficients,

$$\mathcal{L} = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_p.$$

One may think of a lattice as a regular arrangement of points in space, somewhat like atoms composing a crystal in $\mathbb{R}^3$. Given the generating family (e_j), there is great interest in finding a "good" basis of the lattice. By this is meant a basis that is "almost" orthogonal and is formed with vectors of "small" length. The process of constructing a "good" basis from a skewed one is referred to as lattice reduction.

Lattice reduction is of structural interest in various branches of mathematics. For instance, reduction in dimension 2 is completely solved by a method due to Gauss. This entails a complete classification of binary quadratic forms with integer coefficients, a fact that has numerous implications in the analysis of quadratic irrationals and in the representation of integers by quadratic forms, for example Pell's equation

$$x^2 - dy^2 = 1.$$

1.7 Standard Homogeneous Einstein Manifolds and Diophantine Equations

If $M = G/H$ is a homogeneous manifold and G is a semisimple Lie group, then there is a standard Riemannian metric g on M given by restricting the Killing form. An interesting problem is to study when g is an Einstein metric. In many cases the Einstein equations reduce to a series of integer constraints. These Diophantine equations in certain special cases often reduce to variants of Pell's equation. Such a case is as follows. Suppose K, L and R are Lie groups. Let $G = K^r \times R$, for some integer r, and let $H = K \times L$. Suppose that H is embedded in G via (Δ, π), where $\Delta : K \to K^r$ is the diagonal and $\pi : K \times L \to R$ is some representation. There are limited number of possibilities for K, L and R. One of these is $K = SO(n)$, $L = SO(m)$ and $R = SO(n+1)$. The Einstein equations reduce to some Pell's equations in n, m and r and these have infinitely many solutions (see [156] for details).

1.8 Computing Self-Intersections of Closed Geodesics

Let Γ be a subgroup of finite index in the modular group $\Gamma(1) = SL(2,\mathbb{Z})$. An interesting problem is to compute the self-intersection number of a closed geodesic on H/Γ, where H is the hyperbolic plane.

Suppose the geodesic is given as the axis γ of $A \in \Gamma(1)$. Since by assumption $[\Gamma(1) : \Gamma] < \infty$, one can find a least $n \in \mathbb{Z}_+$, with $A^n \in \Gamma$. Fix the standard fundamental region $R = \left\{ z \in H : \ |z| \geq 1, \ |\mathrm{Re}\, z| \leq \frac{1}{2} \right\}$ for $\Gamma(1)$ and let $\mathcal{T}$ be the tessellation of H by images of R under $\Gamma(1)$. As γ cuts $\mathcal{T}$, it is divided into segments. Translating back to R by appropriate products of the generators $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, determined by the order in which γ cuts sides of $\mathcal{T}$, one can obtain a finite family of segments in R whose union projects to cover a fundamental period of A^n disjointly (except that points on ∂R will be covered twice). The algorithm consists in computing the endpoints on R of all these translates of γ (under $\Gamma(1)$) and testing them in pairs for intersections in $\Gamma(1)$ and then in Γ.

It is possible to write down the primitive hyperbolic in $\Gamma(1)$ whose axis joins two conjugate quadratic numbers, using minimal solutions of suitable *Pell's equations* (see [110]).

1.9 Hecke Groups and Continued Fractions

The Hecke groups

$$G_q = \left\langle \begin{pmatrix} 1 & \lambda_q \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle; \quad \lambda_q = 2\cos\frac{\pi}{q}, \quad q \geq 3$$

are Fuchsian groups of the first kind. The λ-continued fractions (λF) can be used to study the geodesics on the modular surfaces determined by G_q. The period of the λF for periodic $\sqrt{D}/C$ has nearly the form of the classical case. The solutions to *Pell's equation* in quadratic extensions of $\mathbb{Q}(\lambda_q)$ as well as the Legendre's constant of Diophantine approximation for G_q, i.e., γ_q such that $\left|\alpha - \frac{P}{Q}\right| < \frac{\gamma_q}{Q^2}$ implies that $\frac{P}{Q}$ of "reduced finite λF form" is a convergent of real $\alpha \notin G_q(\infty)$, play an important role in proving the above result. For details we refer to [186].

1.10 Sets of Type (m, n) in Projective Planes

A set of type (m, n) in a projective plane is a set of points such that each line intersects it in either m or n points. Numerical conditions for the existence of such sets in planes of finite order q can be given. In particular, for $m = 1$ and $n \geq 4$, it is shown that q is of the form $q = (n-1)P_s(n)$, where $P_s(n)$ satisfies the recurrence relation $P_0(n) = 0$, $P_1(n) = 1$, and $P_s(n) = (n-2)P_{s-1}(n) - P_{s-2}(n) + 1$. The proof consists in solving the quadratic Diophantine equation in two variables $x^2 - x - (n-2)xy + y^2 - y = 0$ which is related to a *general Pell's equation* (see [209] for details).