4. Diophantine Equations

A *Diophantine Equation* is simply an equation in one or more variables for which *integer* (or sometimes rational) solutions are sought. For example:

- $x^2 + y^2 = z^2$ has solutions $(x, y, z) = (3, 4, 5), (5, 12, 13), \dots;$
- $x^3 + y^3 = z^3$ has no solutions with x, y, z positive integers;
- $x^2 - 61y^2 = 1$ has infinitely many solutions with $x, y > 0$; the smallest has $x = 1766319049$ and $y = 226153980$.

We will use the techniques we have developed in earlier chapters, as well as one new one, to solve a number of Diophantine equations all of which have had some historical interest. Their solution has led to the development of much of modern algebra and number theory. The new technique we will use is called the *Geometry of Numbers*.

4.1. Geometry of Numbers and Minkowski's Theorem.

We will use the geometry of $\mathbb{R}^n$ and of certain subsets of it:

Definition 4.1.1. *A* lattice *in* $\mathbb{Z}^n$ *is a subgroup* $L \subseteq \mathbb{Z}^n$ *of finite index.*

The lattices we will use are all defined using congruence conditions on the coordinates of vectors in $\mathbb{Z}^n$, and the index of the lattice will be determined from the moduli of these congruences (example to follow soon). There are more general subsets of $\mathbb{R}^n$ called lattices, but we will not need them.

Our general strategy will be to set up a lattice so that the coordinates give a "modular approximation" to the equation being solved; then to get an exact solution we require a second condition, that the vector of coefficients is "small" in some sense. Minkowski's Theorem will show that (under certain conditions) there are short lattice vectors, and we win. Its statement requires the following definitions.

Definition 4.1.2. *A subset $S \subseteq \mathbb{R}^n$ is* symmetric *if $x \in S \iff -x \in S$, and* convex *if $x, y \in S \implies tx + (1-t)y \in S$ for all t with $0 \leq t \leq 1$.*

Here is the result from the geometry of numbers we will use to deduce the existence of solutions to several Diophantine Equations:

Theorem 4.1.3. *[Minkowski] Let $L \leq \mathbb{Z}^n$ be a lattice of index m, and let $S \subseteq \mathbb{R}^n$ be a bounded convex symmetric domain. If S has volume $v(S) > 2^n m$, then S contains a nonzero element of L.*

The same conclusion holds when $v(S) = 2^n m$, provided that S is compact.

4.2. **Sums of squares.** In this section we will give an answer to the questions "which positive integers can be expressed as a sum of 2 squares (S2S), or a sum of 3 squares (S3S), or a sum of 4 squares (S4S)"? In the 3-squares case we will only give a partial proof, since the full proof uses concepts which we will not cover. The reason for the S3S case being harder is that the set of S3S numbers is not closed under multiplication, while for S2S and S4S it is, which then essentially reduces the question to the case of primes.

4.2.1. *Sums of two squares.* To ask whether an integer n is a sum of two squares, $n = a^2 + b^2$, is the same as to ask whether it is the norm of a Gaussian Integer: $n = a^2 + b^2 = N(\alpha)$ where $\alpha = a + bi \in \mathbb{Z}[i]$. Using Theorem 1.5.14 on Gaussian primes, such an integer must be a product of norms of Gaussian primes which are: 2, p for any prime $p \equiv 1 \pmod 4$, and q^2 for any prime $q \equiv 3 \pmod 4$. This proves the following:

Theorem 4.2.1. *The positive integer n may be expressed as a sum of two squares, $n = x^2 + y^2$, if and only if $\operatorname{ord}_q(n)$ is even for all primes $q \equiv 3 \pmod 4$, or equivalently if and only if $n = ab^2$ where a has no prime factors congruent to $3 \pmod 4$.*

Remarks: One can similarly characterize positive integers of the form $n = x^2 + 2y^2$ as those such that $\operatorname{ord}_q(n)$ is even for all primes $q \equiv 5, 7 \pmod 8$. Either a direct proof or one based on unique factorization in the Euclidean Domain $\mathbb{Z}[\sqrt{-2}]$ is possible. A similar result holds for $n = x^2 + 3y^2$ (though is slightly harder to prove since $\mathbb{Z}[\sqrt{-3}]$ is not Euclidean). But the pattern does not continue, and for general m it is a very hard problem to determine exactly which integers n, or even which primes p, have the form $x^2 + my^2$. The study of this question leads on to algebraic number theory, and in particular to the study of the arithmetic properties of quadratic number fields.

Recall from Chapter 1 that the key to determining the Gaussian primes was a fact which we only proved later (Theorem 2.4.2): that if p is a prime such that $p \equiv 1 \pmod 4$ then p is a sum of two squares. We proved this in Chapter 2 by using facts about Gaussian Integers, together with the fact that for such primes the congruence $x^2 \equiv -1 \pmod p$ has a solution. Now we give a different proof that $p \equiv 1 \pmod 4 \implies p = a^2 + b^2$, as a first application of the Geometry of Numbers.

Theorem 4.2.2. *[=Theorem 2.4.2 again] Let p be a prime such that $p \equiv 1 \pmod 4$. Then there exist integers a and b such that $p = a^2 + b^2$.*

Before applying Minkowski again to prove the four-square theorem below, we will briefly (and incompletely) look at sums of three squares.

4.2.2. *Sums of three squares.*

Proposition 4.2.3. *Let n be a positive integer with $n \equiv 7 \pmod 8$. Then n is not a sum of three squares, and nor is any integer of the form $4^k n$ with $n \equiv 7 \pmod 8$.*

The converse of this result is true: every positive integer not of the form $4^k n$ with $n \equiv 7 \pmod 8$ can be written as a sum of three squares. But this is harder to prove and we omit it. Instead we turn to sums of four squares.

4.2.3. *Sums of four squares.*

Theorem 4.2.4. *[Lagrange] Every positive integer may be expressed as a sum of four squares.*

Note that 0 is allowed as one of the squares. The theorem will follow from the following Lemma 4.2.5, which reduces the problem to expressing all primes as S4S, and Proposition 4.2.6 which shows that all primes are S4S.

Lemma 4.2.5. *If $m = a_1^2 + a_2^2 + a_3^2 + a_4^2$ and $n = b_1^2 + b_2^2 + b_3^2 + b_4^2$ then $mn = c_1^2 + c_2^2 + c_3^2 + c_4^2$ where*

$$\begin{aligned}
c_1 &= a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4 \\
c_2 &= a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3 \\
c_3 &= a_1b_3 - a_3b_1 - a_2b_4 + a_4b_2 \\
c_4 &= a_1b_4 - a_4b_1 + a_2b_3 - a_3b_2.
\end{aligned}$$

Proposition 4.2.6. *Every prime number may be expressed as a sum of four squares.*

4.3. **Legendre's Equation.** Here is an example of an equation with **no** nontrivial solutions.

Example: The equation $x^2 + y^2 = 3z^2$ has no integer solutions except $x = y = z = 0$.

For suppose that (x, y, z) is a nonzero solution. Then we may assume that $\gcd(x, y) = 1$ since if both x and y were divisible by some prime p, then $p^2|3z^2$ and so $p|z$, so we could divide through by p^2 to get the smaller nontrivial solution $(x/p, y/p, z/p)$. Next, neither x nor y is divisible by 3 (since if either is then so would the other be). This implies $x \equiv \pm 1 \pmod 3$ and $y \equiv \pm 1 \pmod 3$, so $x^2 + y^2 \equiv 1 + 1 = 2 \not\equiv 0 \pmod 3$, contradicting $x^2 + y^2 = 3z^2$.

We have used two properties of the number 3 here: that it is square-free (so $p^2|3z^2 \implies p|z$) and that $x^2 + y^2 \equiv 0 \pmod 3 \implies x \equiv y \equiv 0 \pmod 3$. So the same argument works for the equations $x^2 + y^2 = qz^2$ where q is any prime congruent to $3 \pmod 4$.

The general equation

$$ax^2 + by^2 = cz^2 \tag{4.3.1}$$

with $a, b, c \in \mathbb{N}$ has been studied since the 19th century, and is known as *Legendre's Equation*. There is a simple criterion for the existence of nontrivial solutions in terms of congruences modulo a, b and c. By a *solution* to (4.3.1) we will always mean a solution other than the trivial one $(x, y, z) = (0, 0, 0)$. By homogeneity, (x, y, z) satisfies (4.3.1) if and only if (rx, ry, rz) also does for any $r \neq 0$; a solution will be called *primitive* if $\gcd(x, y, z) = 1$.

First we reduce to the case where a, b, c are pairwise coprime and square-free:

- If $d = \gcd(a, b) > 1$ then (x, y, z) satisfies (4.3.1) if and only if (dx, dy, z) satisfies the similar equation with coefficients $(a/d, b/d, cd)$. Similarly if $\gcd(a, c) > 1$ or $\gcd(b, c) > 1$. Note that the product abc is reduced (by a factor d) in each case, so after a finite number of such steps we may assume that a, b, c are pairwise coprime.

- If $d^2|a$ then (x, y, z) satisfies (4.3.1) if and only if (dx, y, z) satisfies the similar equation with coefficients $(a/d^2, b, c)$. Similarly with square factors of b or c, so we can assume that each of a, b, c is square-free.

Theorem 4.3.1. *Let $a, b, c \in \mathbb{N}$ be pairwise coprime and square-free. Then a non-trivial solution to (4.3.1) exists if and only if each of the quadratic congruences*

$$x^2 \equiv bc \pmod{a}, \qquad x^2 \equiv ac \pmod{b}, \qquad x^2 \equiv -ab \pmod{c}$$

has a solution.

Our proof just fails to show that there always is a solution satisfying the inequalities $|x| \le \sqrt{bc}$, $|y| \le \sqrt{ac}$, $|z| \le \sqrt{ab}$, because of the adjustment needed at the end; however there is always such a "small" solution (proof omitted).

To make the proof constructive, we would need to have a method for finding short vectors in lattices. Such methods do exist (the most famous is the LLL method named after Lenstra, Lenstra and Lovasz) and have a huge number of applications in computational number theory and cryptography. One reason that lattice-based methods are becoming popular in cryptography is that they are "quantum-resistant", meaning that no-one (yet!) knows how to solve problems such as the SVP (Shortest Vector Problem) using a quantum computer, unlike the case for factorization-based methods such as RSA.

4.4. **Pythagorean Triples.** A classical problem is to find all right-angled triangles all of whose sides have integral length. Letting the sides be x, y and z this amounts (by Pythagoras's Theorem) to finding positive integer solutions to the Diophantine equation

$$x^2 + y^2 = z^2. \tag{4.4.1}$$

A solution (x, y, z) is called a *Pythagorean Triple*. For example, $(3, 4, 5)$ is a Pythagorean Triple.

Clearly if (x, y, z) is a Pythagorean Triple then so is (kx, ky, kz) for all $k \geq 1$, and to avoid this trivial repetition of solutions we will restrict to *Primitive Pythagorean Triples* which have the additional property that $\gcd(x, y, z) = 1$. From (4.4.1) it then follows that x, y, z are pairwise coprime, since a prime divisor of any two would have to divide the third.

Finally, in any primitive Pythagorean Triple, exactly one of x and y is even, the other odd; for they are not both even by primitivity, and cannot both be odd for then $x^2 + y^2 \equiv 2 \pmod 4$, so $x^2 + y^2$ could not be a square. By symmetry we only consider triples with x and z odd, y even.

The following result shows how to parametrize all primitive Pythagorean Triples.

Theorem 4.4.1. *Let u and v be positive coprime integers with $u \not\equiv v \pmod 2$ and $u > v$. Set*

$$x = u^2 - v^2; \qquad y = 2uv; \qquad z = u^2 + v^2.$$

Then (x, y, z) is a primitive Pythagorean Triple. Conversely, all primitive Pythagorean Triples are obtained in this way for suitable u and v.

We will see an application of our parametrization of Pythagorean triples to the Fermat equation $x^4 + y^4 = z^4$ in the next section. This case of Fermat's Last Theorem says that there are no Pythagorean Triples with all three integers perfect squares.

An alternative approach to the previous Theorem is to use the Gaussian Integers $\mathbb{Z}[i]$. Suppose $x^2 + y^2 = z^2$ with $\gcd(x, y) = 1$ and z odd. Then $z^2 = (x + yi)(x - yi)$, and the factors on the right are coprime: for if $\alpha|x+yi$ and $\alpha|x-yi$ for some $\alpha \in \mathbb{Z}[i]$, then $\alpha|2x$ and $\alpha|2yi$, from which $\alpha|2$ since $\gcd(x,y)=1$ and i is a unit. But $\gcd(z,2)=1$ so α is a unit.

Now each of $x \pm yi$ must be a square or a unit times a square, since they are coprime and their product is a square **and $\mathbb{Z}[i]$ is a UFD**. If $x+yi = \pm(u+vi)^2$ then $x = \pm(u^2-v^2)$ and $y = \pm 2uv$; if $x+yi = \pm i(u+vi)^2$ then $x = \mp 2uv$ and $y = \pm(u^2-v^2)$. The proof that $\gcd(u,v)=1$ and $u \not\equiv v \pmod 2$ is as before, or follows from the fact that $u+vi$ and $u-vi$ are coprime in $\mathbb{Z}[i]$.

Other similar equations may be solved by the same method. For example, all primitive solutions to $x^2+2y^2=z^2$ are obtained from $(x,y,z) = (\pm(u^2-2v^2), \pm 2uv, \pm(u^2+2v^2))$. This can be proved using the UFD $\mathbb{Z}[\sqrt{-2}]$ or by elementary means.

4.5. Fermat's Last Theorem.

After our success in finding all solutions to the equation $x^2+y^2=z^2$, it is natural to turn to analogous equation for higher powers. So we ask for solutions in positive integers to the equation

$$x^n + y^n = z^n \qquad \text{with } n \geq 3. \tag{4.5.1}$$

Fermat claimed, in the famous marginal note to his edition of the works of Diophantus, that there are no solutions to (4.5.1). The result is known as *Fermat's Last Theorem*: it is the last of Fermat's unproved claims to be proved (or disproved). Since 1994 it has become possible to state the result as a Theorem:

Theorem 4.5.1. *[Fermat's Last Theorem; Wiles and Taylor–Wiles, 1994] Let $n \geq 3$. Then there are no solutions in positive integers to the equation $x^n+y^n=z^n$.*

The only case which we know that Fermat proved is $n = 4$, which we will prove below. Euler proved the case $n = 3$, using arithmetic in the ring $\mathbb{Z}[\sqrt{-3}]$, though there is some doubt as to the validity of Euler's argument at a crucial step where he tacitly assumed that this ring had unique factorization (which it does not). Subsequent work by Dirichlet, Legendre, Kummer and many others settled many more exponents, at the same time creating most of modern algebraic number theory and algebra. By 1987, the Theorem was known to be true for all $n \leq 150000$. In 1986, an unexpected connection was found, by Frey, between the Fermat equation and another class of Diophantine equation called *Elliptic curves*. A solution to Fermat's equation would lead to the existence of an elliptic curve with properties so strange that they would contradict widely-believed, but then unproved, conjectures about elliptic curves. This connection was proved by Ribet. Finally, Andrew Wiles, with the help of Richard Taylor, proved the elliptic curve conjecture, firmly establishing the truth of Fermat's Last theorem.

We will prove the case $n = 4$ of the theorem.

Theorem 4.5.2. *[Fermat's Last Theorem for exponent 4] The equation $x^4 + y^4 = z^4$ has no solutions in positive integers.*

We will prove a stronger statement: $x^4 + y^4$ cannot be a square, let alone a 4th power:

Theorem 4.5.3. *The equation $x^4 + y^4 = z^2$ has no solutions in positive integers.*

Corollary 4.5.4. *Let $n \in \mathbb{N}$ be a multiple of 4. Then there are no solutions in positive integers to the equation $x^n + y^n = z^n$.*

Now to prove Fermat's Last Theorem in general it suffices to show that the equation $x^p + y^p = z^p$ has no positive integer solutions for each *odd prime* p, since every $n \geq 3$ is divisible either by 4 or by an odd prime, and impossibility for a divisor of n implies impossibility for n itself.

4.6. **Proof of Minkowski's Theorem.** There are several ways to prove Minkowski's Theorem 4.1.3, all of which are based on a continuous analogue of the pigeon-hole principle. We'll use a preliminary result called Blichfeld's Theorem:

Theorem 4.6.1. *[Blichfeld's theorem] Let S be a bounded subset of $\mathbb{R}^n$ whose volume $v(S)$ exists and satisfies $v(S) > m$ for some integer $m \geq 1$. Then there exist $m+1$ distinct points $\underline{x}_0, \underline{x}_1, \ldots, \underline{x}_m \in S$ such that $\underline{x}_i - \underline{x}_j \in \mathbb{Z}^n$ for all i, j.*