Chapter 5

Diophantine Equations

In this chapter, we will give a couple of applications of the number theory we have developed so far:

- the solution of the diophantine equation $x^2 + y^2 = z^2$ (Pythagorean triples),
- Fermat's Last Theorem for the exponent 4;
- and the theorem of Girard[1]- Fermat[2] that primes of the form $4n + 1$ are sums of two squares.

5.1 Fermat's Last Theorem for Exponent 4

The solution of $x^2 + y^2 = z^2$ will help us prove that the diophantine equation

$$X^4 + Y^4 = Z^4 \tag{5.1}$$

has only trivial solutions, namely those with $X = 0$ or $Y = 0$. As a matter of fact, it is a lot easier to prove more, namely that

$$X^4 + Y^4 = Z^2 \tag{5.2}$$

has only trivial solutions (this *is* more: if $X^4 + Y^4$ cannot be a square, it cannot be a fourth power). The proof is quite involved and uses a technique that Fermat called infinite descent.

In a nutshell, the idea behind infinite descent is the following: if we want to prove that a certain diophantine equation is impossible in $\mathbb{N}$, it is sufficient to show that for every solution in natural numbers there is another solution that is "smaller", which eventually leads to a contradiction because there is no natural number smaller than 1.

Here are some simple examples:

[1] Albert Girard (?), 1595 (St Mihiel, France)– 1632 (Leiden, Netherlands)

[2] Pièrre de Fermat, ca. 1607 (Beaumont-de-Lomagne, near Toulouse, France)–1665 (Castres, France)

Proposition 5.1. *The diophantine equation $x^2 + y^2 = 3z^2$ does not have solutions in natural numbers.*

Proof. Assume there are natural numbers $x, y, z > 0$ such that $x^2 + y^2 = 3z^2$. Then $x^2 + y^2 \equiv 0 \pmod 3$. The following table gives the congruence class of $x^2 + y^2$ modulo 3 in terms of x and y:

	0	1	2
0	0	1	1
1	1	2	2
2	1	2	2

Note that, since $2^2 \equiv 1^2 \bmod 3$, the last row and column were actually superfluous. What this table is showing is that if $x^2 + y^2 \equiv 0 \bmod 3$, then $x \equiv y \equiv 0 \bmod 3$. A quicker way of seeing this is provided by the following argument: if $3 \nmid y$, then $x^2 + y^2 \equiv 0 \bmod 3$ implies $(x/y)^2 \equiv -1 \bmod 3$, contradicting the fact that -1 is not a square modulo 3.

Thus $x = 3x_1$ and $y = 3y_1$ for natural numbers x_1, y_1. Now $3z^2 = x^2 + y^2 = 9x_1^2 + 9y_1^2$ implies $z^2 = 3(x_1^2 + y_1^2)$; since the right hand side is divisible by 3, so is the left hand side: $z = 3z_1$ for some integer $z_1 > 0$. But then $9z_1^2 = 3(x_1^2 + y_1^2)$, that is, $x_1^2 + y_1^2 = 3z_1^2$.

We have shown: given any solution (x, y, z) in natural numbers of the equation $x^2 + y^2 = 3z^2$, there is another solution (x_1, y_1, z_1) in natural numbers with $z_1 = z/3$. Repeating this argument gives yet another solution (x_2, y_2, z_2) in natural numbers with $z_2 = z_1/3 = z/9$. Eventually, this will produce a contradiction because natural numbers cannot decrease indefinitely. □

Proposition 5.2. *The equation $x^3 + 3y^3 + 9z^3 = 0$ does not have any solutions in positive integers.*

Proof. Assume that (x, y, z) is a solution in positive integers. Clearly x is divisible by 3, so $x = 3x_1$ for some positive integer x_1. But then $27x_1^3 + 3y^3 + 9z^3 = 0$, hence $9x_1^3 + y^3 + 3z^3 = 0$. Now $y = 3y_1$, and we find $3x_1^3 + 9y_1^3 + z^3 = 0$. Finally, $z = 3z_1$ for some positive integer z_1, and $x_1^3 + 3y_1^3 + 9z_1^3 = 0$.

Thus if (x, y, z) is a solution of the equation $x^3 + 3y^3 + 9z^3 = 0$ in positive integers, then so is $(\frac{x}{3}, \frac{y}{3}, \frac{z}{3})$. Repeating this argument we find that for every positive solution there is a smaller solution in positive integers: but this is nonsense, thus there is no solution in positive integers. □

Proposition 5.3. *The number $\sqrt{2}$ is irrational.*

Proof. Assume not. Then $\sqrt{2} = \frac{m}{n}$ for positive integers m, n, and squaring yields $2n^2 = m^2$. Thus $m = 2p$ is even, and we find $n^2 = 2p^2$. This shows that $n = 2q$ for some positive integer q, hence $2q^2 = p^2$. Thus if $\sqrt{2} = \frac{m}{n}$, then $\sqrt{2} = \frac{p}{q}$ with integers $p = \frac{m}{2}$ and $q = \frac{n}{2}$. Repeating this sufficiently often leads to a contradiction since no positive integer is divisible by 2 infinitely often. □

Fermat used this idea to give a proof of

Theorem 5.4. *The Fermat equation* (5.2) *for the exponent* 4 *does not have any integral solution with* $XYZ \neq 0$.

Proof. Assume that $X, Y, Z \in \mathbb{N} \setminus \{0\}$ satisfy (5.2); we may (and will) assume that these integers are pairwise coprime (otherwise we can cancel common divisors). Now we vaguely follow our solution of the Pythagorean equation: Z must be odd (if Z were even, then X and Y would have to be odd, and we get a contradiction as in the proof of Theorem 5.13).

Thus we may assume that X is odd and Y is even. Since (X^2, Y^2, Z) is a Pythagorean Triple, there exist integers m, n such that $X^2 = m^2 - n^2$, $Y^2 = 2mn$ and $Z = m^2 + n^2$. Clearly $\gcd(m, n)$ divides both X and Y, hence m and n are coprime; moreover, since X is odd, we have $1 \equiv X^2 = m^2 - n^2 \bmod 4$, which implies that m is odd and $n = 2k$ is even. Thus $(Y/2)^2 = mk$ with m and k coprime, hence $m = a^2$ and $k = b^2$, giving $X^2 = a^4 - 4b^4$.

Now we repeat the trick: from $X^2 + 4b^4 = a^4$ we see that $(X, 2b^2, a^2)$ is a Pythagorean triple; thus $X = m_1^2 - n_1^2$, $2b^2 = 2m_1n_1$ and $a^2 = m_1^2 + n_1^2$, where m_1 and n_1 are (necessarily coprime) positive integers. From $m_1n_1 = b^2$ we deduce that $m_1 = r^2$ and $n_1 = s^2$, hence $a^2 = r^4 + s^4$, and we have found a new solution (a, r, s) to our equation $Z^2 = X^4 + Y^4$.

Since $Z = m^2 + n^2 = a^4 + 4b^4$, we find that $0 < a < Z$; this means that for every solution (X, Y, Z) in natural numbers there exists another solution with a smaller Z. This is impossible, so there can't be a nontrivial solution to the Fermat equation in the first place. □

5.2 Fermat's Two-Squares Theorem

A well known theorem first stated by Girard, and probably first proved by Fermat (the first known proof is due to Euler) concerns primes that are sums of two squares, such as $5 = 1^2 + 2^2$ or $29 = 2^2 + 5^2$. The following characterization of such primes is a simple consequence of the notion of congruences; the converse is also true, but much harder to prove.

Proposition 5.5. *If a prime* p *is the sum of two integral squares, then* $p = 2$ *or* $p \equiv 1 \bmod 4$.

Proof. There are 4 residue classes modulo 4; their squares are $[0] = [0]^2$ and $[1] = [1]^2$, and in fact the squares $[2]^2 = [0]$ and $[3]^2 = [1]$ of the remaining classes don't produce new ones.

Now assume that $p = a^2 + b^2$. Since $a^2, b^2 \equiv 0, 1 \bmod 4$, we find that $a^2 + b^2$ must be congruent modulo 4 to one of $0 = 0 + 0$, $1 = 1 + 0 = 0 + 1$, or $2 = 1 + 1$, that is, $p \equiv 0, 1, 2 \bmod 4$. Since no prime is congruent to 0 mod 4, and since 2 is the only prime $\equiv 2 \bmod 4$, we even have $p = 2$ or $p \equiv 1 \bmod 4$ as claimed. □

For the converse, we need to know when $[-1]$ is a square in $\mathbb{Z}/p\mathbb{Z}$ for primes p. Experiments show that $[-1]$ is not a square modulo 3, 7, or 11, and that $[2]^2 = [-1]$ for $p = 5$, and $[5]^2 = [-1]$ for $p = 13$. The general result is

Proposition 5.6. *Let $p \equiv 1 \bmod 4$ be prime; then the congruence $a^2 \equiv -1 \bmod p$ has a solution.*

For the proof, we need some auxiliary results.

Proposition 5.7 (Wilson's Theorem)**.** *For $p > 1$, we have $(p-1)! \equiv -1 \bmod p$ if and only if p is a prime.*

Proof. Let p be a prime; the claim is trivial if $p = 2$, so assume that p is odd. The idea is to look at pairs of the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$. In fact, for every $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ there is an element $a^{-1} \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $a \cdot a^{-1} \equiv 1 \bmod p$. In general, $[a]$ and $[a^{-1}]$ are different: $[a] = [a^{-1}]$ implies $[a^2] = [1]$, so this can only happen (and does in fact happen) if $[a] = [1]$ or $[a] = [-1] = [p-1]$ (here we use that $\mathbb{Z}/p\mathbb{Z}$ is a field; in fields, polynomials of degree 2 such as $x^2 - 1$ have at most 2 roots).

Thus $(\mathbb{Z}/p\mathbb{Z})^\times \setminus \{[-1], [+1]\}$ is the union of pairs $\{[a], [a^{-1}]\}$ with $[a] \neq [a^{-1}]$, hence the product over all elements of $(\mathbb{Z}/p\mathbb{Z})^\times \setminus \{[-1], [+1]\}$ must be $[1]$. We can get $[(p-1)!]$ by multiplying this product with the two missing classes $[1]$ and $[-1]$, and this gives the claimed result $[(p-1)!] = [-1]$.

We still have to prove the converse: assume that $(n-1)! \equiv -1 \bmod n$; if p is a prime divisor of n, this congruence implies $(n-1)! \equiv -1 \bmod p$. But $p < n$ also implies that p occurs as a factor of $(n-1)!$ on the left hand side, hence we would have $0 \equiv (n-1)! \bmod p$. But then $0 \equiv -1 \bmod p$, a contradiction. □

Note that Wilson's theorem provides us with a primality test; unfortunately the only known way to compute $(n-1)!$ is via $n-2$ multiplications, so it takes even longer than trial division!

Proposition 5.8. *Let p be an odd prime and put $a = (\frac{p-1}{2})!$; then we have $a^2 \equiv (-1)^{(p+1)/2} \bmod p$. In particular, $a \equiv \pm 1 \bmod p$ if $p \equiv 3 \bmod 4$, and $a^2 \equiv -1 \bmod p$ if $p \equiv 1 \bmod 4$.*

Proof. We start with Wilson's theorem $(p-1)! \equiv -1 \bmod p$; if, in the product $(p-1)!$, we replace the elements $\frac{p+1}{2}$, $\frac{p+3}{2}$, …, $p-1$ by their negatives $-\frac{p+1}{2} \equiv \frac{p-1}{2}$, $-\frac{p+3}{2} \equiv \frac{p-3}{2}$, …, $-(p-1) \equiv 1 \bmod p$, then we have introduced exactly $\frac{p-1}{2}$ factors -1; thus $(p-1)! \equiv (-1)^{(p-1)/2} a^2 \bmod p$ with $a = (\frac{p-1}{2})!$). This proved the claim. □

Now we can prove Proposition 5.6: if $p \equiv 1 \bmod 4$, then we have just constructed a solution of the congruence $a^2 \equiv -1 \bmod p$. The converse is also true: if p is an odd prime such that $a^2 \equiv -1 \bmod p$ has a solution, then p must be $\equiv 1 \bmod 4$. This will follow from Fermat's Little Theorem.

The solvability of $x^2 \equiv -1 \bmod p$ is the first of two steps in our proof of the Theorem of Girard-Fermat; the second one is a result due to Birkhoff, rediscovered by Aubry, and named after Thue:

Proposition 5.9. *Given an integer a not divisible by p, there exist $x, y \in \mathbb{Z}$ with $0 < |x|, |y| < \sqrt{p}$ such that $ay \equiv x \bmod p$.*

Proof. Let f be the smallest integer greater than $\sqrt{p}$, and consider the residue classes $\{[u+av] : 0 \le u, v < f\}$ modulo p. There are $f^2 > p$ such expressions, but only p different residue classes, hence there must exist u, u', v, v' such that $u + av \equiv u' + av' \bmod p$. Put $x = u - u'$ and $y = v' - v$; then $x \equiv ay \bmod p$, and moreover $-f < x, y < f$. □

Now we can prove

Theorem 5.10 (Girard-Fermat-Euler)**.** *Every prime $p \equiv 1 \bmod 4$ is a sum of two integral squares.*

Proof. Since $p \equiv 1 \bmod 4$, there is an $a \in \mathbb{Z}$ such that $a^2 \equiv -1 \bmod 4$. By Thue's result, there are integers x and y such that $ay \equiv x \bmod p$ and $0 < x, y < \sqrt{p}$. Squaring gives $-y^2 \equiv x^2 \bmod p$, that is, $x^2 + y^2 \equiv 0 \bmod p$. Since $0 < x^2, y^2 < p$, we find $0 < x^2 + y^2 < 2p$; since $x^2 + y^2$ is divisible by p, we must have $x^2 + y^2 = p$. □

5.3 Quadratic Equations

Next we will apply the Unique Factorization Theorem to the solution of the diophantine equation

$$x^2 + y^2 = z^2$$

in integers $x, y, z \in \mathbb{Z}$. Such triples of solutions are called Pythagorean[3] triples. The most famous of these triples is of course $(3, 4, 5)$. It is quite easy to give formulas for producing such triples: for example, take $x = 2mn$, $y = m^2 - n^2$ and $z = m^2 + n^2$ (special cases were known to the Babylonians, the general case occurs in Euclid). It is less straightforward to verify that there are no other solutions (this was first done by the Arabs in the 10th century).

Assume that (x, y, z) is a Pythagorean triple. If d divides two of these, it divides the third, and then $(x/d, y/d, z/d)$ is another Pythagorean triple. We may therefore assume that x, y and z are pairwise coprime; such triples are called primitive. In particular, exactly one of them is even.

Claim 1. The even integer must be one of x or y. In fact, if z is even, then x and y are odd. Writing $x = 2X + 1$, $y = 2Y + 1$ and $z = 2Z$, we find $4X^2 + 4X + 4Y^2 + 4Y + 2 = 4Z^2$: but the left hand side is not divisible by 4: contradiction.

Exchanging x and y if necessary we may assume that x is even. Now we transfer the additive problem $x^2 + y^2 = z^2$ into a multiplicative one (if we are to use unique factorization, we need products, not sums) by writing $x^2 = z^2 - y^2 = (z - y)(z + y)$.

Claim 2. $\gcd(z - y, z + y) = 2$. In fact, put $d = \gcd(z - y, z + y)$. Then d divides $z - y$ and $z + y$, hence their sum $2z$ and their difference $2y$. Now $\gcd(2y, 2z) = 2\gcd(y, z) = 2$, so $d \mid 2$; on the other hand, $2 \mid d$ since $z - y$ and $z + y$ are even since z and y are odd. Thus $d = 2$ as claimed.

This is the point where Unique Factorization comes in:

[3] Pythagoras of Samos (ca. 569 – 475 BC.).

Proposition 5.11. *Let $a, b \in \mathbb{N}$ be coprime integers such that ab is a square. Then a and b are squares.*

Proof. Write down the prime factorizations of a and b as

$$a = p_1^{a_1} \cdots p_r^{a_r}, \quad b = q_1^{b_1} \cdots q_s^{b_s}.$$

Now a and b are coprime, so the set of p_i and the set of q_j are disjoint, and we conclude that the prime factorization of ab is given by

$$ab = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}.$$

Since ab is a square, all the exponents in the prime factorization of ab must be even. This implies that the a_i and the b_j are even, therefore a and b are squares. □

Corollary 5.12. *Let $a, b \in \mathbb{N}$ be integers with $\gcd(a, b) = d$ such that ab is a square. Then a/d and b/d are squares.*

Proof. Apply the proposition to the pair a/d and b/d. □

Applying the corollary to the case at hand (and observing that $z - y \in \mathbb{N}$, since $z + y > 0$ and $(z - y)(z + y) = x^2 > 0$) we find that there exist $m, n \in \mathbb{N}$ such that $z - y = 2n^2$ and $z + y = 2m^2$. Adding and subtracting these equations gives $z = m^2 + n^2$ and $y = m^2 - n^2$, and from $x^2 = (z - y)(z + y) = m^2 n^2$ and $x \in \mathbb{N}$ we deduce that $x = 2mn$.

Note that we must have $\gcd(m, n) = 1$: in fact, any common divisor of m and n would divide x, y and z contradicting our assumption that our triple be primitive. We have shown:

Theorem 5.13. *If (x, y, z) is a primitive Pythagorean triple with x even, then there exist coprime integers $m, n \in \mathbb{N}$ such that $x = 2mn$, $y = m^2 - n^2$ and $z = m^2 + n^2$.*

Note that if y is even, then the general solution is given by $x = m^2 - n^2$, $y = 2mn$ and $z = m^2 + n^2$. Moreover, if we drop the condition that the triples be primitive then the theorem continues to hold if we also drop the condition that the integers m, n be relatively prime.

Lagrange's Trick

The same technique we used for solving $x^2 + y^2 = z^2$ can be used to solve equations of the type $x^2 + ay^2 = z^2$: just write the equation in the form $ay^2 = (z - x)(z + x)$ and use unique factorization.

Equations like $x^2 + y^2 = 2z^2$ at first seem intractable using this approach because we can't produce a difference of squares. Lagrange, however, saw that in this case multiplication by 2 saves the day because $(2z)^2 = 2x^2 + 2y^2 = (x + y)^2 + (x - y)^2$, hence $(2z - x - y)(2z + x + y) = (x - y)^2$, and now the solution proceeds exactly as for Pythagorean triples.

Let us now show that we can do something similar for any equation of type $AX^2 + BY^2 = CZ^2$ having at least one solution. First, multiplying through by A shows that it is sufficient to consider equations $X^2 + aY^2 = bZ^2$. Assume that (x, y, z) is a solution of this equation. Then

$$\begin{aligned}(bzZ)^2 &= bz^2X^2 + abz^2Y^2 \\ &= (x^2 + ay^2)X^2 + (ax^2 + a^2y^2)Y^2 \\ &= (xX + ayY)^2 + a(yX - xY)^2.\end{aligned}$$

Thus $a(yX - xY)^2 = (bzZ)^2 - (xX + ayY)^2$ is a difference of squares, and we can proceed as for Pythagoren triples. We have proved:

Theorem 5.14. *If the equation $ax^2 + by^2 = cz^2$ has a nontrivial solution in integers, then this equation can be factored over the integers (possibly after multiplying through by a suitable integer).*

Exercises

5.1 Solve the diophantine equation $x^2 + 2y^2 = z^2$.

5.2 Solve the diophantine equation $x^2 - 2y^2 = z^2$.

5.3 Solve the diophantine equation $x^2 + y^2 = 2z^2$.

5.4 Solve the diophantine equation $x^2 - y^2 = 3$.

5.5 Prove that each odd prime p can be written as a difference of squares of natural numbers ($p = y^2 - x^2$ for $x, y \in \mathbb{N}$) in a unique way.

5.6 Fermat repeatedly challenged English mathematicians by sending them problems he claimed to have solved and asking for proofs. Two of them were the following that he sent to Wallis:

- Prove that the only solution of $x^2 + 2 = y^3$ in positive integers is given by $x = 5$ and $y = 3$;
- Prove that the only solution of $x^2 + 4 = y^3$ in positive integers is given by $x = 11$ and $y = 5$.

In a letter to his English colleague Digby, Wallis called these problems trivial and useless, and mentioned a couple of problems that he claimed were of a similar nature:

- $x^2 + 12 = y^4$ has unique solution $x = 2$, $y = 2$ in integers;
- $x^4 + 9 = y^2$ has unique solution $x = 2$, $y = 5$ in integers;
- $x^3 - y^3 = 20$ has no solution in integers;
- $x^3 - y^3 = 19$ has unique solution $x = 3$, $y = 2$ in integers.

When Fermat learned about Wallis's comments, he called Wallis's problems mentioned above "amusements for a three-day arithmetician" in a letter to Digby. In fact, while Fermat's problems were hard (and maybe not even solvable using the mathematics known in his times), Wallis's claims are easy to prove. Do this.

5.7 Assume that $ab = rx^n$ for $a, b, r, x \in \mathbb{N}$ and $\gcd(a, b) = 1$. Show that there exist $u, v, y, z \in \mathbb{N}$ such that $a = uy^n$, $b = vz^n$, and $uv = r$.

5.8 Use infinite descent to prove that $\sqrt{3}$ is irrational.

5.9 Let p be a prime; show that $x^3 + py^3 + p^2z^3 = 0$ does not have a solution.