Chapter 7
Diophantine Equations

Diophantine equations, i. e., equations with integer coefficients for which integer solutions are sought, are among the oldest subjects in mathematics. Early historical occurrences often appeared in the guise of *puzzles*, and perhaps for that reason, Diophantine equations have been largely neglected in our mathematical schooling. Ironically, though, Diophantine equations play an ever-increasing role in modern applications, not to mention the fact that some Diophantine problems, especially the unsolvable ones, have stimulated an enormous amount of mathematical thinking, advancing the subject of number theory in a way that few other stimuli have.

Here we shall deal with some of the basic facts and rules and get to know *triangular* and *Pythagorean numbers, Fermat's Last Theorem*, an unsolved conjecture by *Goldbach*, and another conjecture by *Euler* – one that was refuted, although it looked quite convincing while it lasted.

7.1 Relation with Congruences

The congruence

$$ax \equiv c \pmod{m} \tag{7.1}$$

has a solution *iff* $(a,m) \mid c$. In fact, there are then (a,m) solutions that are incongruent modulo m [7.1].

Example:

$$3x \equiv 9 \pmod{6}. \tag{7.2}$$

With $(3,6) = 3$ and $3 \mid 9$, there are exactly three incongruent solutions: $x = 1$, 3 and 5. Adding or subtracting multiples of 6 to these three solutions gives additional solutions *congruent* to the three already found (7, 9, 11, 13, etc.).

For $(a,m) = 1$, the solution is *unique* modulo m.

M. Schroeder, *Number Theory in Science and Communication*, 5th ed.,
DOI 10.1007/978-3-540-85298-8_7, © Springer-Verlag Berlin Heidelberg 2009

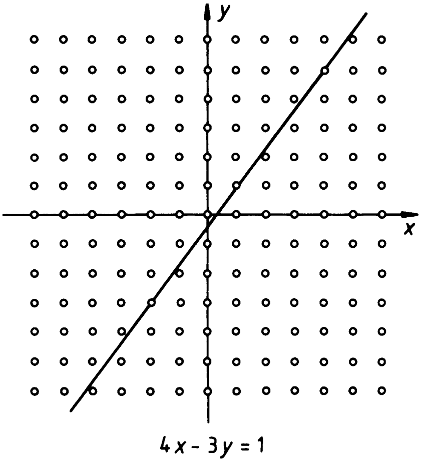

Fig. 7.1 Linear Diophantine equations have simple geometric interpretations: the straight line $3y = 4x - 1$ cuts through points $\{-2, -3\}$ and $\{4, 5\}$, two solutions of the equation

The solution of the congruence $ax \equiv c \pmod{m}$ is identical with solutions in integers x and y of the *Diophantine equation* [7.1]:

$$ax = my + c, \tag{7.3}$$

so named after Diophantus of Alexandria (ca. A. D. 150) [7.2].

For $(a, m) = d$ and $m = m'd$, $a = a'd$ and $c = c'd$ [note that (a, m) must divide c for a solution to exist], we can write instead of the above equation

$$a'x = m'y + c', \tag{7.4}$$

whose solution is unique modulo m', because $(a', m') = 1$. Additional solutions that are incongruent modulo m are obtained by adding km', where $k = 1, 2, \ldots, d - 1$.

Diophantine equations also have a geometric interpretation, which is illustrated for $3y = 4x - 1$ in Fig. 7.1. The straight line representing this equation goes through only those points of the two-dimensional integer lattice shown in Fig. 7.1 for which x and y are solutions. In the illustration this is the case for the points $\{x, y\} = \{-2, -3\}$, $\{1, 1\}$ and $\{4, 5\}$. Additional solutions are obviously given by linear extrapolation with multiples of the difference $\{4, 5\} - \{1, 1\} = \{3, 4\}$.

7.2 A Gaussian Trick

For $(b, m) = 1$, *Gauss* [7.3] suggested writing the congruence $bx \equiv c \pmod{m}$ as

$$x \equiv \frac{c}{b} \pmod{m} \tag{7.5}$$

and adding or subtracting multiples of m to c and b so that cancellation becomes possible *as if* c/b were, in fact, a fraction.

Example: $27x \equiv 1 \pmod{100}$.

Solution:

$$x \equiv \frac{1}{27} \equiv \frac{-99}{27} \equiv \frac{-11}{3} \equiv \frac{-111}{3} \equiv -37 \equiv 63 \pmod{100}.$$

Check: $27 \cdot 63 = 1701 \equiv 1 \pmod{100}$. Check!

Another method uses Euclid's algorithm (Sect. 2.7) for solving congruences or Diophantine equations. A congruence is first converted into a Diophantine equation. For example, the congruence

$$15x \equiv 1 \pmod{11} \tag{7.6}$$

has a solution, because $(15,11) = 1$ divides 1. The corresponding Diophantine equation is

$$15x = 11y + 1. \tag{7.7}$$

Solving for y, we obtain

$$y = x + \frac{4x-1}{11}. \tag{7.8a}$$

For (7.8a) to have an integer solution $4x - 1$ must be a multiple of 11:

$$4x - 1 = 11w.$$

Now solving for x, we get

$$x = 2w + \frac{3w+1}{4}. \tag{7.8b}$$

By now, the denominator has become so small that a solution is obvious: for x to be an integer, $3w + 1$ must be a multiple of 4, for example $w = 1$. Or, more formally:

$$3w + 1 = 4v,$$

whence

$$w = v + \frac{v-1}{3}. \tag{7.8c}$$

Here an integer solution is even more obvious: $v = 1$.

Solutions for x and y are now obtained by *backward* substitutions: with $v = 1$, (7.8c) gives $w = 1$ (as we noted before); and with $w = 1$, (7.8b) gives $x = 3$ and finally, if we so desire, (7.8a) gives $y = 4$.

Check: $15 \cdot 3 = 11 \cdot 4 + 1 = 45 \equiv 1 \pmod{11}$. Check!

The trick of this method of solution is that, in going from (7.8a) to (7.8b) and (7.8c), we have made the denominators smaller and smaller – just as in the Euclidean algorithm. In fact, the Euclidean algorithm applied to $15/11$, the original factors in

(7.7), gives precisely the emainders and denominators as appear in the equations (7.8a–c):

$$\begin{aligned} 15:11 &= 1+\frac{4}{11} \\ 11:4 &= 2+\frac{3}{4} \\ 4:3 &= 1+\frac{1}{3}. \end{aligned}$$

For numerous calculations with the same modulus, it is most convenient to calculate a *table* of inverses once and for all. Such a table for the modulus 11 would contain, for example, the entry $4^{-1} = 3$. Check: $4 \cdot 3 = 12 \equiv 1 \pmod{11}$. Check!

Thus, the solution of $4x \equiv 7 \pmod{11}$ becomes $x \equiv 4^{-1} \cdot 7 = 21 \equiv 10 \pmod{11}$. Check: $4 \cdot 10 = 40 \equiv 7 \pmod{11}$. Check!

7.3 A Stamp Problem

Suppose you have an unlimited supply of 26-cent and 41-cent postage stamps. Which postage amounts can you cover exactly? Obviously, the smallest amounts that are covered (26, 41, 52, 78, 82 cents etc) have sizeable gaps that cannot be covered (1 to 25 cents, 27 to 40 cents etc.) But for larger amounts, these gaps get smaller and smaller. Thus, the question arises whether there is an amount after which *all* postages can be covered. An answer to this question (not in this guise, of course) was provided by the English mathematician J. Sylvester in 1884, who showed that for two kinds of stamps whose different values, a and b, are relatively prime, the critical amount is $(a-1)(b-1)$, or 1000 cents for $a = 26$ and $b = 41$ cents. Let us see whether there is a solution for $26x + 41y \equiv 1000$ as promised by Sylvester. First we solve the standard linear Diophantine equation.

$$26x + 41y = 1$$

Using the (Euclidean) algorithm described in this section, we find $x = -11$ and $y = 7$ Check:

$$-11 \cdot 26 \div 7 \cdot 41 = 1$$

(Alternatively, the solution can be found with the Mathematica^{TM} command “Extended GCD” which does Euclid’s algorithm for you.)

To get the solution for 1000, we multiply the solution for 1 by 1000 and add (subtract) k 26 41 to the first (second) term:

$(-11000 + k41)26 + (7000 - k - 26)41 = 1000$ For the factor of 26 to become positive k has to exceed 268. For k = 269 we get

$$29 \cdot 26 + 6 \cdot 41 = 1000$$

for the basic solution.

For the 1001 we simply add the basic solution $-11\cdot 26+7\cdot 41=1$ to yield

$$18\cdot 26+13\cdot 41=1001$$

and similarly for 1002:

$$7\cdot 26+20\cdot 41=1002.$$

Proceeding in the same manner we would get for 1003

$$-4\cdot 26+27\cdot 41=1003$$

Of course, there are no negative postages, but by adding (subtracting) $26\cdot 41$ to the first (second) term we get

$$37\cdot 26+1\cdot 41=1003$$

This procedure can be continued indefinitely for all higher postages. But what about 999? By subtracting our basic solution ($-11\cdot 26+7\cdot 41=1$) from the one for 1000 we obtain

$$40\cdot 26-1\cdot 41=999$$

Again we run into a negative postage, but this time there is no way out. We are stuck By adding $26\cdot 41$ to the second term to make it positive while subtracting $26\cdot 41$ from the first summand, we get

$$-1\cdot 26+25\cdot 41=999$$

But now we need a negative 26-cent stamp. In other words the postage 999 cents cannot be covered by 26-cent and 41-cent stamps. In fact, 1000 cents is the smallest postage after which all higher postages can be realized. According to Sylvester this crossover should occur at (a-1)(b-1) or, for a = 26 and b = 41, at $25\times 40=1000$. The interested reader may want to prove this result for general coprime a and b.

Unfortunately, there is no simple formula for the largest impossible amount for three or more postages. This was shown to be a NP-hard problem (see B. Cipra: "Exact Postage Poser Still Not Licked" in *Science* Vol. **319**, page. 899).

With an unlimited supply of 26-cent and 41-cent stamps 500 postages (between 1 cent and 999 cents) cannot be covered. Suppose the post office decides to issue a third stamp, which value (above 41 cents) should it be given to minimize the number of uncovered postages? The surprising answer is 42 cents, which leaves only 152 postages uncovered. If values above 26 cents are considered, the optimum stamp value is 32 cents, which leaves just 134 postages uncovered. Of course, some of those choices require a lot of stamp licking.

The stamp problem described here is related to the work (on linear forms with integer coefficients) of the German mathematician F.G. Frobenius (1849–1917), a student of Kronecker, Kummer and Weierstrass in Berlin. He was the teacher of Edmund Landau and Issai Schur to mention only the two most famous alummi.

7.4 Nonlinear Diophantine Equations

A simple example of a nonlinear Diophantine equation is

$$x^2 - Ny^2 = \pm 1, \tag{7.9}$$

where x and y are integers. Two solutions for $+1$ on the right-hand side (the so-called Pell equation) are obviously $x = \pm 1$, $y = 0$. Are there others? For $N = 2$,

$$x^2 - 2y^2 = \pm 1 \tag{7.10}$$

has the solution $x = \pm 3$, $y = \pm 2$. Are there more? Yes, and they are obtained by the continued-fraction (CF) expansion of $\sqrt{N}$. For $n = 2$, we have

$$\sqrt{2} = 1 + \sqrt{2} - 1, \tag{7.11}$$

$$\frac{1}{\sqrt{2}-1} = 2 + \sqrt{2} - 1, \tag{7.12}$$

i. e., as we already know, we obtain the periodic CF:

$$\sqrt{2} = \left[1;\overline{2}\right]. \tag{7.13}$$

The approximants A_k and B_k are thus obtained recursively from

$$A_k = 2A_{k-1} + A_{k-2}, \tag{7.14}$$

and similarly for the B_k. With the initial conditions $A_0 = A_1 = 1$ and $B_0 = 0$, $B_1 = 1$, we obtain

$$\begin{aligned} A_k &= 1,\ 1,\ 3,\ 7,\ 17,\ 41,\ 99, \ldots \\ B_k &= 0,\ 1,\ 2,\ 5,\ 12,\ 29,\ 70, \ldots . \end{aligned} \tag{7.15}$$

Here each pair of values (A_k, B_k) corresponds alternately to a solution of $x^2 - 2y^2 = 1$ and $x^2 - 2y^2 = -1$. This is not really too surprising, because we already know that A_k/B_k will tend to $\sqrt{2}$ alternately from above and below. However, the general proof is a bit tedious [7.1].

The first two solutions $\{1,0\}$ and $[1,1]$ we already know. We will check the third and fourth solutions: $7^2 - 2 \cdot 5^2 = -1$. $17^2 - 2 \cdot 12^2 = 1$. Check!

The CF's of the squareroots of integers are not only periodic; they are also palindromic, i. e., the periods are symmetric about their centres, except for the last number of the period, which equals twice the very first number (left of the semicolon). For example, $\sqrt{29} = [5;\overline{2,1,1,2,10}]$ or $\sqrt{19} = [4;\overline{2,1,3,1,2,8}]$.

Some periods are very short, such as those of numbers of the form $n^2 + 1$, which have period length 1. For example, $\sqrt{10} = [3;\overline{6}]$ or $\sqrt{101} = [10;\overline{20}]$. But the squareroots of other integers can have rather long periods. For example, $\sqrt{61} = [7;\overline{1,4,3,1,2,2,1,3,4,1,14}]$ has a period length of 11, and $\sqrt{109}$ has a period length of 15. There seems to be no simple formula that predicts long-period lengths.

Solving Pell's equation for such integers is quite tedious, a fact that Fermat exploited when he wrote his friend Frénicle in 1657, rather mischievously, to try $N = 61$ and $N = 109$ "pour ne vous donner pas trop de peine". (The *smallest* solution of the latter problem has 14 and 15 decimal places, respectively. Poor Frénicle!)

7.5 Triangular Numbers

The *k*th *triangular number* is defined as

$$\Delta_k = 1 + 2 + \ldots + k = \tfrac{1}{2}k(k+1). \tag{7.16}$$

Δ_k is the number of unordered pairs of $k+1$ objects or, more tangibly, the number of handshakings when $k+1$ persons meet (no self-congratulations, please!). The smallest Δ_k are 0, 1, 3, 6, 10, 15, ... Their first differences form a linear progression: 1, 2, 3, 4, 5, ...

On July 10, 1796, Gauss wrote in his still very fresh diary (then in its 103rd day):

$$\text{Eureka!} \quad n = \Delta + \Delta + \Delta, \tag{7.17}$$

by which he meant that every integer can be represented by the sum of 3 triangular numbers. For example, $7 = 3 + 3 + 1 = 6 + 1 + 0$; $8 = 6 + 1 + 1$; $9 = 3 + 3 + 3 = 6 + 3 + 0$; $10 = 6 + 3 + 1$, etc. What this means is that the Δ_k, although they grow like $k^2/2$, are still distributed densely enough among the integers that three of them suffice to reach any (nonnegative) whole number.

Gauss's discovery implies that every integer of the form $8n + 3$ as a sum of three odd squares, an interesting *nonlinear* Diophantine equation, is always solvable. First we note that the square of an odd number, $2k+1$, equals 8 times a triangular number plus 1:

$$(2k+1)^2 = 4k^2 + 4k + 1 = 8\Delta_k + 1. \tag{7.18}$$

Hence if

$$n = \Delta_{k_1} + \Delta_{k_2} + \Delta_{k_3},$$

then we obtain, in view of Gauss's Eureka discovery, a solution to the following nonlinear Diophantine equation:

$$\sum_{m=1}^{3} (2k_m + 1)^2 = 8n + 3. \tag{7.19}$$

Example: $35 = 4 \cdot 8 + 3 = 1 + 9 + 25$.

Finally, there is a connection with the perfect numbers P_p: every even perfect number is also a triangular number:

$$P_p = (2^p - 1)2^{p-1} = (2^p - 1)2^p \tfrac{1}{2} = \Delta_{2^p - 1}. \tag{7.20}$$

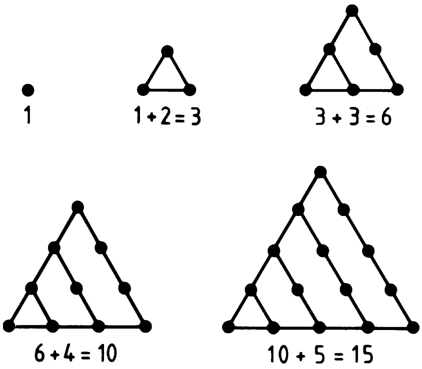

Fig. 7.2 Geometrical interpretation of the triangular numbers (and the reason for their name). Note the simple recursion

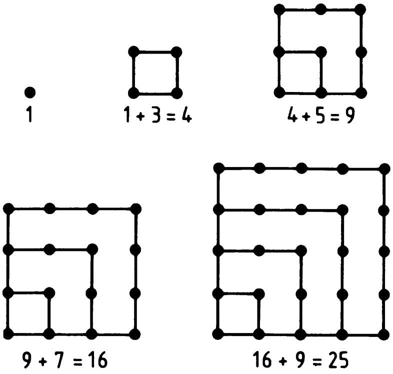

Fig. 7.3 The square numbers, their geometrical interpretation and their recursion

Triangular numbers can also be illustrated *geometrically* as the number of equidistant points in triangles of different sizes (Fig. 7.2). They were defined this way in antiquity (by the Pythagoreans). These points form a triangular lattice.

In a generalization of this concept, *square numbers* are defined by the number of points in square lattices of increasing size, as illustrated in Fig. 7.3.

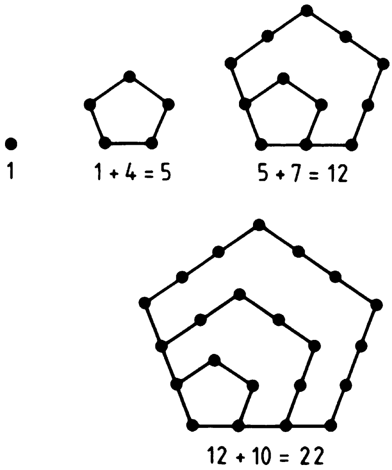

Fig. 7.4 The pentagonal numbers, their geometrical interpretation and their recursion. The pentagonal numbers, $n(3n-1)/2$, also play a role in partitioning problems (see Chap. 22)

Higher n-gonal or *figurate* numbers, such as pentagonal numbers (Fig. 7.4) and hexagonal numbers, are defined similarly. Can the reader derive the general formula for figurate numbers? Calling the kth (beginning with $k = 0$) n-gonal number $g_n(k)$, the answer is

$$g_n(k) = \tfrac{1}{2}(n-2)k^2 + \tfrac{1}{2}nk + 1, \tag{7.21}$$

which for $n = 4$ gives the square numbers $g_4(k) = (k+1)^2$. Check!

7.6 Pythagorean Numbers

Another nonlinear Diophantine equation is the well-known

$$x^2 + y^2 = z^2, \tag{7.22}$$

expressing Pythagoras's theorem for right triangles. Solutions in integers are called Pythagorean *triplets*, the smallest positive one being 4, 3, 5:

$$4^2 + 3^2 = 5^2.$$

To avoid redundancy, we shall require x to be even and y to be odd. (If both x and y were even, then z would also be even and the equation could be divided by 4.) All *basic* solutions, i. e., those for which x, y and z do not have a common divisor and x is even, are obtained from the two coprime integers m and n, $m > n > 0$, at least one of which must be even, as follows:

$$\begin{aligned} x &= 2mn \\ y &= m^2 - n^2 \\ z &= m^2 + n^2. \end{aligned} \tag{7.23}$$

It is easy to verify that $x^2 + y^2 = z^2$ and that x is even and $y > 0$ is odd. Of course, z is also odd.

With these conventions, the first case is $m = 2$, $n = 1$, yielding the triplet $(4,3;5)$. The next basic case is $m = 3$, $n = 2$, yielding $(12,5;13)$. The third basic case, $m = 4$, $n = 1$, yields $(8,15;17)$.

Incidentally, at least one pair of basic Pythagorean triples has the same product xy, meaning that there are (at least) two incongruent right triangles with integer sides and equal areas:

$$\begin{aligned} m = 5, \quad n = 2 &: (20,21;29) \\ m = 6, \quad n = 1 &: (12,35;37) \end{aligned} \tag{7.24}$$

both of which have area 210. Are there other equal-area pairs?

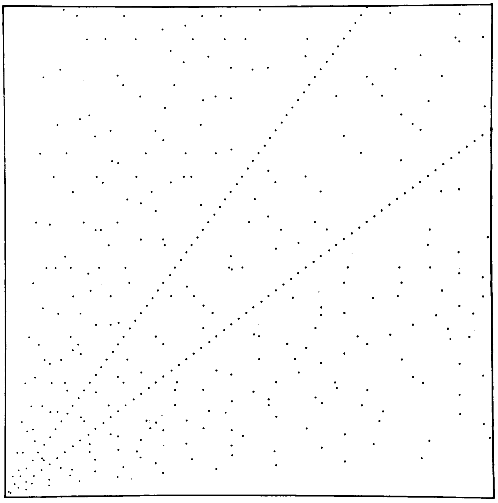

Fig. 7.5 The Pythagorean numbers $x^2+y^2=z^2$ in the range $1 \leq x \leq 52$, $1 \leq y \leq 52$. The two prominent straight "lines" correspond to the basic triplet $4^2+3^2=5^2$, the triplet $3^2+4^2=5^2$ and their multiples

Figure 7.5, prepared by Suzanne Hanauer of Bell Laboratories, shows the x and y values of all (not just the basic) Pythagorean triplets up to $x,y=52$. The two pronounced straight "lines" are the solutions obtained from the basic triplet $(3,4;5)$. Each plotted point in Fig. 7.5 is one corner of an integer right triangle obtained by connecting it with the origin $\{0,0\}$ and drawing the normal to the abscissa through it. It is apparent that there is a certain "thinning out" as x and y get larger.

7.7 Exponential Diophantine Equations

Another type of Diophantine equation, in which the unknowns appear in the exponent is exemplified by

$$2^n = 3^m - 1. \qquad (7.25)$$

The background against which the author encountered this equation is the following. The Fast Fourier Transform (FFT) works most efficiently for data whose length is a power of 2. On the other hand, pseudorandom "maximum-length" sequences, which are ideal for precision measurements (see Chap. 27), have period lengths $p^m - 1$, where p is a prime. In most applications, the preferred sequences are binary, i. e., $p=2$. Of course, there is no integer solution to the equation $2^n = 2^m - 1$, except the uninteresting one $n=0$, $m=1$.

For some physical applications, ternary-valued sequences would also be acceptable. Thus, the question arises whether the equation $2^n = 3^m - 1$ has integer solutions other than the two obvious ones $n=1$, $m=1$ and $n=3$, $m=2$.[1] Lewi Ben Gerson (1288–1344) proved that these are indeed the only solutions.

[1] In fact, in 1844 *Catalan* [7.4] posed a more general question and conjectured that 2^3 and 3^2 are the only perfect powers that differ by 1.

7.8 Fermat's Last "Theorem"

Perhaps the most famous Diophantine equation is

$$x^n + y^n = z^n, \qquad (n > 2) \tag{7.26}$$

for which Fermat asserted that no nontrivial $(xyz \neq 0)$ solution in integers exists. Fermat thought he had a proof, but this seems more than doubtful after centuries of vain efforts by some of the greatest mathematicians who came after Fermat.

Some special cases for n are relatively easy to prove, for example the quartic case, $n = 4$. The cubic case, $n = 3$, was solved by Euler. Sophie Germain in Paris, who mailed her proof to Gauss in Göttingen under the male pseudonym of Monsieur Le Blanc [7.5], showed Fermat's Last Theorem to be likely true for all odd primes p such that $2p+1$ is also prime. These primes are now called Sophie Germain primes, the smallest being $p = 3$.

The greatest breakthrough (as some would say today) was made in 1851 by the German mathematician Ernst Eduard Kummer. He showed that Fermat's Last Theorem (FLT) was true for what he called regular primes p_r, defined as those primes which do not divide any of the numerators of the Bernoulli numbers B_k up to B_{p_r-3} [7.6].

The only irregular primes below 100 are 37, 59, and 67, i. e., three primes out of 25. It is believed that the asymptotic fraction of the irregular primes tends toward $1 - 1/\sqrt{\mathrm{e}} = 0.393469\ldots$. Thus, there would be an infinity of irregular primes, roughly 40 % of all primes. This is in stark contrast to the Fermat primes, of which only 5 are presently known.

In 1908 the Göttingen Academy of Sciences established the Wolfskehl Prize to the tune of 100,000 (gold!) marks for proving FLT. In 1958, two World Wars later, this was reduced to 7,600 Deutsche Mark, but FLT had still not been proved or disproved. By 1976, it had been shown to be correct for all prime exponents smaller than 125,000.

If the proof of FLT has proved so difficult, perhaps the theorem is just not true, and one should look for a counterexample. (One counterexample, of course, would suffice to demolish FLT once and for all.) But unfortunately, since the exponent n has to be larger than 125000, and it can also be shown that x must be greater than 10^5, any counterexample would involve numbers *millions* of decimal digits long [7.7]. Hence the counterexample route seems closed, even if FLT was false. Consequently, we will have to conclude, more than 300 years after its somewhat offhand assertion, that FLT will probably never be disproved. However work on the FLT has led to some profound mathematical insights and innovations.

In the meantime, the "impossible" *has* happened and Fermat's Last Theorem has been proved. Although the proof, presented by Andrew Wiles on 23 June 1993, was still defective, all holes, even the most recalcitrant ones, have been closed with the collaboration of Richard Taylor. The proposition proved by Wiles and Taylor is the main part of the Shimura-Taniyama-Weil conjecture related to elliptic curves $y^2 = x^3 + ax + b$ [7.8].

In the summer of 1997 the Göttingen Academy of Sciences, after due consideration of the published proof, is expected to award Wiles the Wolfskehl Prize, which now amounts to about 70,000 Marks.

FLT, although for long the most famous unsolved case, is not an isolated quirk. Another seemingly unprovable (but probably false) conjecture is the following one by Georg Cantor: All numbers generated by the recursion

$$p_{n+1} = 2^{p_n} - 1, \quad \text{with} \quad p_0 = 2 \tag{7.27}$$

are prime. The first Cantor numbers after 2 are $p_1 = 3$, $p_2 = 7$, $p_3 = 127$ and $p_4 = 2^{127} - 1$, all of which are (Mersenne) primes. Unfortunately, little is known about the next Cantor number, p_5, other than that it has more than 5×10^{37} decimal digits! (This should not be confounded with the large – but "infinitely" smaller – number 5×10^{37}, which has only 38 digits.) Nevertheless, with the latest advances in primality testing (see Chap. 12) perhaps the primality of p_5 can be confirmed – or refuted, thereby demolishing another conjecture. (Note: if p_m is composite, then *all* p_n, $n \geq m$ are composite – see Sect. 3.5).

One of the perennial conjectures is the famous *Goldbach conjecture*, asserting that every even number > 2 is the sum of two primes. Some progress has been made on related weaker assertions, and the Goldbach conjecture itself has been *numerically* confirmed up to very large numbers. But alas, even if it had been shown to hold up to $10^{10^{10}}$, there would be no guarantee that it would not fail for $10^{10^{10}} + 2$. See Sect. 4.13 for some numerical results and an heuristic estimate.

7.9 The Demise of a Conjecture by Euler

Euler conjectured that (excepting trivial cases)

$$x_1^n + x_2^n + \ldots + x_k^n = z^n \tag{7.28}$$

has nontrivial integer solutions *iff* $k \geq n$. For $n = 3$ and $k = 2$, Euler's conjecture corresponds to the proven case $n = 3$ of FLT: the sum of 2 cubes cannot be another cube. For $n = 3$ and $k = 3$, (7.28) asserts that the sum of *three* cubes can be another cube. Euler's conjecture stood for two centuries but fell in 1966 to the joint effort of Lander and Parkin, who found a counterexample for $n = 5$:

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5, \tag{7.29}$$

which can be verified with a good pocket calculator (and which Euler himself could have done in his head).

Thus Fermat was avenged, whose fifth "prime" Euler had shown to be composite.

In fact, in 1987 Noam Elkies, a Harvard graduate student, found a first case where only *three* fourth powers are needed to get another fourth power. A year later, R. Frye found a solution in which the sum of three fourth powers equals 422481^4.

Another, more difficult problem that has also been successfully tackled, is the Diophantine equation

$$\mathrm{a}^4+\mathrm{b}^4+\mathrm{c}^4+\mathrm{d}^4=(\mathrm{a}+\mathrm{b}+\mathrm{c}+\mathrm{d})^4.$$

(See *The American Mathematical Monthly*, March 2008).

7.10 A Nonlinear Diophantine Equation in Physics and the Geometry of Numbers

In 1770, Lagrange proved that “the set of squares is a basis of order 4”. This means that *every* positive integer can be represented as the sum of 4 squares. If we allow ourselves just 3 squares, then some integers cannot be so represented.

Which integers n can be expressed as the sum of 3 squares? The author first encountered this problem in the formula for the resonant frequencies of a cube-shaped resonator, which in units of the lowest resonant frequency are:

$$f_{x,y,z}^2=x^2+y^2+z^2. \tag{7.30}$$

An important question in some areas of physics is whether $f_{x,y,z}^2$ can take on all positive integer values or whether there are gaps. (This problem occurred in the author’s Ph.D. thesis on normal-mode statistics.) To answer this question let us consider the complete residue system modulo 8:

$$r=0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7. \tag{7.31}$$

Hence,

$$r^2\equiv 0,\ 1\quad\text{or}\quad 4\pmod 8.$$

Thus, the sum of 3 squares modulo 8 is precisely those numbers that can be generated by adding 3 of the integers 0, 1, 4 (with repetition allowed). This is possible for integers 0 through 6, but *not* 7. Thus, certainly,

$$x^2+y^2+z^2\neq 8m+7. \tag{7.32}$$

However, it can be shown that these “forbidden” numbers, when multiplied by a nonnegative power of 4, are also not possible as the sum of 3 squares [7.1]. In fact,

$$x^2+y^2+z^2=n \tag{7.33}$$

has a solution in integers *iff*

$$n\neq 4^k(8m+7),\qquad k\geq 0. \tag{7.34}$$

This means that on average, the fraction

$$\frac{1}{8}+\frac{1}{4\cdot 8}+\frac{1}{16\cdot 8}+\ldots=\frac{1}{6} \tag{7.35}$$

of all integers cannot be represented as the sum of 3 squares.

Since any positive integer n can be represented by a sum of 4 squared integers, it is interesting to ask how many ways $r_2(n)$ a given n can be so represented. The answer (due to Jacobi), including permutation, signs and 0's, is

$$r_2(n)=8\sum_{d|n,4\not{|}d} d, \tag{7.36}$$

i. e., 8 times the sum of the divisors of n that are not divisible by 4.

Example: $r_2(4)=8(1+2)=24$. Check:

$$\begin{aligned}
&4=(\pm1)^2+(\pm1)^2+(\pm1)^2+(\pm1)^2 \quad &&(16 \text{ cases}) \qquad &&\text{and}\\
&4=(\pm2)^2+0^2+0^2+0^2 &&(+8 \text{ cases}) &&\text{Check!}
\end{aligned}$$

For a recent proof see *Hirschhorn* [7.9].

On the other hand, Fermat proved that a certain class of integers can be represented by the sum of just 2 squares, and in a *unique* way at that. This class consists of all primes of the form $4k+1$.

This result has an enticing geometrical interpretation. Consider the *integer lattice* in the plane, i. e., all the points (x,y) in the plane with integer coordinates. Draw a circle around the origin $(0,0)$ with radius $p^{1/2}$, where p is a prime with $p\equiv 1 \pmod 4$. Then there are exactly eight lattice points on the circle.

No solutions exist for the primes $p\equiv -1 \pmod 4$. For composite n, we have to distinguish between the factor 2 and the two kinds of primes $p_i\equiv 1 \pmod 4$ and $q_i\equiv -1 \pmod 4$:

$$n=2^{\alpha}\prod_{p_i} p_i{}^{\beta_i}\prod_{q_i} q_i{}^{\gamma_i}.$$

Solutions for $n=x^2+y^2$ exist only if all γ_i are even. *Hardy* and *Wright* [7.1, p. 299] give four different proofs, no less, one going back to Fermat and his "method of descent".

If all γ_i are even, the number of solutions is $\prod_i(\beta_i+1)$, including permutations. ("Trivial" solutions with x or y equal to 0 are counted only once.) Example: $325=5^2\cdot 13$ has 6 solutions. $325=1^2+18^2=6^2+17^2=10^2+15^2=15^2+10^2=17^2+6^2=18^2+1^2$ and no others.

The question *which* squared integers sum to a given prime p is a little trickier to answer. It requires the *Legendre symbol* (a/p), see Eq. (16.17), which equals $+1$ if a is a quadratic residue modulo p, and -1 for a a nonresidue, and 0 for $a\equiv 0 \bmod p$. Thus, for example, for $p=5$, beginning with $a=0$

$$(a/5)=0 \quad +1 \quad -1 \quad -1 \quad +1 \quad 0 \quad \ldots$$

Now taking the product of 3 consecutive terms, beginning with $0\ +1\ -1$, yields

$$0 \quad +1 \quad +1 \quad 0$$

summing to $+2$. Thus, $5 = 2^2 + y^2$ where, obviously, $y = 1$.

For $p = 173$, the same procedure yields $233 = 13^2 + y^2$ with $y = 8$.

The *two-squares theorem*, as it has been called, has an unexpected application in the generation of circulary polarized sound waves. Ordinarily, sound waves in air are thought of as *longitudinal* waves with no transverse field components that could give rise to elliptic or circular polarizations. But in a laterally restricted medium, such as an air-filled duct, sound waves do exhibit lateral motions and are thus polarizable.

Figure 7.6 shows a square box, a short piece of duct with a square cross-section, covered with plexiglas. This cavity resonator supports acoustic modes at frequencies

$$f_n = \frac{c}{2L}\sqrt{n},$$

where c is the velocity of sound in air, L is the side length of the box and n is a positive integer equal to the sum of two squares, the number of half-wavelengths along the side of the box:

$$n = k^2 + m^2.$$

To excite an elliptic wave, the mode must be degenerate, i. e., k and m must be different. Also, to avoid a mode "salad", we require precisely *two* modes at the same resonance frequency. Thus all exponents β_i in the above factorization of n must be 0 except one, which must equal 1, or n must be a square, in which case all β_i must

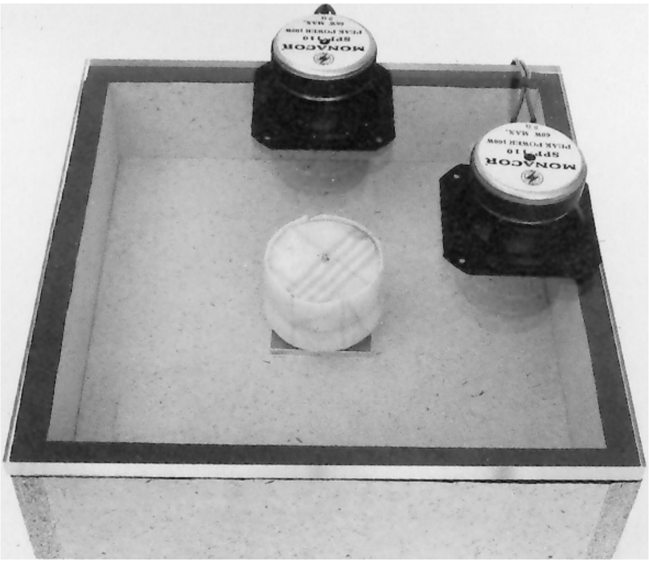

Fig. 7.6 Acoustic resonator with a square cross-section for circularly polarized sound waves

equal 0. Values of n which fulfill these conditions are $1 = 1^2 + 0^2$, $4 = 2^2 + 0^2$, $5 = 2^2 + 1^2$, $9 = 3^2 + 0^2$, $10 = 3^2 + 1^2$, $13 = 3^2 + 2^2$, etc. If the cavity shown in Fig. 7.6 is excited at one of these resonances by means of the two loudspeakers with a phase difference of 90°, a circularly polarized acoustic field will fill the cavity. The circularity can be made visible by a piece of sound-absorbing material supported by a sharp needle in the centre of the cavity: turn on the loudspeakers and the "carousel" will start rotating because the absorber absorbs sound energy, which, in a circularly polarized field, has an angular momentum. Reverse the electrical connections to one of the loudspeakers and the carousel will slow down and start rotating the other way. Replace the absorber by an empty yoghurt cup, which does not absorb much sound, and nothing will happen [7.10].

Geometrically speaking, the resonance frequencies of our square cavity form a two-dimensional square lattice. According to a well-known result by H. Weyl the asymptotic number of resonances ("eigenvalues") up to a given frequency f equals $\pi L^2 f^2/c^2$, which agrees with a result already obtained by Gauss concerning the asymptotic number of representations of the integers by the sum of two squares.

The connection between geometry and number theory was forged into a strong link by Hermann Minkowski. In his *Geometrie der Zahlen* (published in 1896) Minkowski established and proved many beautiful relationships at the interface of geometry and number theory. His most famous result, known as *Minkowski's theorem*, says that *any* convex region symmetrical about $(0,0)$ having an area greater than 4 contains integer lattice points other than $(0,0)$. This theorem, and its generalization to higher dimensional spaces, is particularly useful in proofs concerning the representation of numbers by quadratic forms, such as the above result on the decomposition of certain primes into sums of squares.

In an address before the Göttingen Mathematical Society commemorating the 100th anniversary of Dirichlet's birth, Minkowski hypothesized that some day soon, number theory would triumph in physics and chemistry and that, for example, the decomposition of primes into the sum of two squares would be seen to be related to important properties of matter.[2]

Another intriguing geometrical concept by Minkowski is that of a *Strahlkörper* (literally: ray body) defined as a region in n-dimensional Euclidean space containing the origin and whose surface, as seen from the origin, exhibits only one point in any direction. In other words, if the inner region was made of transparent glass and only the surface was opaque, then the origin would be visible from each surface point of the Strahlkörper (i. e., there are no intervening surface points). Minkowski proved that if the volume of such a Strahlkörper does not exceed $\zeta(n)$, a volume preserving linear transformation exists such that the Strahlkörper has no points in common with the integer lattice (other than the origin). Here $\zeta(n)$ is Riemann's zetafunction which we encountered already in Chap. 4 in connection with the distribution of primes.

[2] "In letzterer Hinsicht bin ich übrigens für die Zahlentheorie Optimist und hege still die Hoffnung, dass wir vielleicht gar nicht weit von dem Zeitpunkt entfernt sind, wo die unverfälschteste Arithmetik gleichfalls in Physik und Chemie Triumphe feiern wird, und sagen wir z. B., wo wesentliche Eigenschaften der Materie als mit der Zerlegung der Primzahlen in zwei Quadrate im Zusammenhang stehend erkannt werden." [7.11].

The fact that $\zeta(n)$ should determine a Strahlkörper property is not totally surprising. If we look at our "coprimality function", Fig. 4.8, it consists of precisely all those points of the lattice of positive integers from which the origin is visible, i. e., the white dots in Fig. 4.8 define the surface of a (maximal) Strahlkörper. And the asymptotic density of dots is $1/\zeta(2) = 6/\pi^2$ (see Sect. 4.4) or, in n dimensions, $1/\zeta(n)$.

The reader may wants to explore the more general decomposition of primes p

$$p = x^2 + cy^2$$

with $c = \pm 2, \pm 3, \ldots$.
For $c = 2$, Lagrange showed that all primes

$$p \equiv 3 \bmod 8$$

are *uniquely* representable, e. g. $19 = 1 + 2 \cdot 3^2$.

For $c = -2$ and $p \equiv 7 \bmod 8$ there are infinitely many solutions obtainable by a simple linear recursion, which the reader may want to discover.

7.11 Normal-Mode Degeneracy in Room Acoustics (A Number-Theoretic Application)

The minimum frequency spacing of two nondegenerate normal modes of a cubical room, in the units used above in (7.30), is

$$\Delta f_{\mathrm{min}} = \frac{1}{2f_{x,y,z}}. \tag{7.37}$$

Because of the gaps in the numbers representable by the sum of 3 squares, the *average* nondegenerate frequency spacing becomes $7/6$ of this value:

$$\overline{\Delta f} = \frac{7}{12f}. \tag{7.38}$$

The asymptotic density of normal modes per unit frequency (using a famous formula on the distribution of eigenvalues, proved in its most general form by Hermann Weyl) is

$$\Delta Z = \frac{\pi}{2} \cdot f^2. \tag{7.39}$$

Thus the average degree of degeneracy D (i. e., the number of modes having the *same* resonance frequency) becomes [7.12]:

$$D = \Delta Z \cdot \overline{\Delta f} = \frac{7\pi}{24} \cdot f \simeq 0.92 \cdot f. \tag{7.40}$$

The degree of degeneracy is important because a high degeneracy can be detrimental to good room acoustics: normal modes that coincide in frequency are missing elsewhere and leave gaps in the frequency scale. Consequently, musical notes generated at those frequencies are not well transmitted to the attending audience (or microphones). This problem is most significant for small enclosures such as recording studios, where the mode density, especially at the lower end of the audiofrequency range, is already small and any unnecessary degeneracy impairs the acoustic responsiveness [7.12].

7.12 Waring's Problem

A problem that has stimulated much mathematical thought, by Hilbert among others, is *Waring's problem* [7.1]: given a positive integer $n > 0$, what is the least number of terms $G(k)$ in the sum:

$$n = \sum_j m_j^k \tag{7.41}$$

for all *sufficiently* large n?

Another question is how many terms $g(k)$ are needed so that *all* n can be represented as in (7.41). Of course:

$$g(k) \geq G(k). \tag{7.42}$$

As we saw in Sect. 7.9, $g(2) = 4$. It is also known that $g(3) = 9$. In fact, there are only finitely many n for which 9 third powers are required. Probably the only two cases are

$$\begin{aligned} 23 &= 2 \cdot 2^3 + 7 \cdot 1^3 \quad \text{and} \\ 239 &= 2 \cdot 4^3 + 4 \cdot 3^3 + 3 \cdot 1^3. \end{aligned}$$

Thus, by definition:

$$G(3) \leq 8.$$

Also $G(3) \geq 4$, but the actual value of $G(3)$ is still not known – another example of how a seemingly innocent question can lead to mathematically most intractable problems!

If we ask *how many different* ways $r_k(n)$ an integer n can be represented as the sum of kth powers (including different sign choices and permutations), then for example by (7.36), $r_2(5) = 8$. Of particular interest are the following asymptotic averages [7.1]:

$$\sum_{n=1}^{N} r_2(n) = \pi N + 0\left(\sqrt{N}\right) \quad \text{and} \tag{7.43}$$

$$\sum_{n=1}^{N} r_3(n) = \frac{4\pi}{3} N^{3/2} + 0(N). \tag{7.44}$$

Both (7.43) and (7.44) are intuitively obvious because they count the number of integer lattice points in a circle and, respectively, a sphere of radius $\sqrt{N}$.