I.2

Some Classical Diophantine Equations

2.1 Linear Diophantine Equations

An equation of the form

$$a_1x_1 + \cdots + a_nx_n = c, \tag{2.1.1}$$

where $a_1, a_2, \ldots, a_n, b$ are fixed integers, is called a *linear Diophantine equation*. We assume that $n \geq 1$ and that coefficients $a_1, \ldots, a_n$ are all different from zero.

We begin with the case $n = 2$. The main result concerning linear Diophantine equations is the following (see also the lemma in Example 5 of Section 1.3).

Theorem 2.1.1. *Let a, b, c be integers, a and b nonzero. Consider the linear Diophantine equation*

$$ax + by = c. \tag{2.1.2}$$

T. Andreescu et al., *An Introduction to Diophantine Equations: A Problem-Based Approach*,
DOI 10.1007/978-0-8176-4549-6_2, © Springer Science+Business Media, LLC 2010

1. *The equation (2.1.2) is solvable in integers if and only if* $d = \gcd(a, b)$ *divides* c.

2. *If* $(x, y) = (x_0, y_0)$ *is a particular solution to (2.1.2), then every integer solution is of the form*

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t, \tag{2.1.3}$$

where t *is an integer.*

3. *If* $c = \gcd(a, b)$ *and* $|a|$ *or* $|b|$ *is different from* 1*, then a particular solution* $(x, y) = (x_0, y_0)$ *to (2.1.3) can be found such that* $|x_0| < |b|$ *and* $|y_0| < |a|$.

Proof. 1. If d does not divide c, then the equation is clearly not solvable. If d divides c, then, dividing both sides of (2.1.2) by $\frac{d}{c}$, it suffices to prove that d is a linear combination with integer coefficients of a and b. For this we use the Euclidean algorithm.

Suppose $a = bq + r$ for integers a, b, r, and q. It is easy to see that every common divisor of a and b is a common divisor of b and r, and conversely. Clearly, if $b \mid a$, then $\gcd(a, b) = b$. In general, we have $\gcd(a, b) = \gcd(b, r)$. These observations lead to a straightforward calculation of the gcd of two numbers. To be systematic, we write $a = r_{-1}$ and $b = r_0$ (assumed positive and $a \geq b$):

$$\begin{aligned}
r_{-1} &= r_0 q_0 + r_1, && 0 \leq r_1 < r_0,\\
r_0 &= r_1 q_1 + r_2, && 0 \leq r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3, && 0 \leq r_3 < r_2,\\
r_2 &= r_3 q_3 + r_4, && 0 \leq r_4 < r_3,\\
&\vdots
\end{aligned}$$

This division process eventually terminates, since the remainders get smaller and smaller,

$$r_{-1} > r_0 > r_1 > r_2 > \cdots,$$

and yet remain nonnegative. In other words, some r_n divides the preceding r_{n-1} (and leaves a remainder $r_{n+1} = 0$).

We obtain

$$\begin{aligned} &\vdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, \quad 0 \le r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n. \end{aligned}$$

From these,

$$r_n = \gcd(r_{n-1}, r_n) = \gcd(r_{n-2}, r_{n-1}) = \cdots = \gcd(r_{-1}, r_0) = \gcd(a, b).$$

The above calculation of $\gcd(a, b)$ can be retraced to give $\gcd(a, b)$ as an integer combination of a and b.

Define the integers x_k and y_k recursively by

$$\begin{aligned} x_k &= x_{k-2} - q_{k-1}x_{k-1}, & x_{-1} &= 1, \quad x_0 = 0, \\ y_k &= y_{k-2} - q_{k-1}y_{k-1}, & y_{-1} &= 0, \quad y_0 = 1. \end{aligned}$$

In each of these steps, $r_k = ax_k + by_k$. In particular,

$$\gcd(a, b) = r_n = ax_n + by_n.$$

It can be checked that (x_i) and (y_i) alternate in sign, $|x_{n+1}| = b/\gcd(a, b)$, and $|y_{n+1}| = a/\gcd(a, b)$. It follows that $|x_n| < b$ and $|y_n| < a$ unless $n = 0$ and $q_0 = 1$, that is, unless $a = b = 1$.

2. We have

$$ax + by = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + by_0 = c.$$

3. The result has already been proven in part 1. □

The central result concerning the general linear Diophantine equation (2.1.1) is the following:

Theorem 2.1.2. *The equation (2.1.1) is solvable if and only if*

$$\gcd(a_1, \ldots, a_n) \mid c.$$

In case of solvability, one can choose $n-1$ solutions such that each solution is an integer linear combination of those $n-1$ solutions.

Proof. Let $d = \gcd(a_1, \ldots, a_n)$. If c is not divisible by d, then (2.1.1) is not solvable, since for any integers $x_1, \ldots, x_n$, the left-hand side of (2.1.1) is divisible by d and the right-hand side is not.

Actually, we need to prove that $\gcd(x_1, x_2, \ldots, x_n)$ is a linear combination with integer coefficients of $x_1, x_2, \ldots, x_n$. For $n = 2$ this follows from Theorem 2.1.1. Because

$$\gcd(x_1, \ldots, x_n) = \gcd(\gcd(x_1, \ldots, x_{n-1}), x_n),$$

$\gcd(x_1, \ldots, x_n)$ is a linear combination of x_n and $\gcd(x_1, \ldots, x_{n-1})$. Then inductively $\gcd(x_1, \ldots, x_n)$ is a linear combination of $x_1, \ldots, x_{n-1}, x_n$. □

Example 1. *Solve the equation*

$$3x + 4y + 5z = 6.$$

Solution. Working modulo 5 we have $3x + 4y \equiv 1 \pmod 5$, and hence

$$3x + 4y = 1 + 5s, \quad s \in \mathbb{Z}.$$

A solution to this equation is $x = -1 + 3s$, $y = 1 - s$. Applying (2.1.3), we obtain $x = -1 + 3s + 4t$, $y = 1 - s - 3t$, $t \in \mathbb{Z}$, and substituting back into the original equation yields $z = 1 - s$. Hence all solutions are

$$(x, y, z) = (-1 + 3s + 4t, 1 - s - 3t, 1 - s), \quad s, t \in \mathbb{Z}.$$

For any positive integers $a_1, \ldots, a_n$ with $\gcd(a_1, \ldots, a_n) = 1$, define $g(a_1, \ldots, a_n)$ to be the greatest positive integer N for which the equation

$$a_1x_1 + \cdots + a_nx_n = N$$

is not solvable in nonnegative integers. The problem of determining $g(a_1, \ldots, a_n)$ is known as the *Frobenius coin problem* (it was he who posed the problem of finding the largest amount of money that cannot be paid using coins worth $a_1, \ldots, a_n$ cents).

Example 2. (Sylvester, 1884) *Let a and b be positive integers with* $\gcd(a, b) = 1$. *Then*

$$g(a, b) = ab - a - b.$$

Solution. Suppose that $N > ab - a - b$. From (2.1.3) it follows that the solutions to the equation $ax + by = N$ are of the form $(x, y) = (x_0 + bt, y_0 - at)$, $t \in \mathbb{Z}$. Let t be an integer such that $0 \leq y_0 - at \leq a - 1$. Then

$$(x_0 + bt)a = N - (y_0 - at)b > ab - a - b - (a - 1)b = -a,$$

which implies $x_0 + bt > -1$, i.e., $x_0 + bt \geq 0$. It follows that in this case the equation $ax + by = N$ is solvable in nonnegative integers. Thus

$$g(a, b) \leq ab - a - b.$$

Now we need only to show that the equation

$$ax + by = ab - a - b$$

is not solvable in nonnegative integers. Otherwise, we have

$$ab = a(x + 1) + b(y + 1).$$

Since $\gcd(a, b) = 1$, we see that $a \mid (y + 1)$ and $b \mid (x + 1)$, which implies $y + 1 \geq a$ and $x + 1 \geq b$. Hence

$$ab = a(x + 1) + b(y + 1) \geq 2ab,$$

and this contradiction shows that

$$g(a, b) \geq ab - a - b.$$

Therefore $g(a, b) = ab - a - b$.

Remarks. (1) The case $n = 3$ was first solved explicitly by Selmer and Beyer, using a continued fraction algorithm. Their result was simplified by Rödseth and later by Greenberg.

(2) No general formulas are known for $n \geq 4$. However, some upper bounds have been proven. In 1942, Brauer showed that

$$g(a_1, \ldots, a_n) \leq \sum_{i=1}^{n} a_i \left(\frac{d_{i-1}}{d_i} - 1 \right),$$

where $d_i = \gcd(a_1, \ldots, a_i)$. Erdős and Graham (1972) showed that

$$g(a_1, \ldots, a_n) \leq 2a_{n-1} \left[\frac{a_n}{n} \right] - a_n,$$

and that

$$\frac{t^2}{n-1} - 5t \le \gamma(n,t) \le \frac{2t^2}{n},$$

where

$$\gamma(n,t) = \max_{0<a_1<\cdots<a_n\le t} g(a_1,\dots,a_n).$$

Suppose that the equation

$$a_1x_1 + \cdots + a_mx_m = n,$$

where $a_1,\dots,a_m > 0$, is solvable in nonnegative integers, and let A_n be the number of its solutions $(x_1,\dots,x_m)$.

Theorem 2.1.3. *(1) The generating function of the sequence* $(A_n)_{n\ge1}$ *is*

$$f(x) = \frac{1}{(1-x^{a_1})\dots(1-x^{a_m})}, \quad |x|<1, \tag{2.1.6}$$

that is, A_n *is equal to the coefficient of* x^n *in the power series expansion of* f*.*

(2) The following equality holds:

$$A_n = \frac{1}{n!}f^{(n)}(0). \tag{2.1.7}$$

Proof. (1) Using a geometric series, we have

$$\frac{1}{1-x^{a_k}} = 1 + x^{a_k} + x^{2a_k} + \cdots, \quad k = 1,\dots,m;$$

hence

$$\begin{aligned} f(x) &= (1 + x^{a_1} + x^{2a_1} + \cdots)\cdots(1 + x^{a_m} + x^{2a_m} + \cdots) \\ &= 1 + A_1x + \cdots + A_nx^n + \cdots. \end{aligned}$$

(2) Passing to the nth derivative, we obtain formula (2.1.7). □

Example 3. *Find the number of pairs (x, y) of nonnegative integers such that*

$$x + 2y = n.$$

Solution. From Theorem 2.1.3 it follows that the desired number is

$$A_n = \frac{1}{n!} f^{(n)}(0),$$

where

$$f(t) = \frac{1}{(1-t)(1-t^2)}.$$

We have

$$f(t) = \frac{1}{2} \cdot \frac{1}{(t-1)^2} - \frac{1}{4} \cdot \frac{1}{t-1} + \frac{1}{4} \cdot \frac{1}{t+1}$$

hence

$$f^{(n)}(t) = \frac{1}{2} \frac{(-1)^n (n+1)!}{(t-1)^{n+2}} - \frac{1}{4} \frac{(-1)^n n!}{(t-1)^{n+1}} + \frac{1}{4} \frac{(-1)^n n!}{(t+1)^{n+1}}.$$

Thus

$$f^{(n)}(0) = \frac{(n+1)!}{2} + \frac{n!}{4} + \frac{(-1)^n n!}{4}$$

and

$$A_n = \frac{1}{n!} f^{(n)}(0) = \frac{2n + 3 + (-1)^n}{4}.$$

Exercises and Problems

1. Solve the equation

$$6x + 10y - 15z = 1.$$

2. Let a, b, c be pairwise relatively prime positive integers. Show that $2abc-ab-bc-ca$ is the largest integer that cannot be expressed in the form $xbc + yca + zab$, where x, y, z are nonnegative integers.

(24th IMO)

3. Find the number of triples (x, y, z) of nonnegative integers such that

$$x + y + 2z = n.$$

4. Determine the positive integer n such that the equation

$$x + 2y + z = n$$

has exactly 100 solutions (x, y, z) in nonnegative integers.

5. Let a, b, c, d be integers such that for all integers m and n there exist integers x and y for which $ax + by = m$ and $cx + dy = n$. Prove that $ad - bc = \pm 1$.

(Eötvös Mathematics Competition)

6. Let n be an integer greater than 3 and let X be a $3n^2$-element subset of $\{1, 2, \ldots, n^3\}$. Prove that there exist nine distinct numbers $a_1, a_2, \ldots, a_9$ in X such that the system

$$\begin{cases} a_1x + a_2y + a_3z = 0, \\ a_4x + a_5y + a_6z = 0, \\ a_7x + a_8y + a_9z = 0, \end{cases}$$

is solvable in nonzero integers.

(Romanian Mathematical Olympiad)

7. Let

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1q}x_q = 0, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2q}x_q = 0, \\ \vdots \\ a_{p1}x_1 + a_{p2}x_2 + \cdots + a_{pq}x_q = 0, \end{cases}$$

be a system of linear equations, where $q = 2p$ and $a_{ij} \in \{-1, 0, 1\}$. Prove that there exists a solution $(x_1, x_2, \ldots, x_q)$ of the system with the following properties:

(a) x_j is an integer for every $j = 1, 2, \ldots, q$;

(b) there exist j such that $x_j \neq 0$;

(c) $|x_j| \leq q$ for every $j = 1, 2, \ldots, q$.

(18th IMO)

2.2 Pythagorean Triples and Related Problems

One of the most celebrated Diophantine equations is the *Pythagorean equation*

$$x^2 + y^2 = z^2. \tag{2.2.1}$$

Studied in detail by Pythagoras in connection with the right triangles whose side lengths are all integers, this equation was known even to the ancient Babylonians.

Note first that if the triple of integers (x_0, y_0, z_0) satisfies equation (2.2.1), then all triples of the form (kx_0, ky_0, kz_0), $k \in \mathbb{Z}$, also satisfy (2.2.1). That is why it is sufficient to find solutions (x, y, z) to (2.2.1) with $\gcd(x, y, z) = 1$. This is equivalent to the fact that x, y, z are pairwise relatively prime.

A solution (x_0, y_0, z_0) to (2.2.1) with x_0, y_0, z_0 pairwise relatively prime is called a *primitive solution*. It is clear that in a primitive solution exactly one of x_0 and y_0 is even.

Theorem 2.2.1. *Any primitive solution (x, y, z) in positive integers to the equation (2.2.1) with y even is of the form*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2, \tag{2.2.2}$$

where m and n are relatively prime positive integers such that $m > n$ and $m + n$ is odd.

Proof. The integers x and y cannot both be odd, for otherwise

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4,$$

a contradiction. Hence exactly one of the integers x and y is even.

The identity

$$\left(m^2 - n^2\right)^2 + \left(2mn\right)^2 = \left(m^2 + n^2\right)^2$$

shows that the triple given by (2.2.2) is indeed a solution to the equation (2.2.1) and y is even. Because x must be odd, we may assume without loss of generality that m is odd and n is even.

Moreover, if $\gcd\left(m^2 - n^2, 2mn, m^2 + n^2\right) = d \geq 2$, then d divides

$$2m^2 = \left(m^2 + n^2\right) + \left(m^2 - n^2\right)$$

and d divides

$$2n^2 = \left(m^2 + n^2\right) - \left(m^2 - n^2\right).$$

Because m and n are relatively prime it follows that $d = 2$. Hence $m^2 + n^2$ is even, in contradiction to m odd and n even. It follows that $d = 1$, so the solution (2.2.2) is primitive.

Conversely, let (x, y, z) be a primitive solution to (2.2.1) with $y = 2a$. Then x and z are odd, and consequently the integers $z + x$ and $z - x$ are even. Let $z + x = 2b$ and $z - x = 2c$. We may assume that b and c are relatively prime, for otherwise z and x would have a nontrivial common divisor. On the other hand, $4a^2 = y^2 = z^2 - x^2 = (z + x)(z - x) = 4bc$, i.e., $a^2 = bc$. Since b and c are relatively prime, it follows that $b = m^2$ and $c = n^2$ for some positive integers m and n. We obtain that $m + n$ is odd and

$$x = b - c = m^2 - n^2, \quad y = 2mn, \quad z = b + c = m^2 + n^2. \qquad \square$$

A triple (x, y, z) of the form (2.2.2) is called *primitive*. In order to list all primitive solutions to equation (2.2.1), we assign values $2, 3, 4, \ldots$ to m and then for each of these values we take those integers n that are relatively prime to m and less than m.

Here is a table of the first 20 primitive solutions listed according to the above-mentioned rule. The last column refers to the area.

m	n	x	y	z	area
2	1	3	4	5	6
3	2	5	12	13	30
4	1	15	8	17	60
4	3	7	24	25	84
5	2	21	20	29	210
5	4	9	40	41	180
6	1	35	12	37	210
6	5	11	60	61	330
7	2	45	28	53	630
7	4	33	56	65	924

m	n	x	y	z	area
7	6	13	84	85	546
8	1	63	16	65	504
8	3	55	48	73	1320
8	5	39	80	89	1560
8	7	15	112	113	840
9	2	77	36	85	1386
9	4	65	72	97	2340
9	8	17	144	145	1224
10	1	99	20	101	990
10	3	91	60	109	2730

Corollary 2.2.2. *The general integral solution to (2.2.1) is given by*

$$x = k(m^2 - n^2), \quad y = 2kmn, \quad z = k(m^2 + n^2), \tag{2.2.3}$$

where $k, m, n \in \mathbb{Z}$.

The immediate extension to equation (2.2.1) is

$$x^2 + y^2 + z^2 = t^2. \tag{2.2.4}$$

The positive solutions (x, y, z, t) to (2.2.4) represent the dimensions and the length of the diagonal of a rectangular box. We want to find all situations in which these components are all integers.

Theorem 2.2.3. *All the solutions to equation (2.2.4) in positive integers* x, y, z, t *with* y, z *even are given by*

$$x = \frac{l^2 + m^2 - n^2}{n}, \quad y = 2l, \quad z = 2m, \quad t = \frac{l^2 + m^2 + n^2}{n}, \tag{2.2.5}$$

where l, m *are arbitrary positive integers and* n *is any divisor of* $l^2 + m^2$ *less than* $\sqrt{l^2 + m^2}$. *Every solution is obtained exactly once in this way.*

Proof. The identity

$$\left(\frac{l^2 + m^2 - n^2}{n}\right)^2 + (2l)^2 + (2m)^2 = \left(\frac{l^2 + m^2 + n^2}{n}\right)^2$$

shows that the quadruple in (2.2.5) is a solution to equation (2.2.4) and that y and z are even.

Conversely, note that at least two of the integers x, y, z must be even; otherwise, $t^2 \equiv 2, 3 \pmod 4$, a contradiction. Suppose that $y = 2l$, $z = 2m$ for some positive integers l and m. Setting $t - x = u$, we obtain

$$x^2 + 4l^2 + 4m^2 = (x + u)^2, \quad \text{or} \quad u^2 = 4(l^2 + m^2) - 2ux.$$

Therefore u^2 is even, so $u = 2n$ for some positive integer n. It follows that $x = \frac{l^2+m^2-n^2}{n}$ and $t = x + u = x + 2n = \frac{l^2+m^2+n^2}{n}$, where l, m, n are positive integers and n is a divisor of $l^2 + m^2$ less than $\sqrt{l^2 + m^2}$.

It is not difficult to see that every solution (x, y, z, t) to (2.2.4) with y and z even is obtained exactly once from the formulas (2.2.5). Indeed, by (2.2.5) we have $l = \frac{y}{2}$, $m = \frac{z}{2}$, $n = \frac{t-x}{2}$; hence the integers l, m, n are uniquely determined by (x, y, z, t). □

Theorem 2.2.3 not only states the existence of the solutions to equation (2.2.4) but also gives a method for finding these solutions. It is not difficult to see that in order to eliminate the solutions with reversed unknowns we may reject the pairs (l, m) with $l < m$ and consider only those n for which x is odd. Hence we eliminate also the solutions for which x, y, z, t are all even.

Here are the first 10 solutions obtained in this way.

l	m	$l^2 + m^2$	n	x	y	z	t
1	1	2	1	1	2	2	3
2	2	8	1	7	4	4	9
3	1	10	1	9	6	2	11
3	1	10	2	3	6	2	7
3	3	18	1	17	6	6	19
3	3	18	2	7	6	6	11
3	3	18	3	3	6	6	9
4	2	20	1	19	8	4	21
4	2	20	4	1	8	4	9
4	4	32	1	31	8	8	33

Remarks. (1) A well-known way to produce "Pythagorean quadruples" is

$$x = l^2 + m^2 - n^2, \quad y = 2lm, \quad z = 2mn, \quad t = l^2 + m^2 + n^2,$$

where l, m, n are positive integers. It is also known that not all quadruples are generated in this way; for instance, $(3, 36, 8, 37)$ is excluded. On the other hand, this family of solutions is quite similar to the family of solutions to (2.2.1).

(2) The following formulas produce all Pythagorean quadruples of integers:

$$\begin{aligned} x &= m^2 + n^2 - p^2 - q^2, \\ y &= 2(mp + nq), \\ z &= 2(np - mq), \\ t &= m^2 + n^2 + p^2 + q^2, \end{aligned}$$

where m, n, p, q are arbitrary integers. For a proof that uses Gaussian integers see Section 4.1.

(3) The equation

$$x_1^2 + x_2^2 + \cdots + x_k^2 = x_{k+1}^2 \tag{2.2.6}$$

is the natural extension of (2.2.1) and (2.2.4). From a geometrical point of view, the solutions $(x_1, x_2, \ldots, x_k, x_{k+1})$ represent the dimensions $x_1, x_2, \ldots, x_k$ of a cuboid in $\mathbb{R}^k$ and the length x_{k+1} of its diagonal, respectively. All positive integer solutions $(x_1, x_2, \ldots, x_k, x_{k+1})$ with $\gcd(x_1, x_2, \ldots, x_k) = 1$ to the equation

(2.2.6) are given by

$$\begin{aligned} x_1 &= \frac{1}{q}\Big(m_1^2 + m_2^2 + \cdots + m_{k-1}^2 - m_k^2\Big), \\ x_2 &= \frac{2}{q} m_1 m_k, \\ &\vdots \\ x_k &= \frac{2}{q} m_{k-1} m_k, \\ x_{k+1} &= \frac{1}{q}\Big(m_1^2 + m_2^2 + \cdots + m_{k-1}^2 + m_k^2\Big). \end{aligned}$$

Here $m_1, m_2, \ldots, m_k$ are arbitrary integers and $q > 0$ is taken such that $\gcd(x_1, x_2, \ldots, x_k) = 1$.

(4) For $k = 5$, arguments involving spinors in physics produce Pythagorean hexads:

$$\begin{aligned} x_1 &= m^2 - n^2, \\ x_2 &= 2(n_0 m_1 - n_1 m_0 + m_3 n_2 - m_2 n_3), \\ x_3 &= 2(n_0 m_2 - n_2 m_0 + m_1 n_3 - m_3 n_1), \\ x_4 &= 2(n_0 m_3 - n_3 m_0 + m_2 n_1 - m_1 n_2), \\ x_5 &= 2mn, \\ x_6 &= m^2 + n^2, \end{aligned}$$

where $m, n, m_0, m_1, m_2, m_3, n_0, n_1, n_2, n_3$ are integers such that

$$mn = m_0 n_0 + m_1 n_1 + m_2 n_2 + m_3 n_3.$$

Example 1. *(the "negative" Pythagorean equation) Solve in positive integers the equation*

$$x^{-2} + y^{-2} = z^{-2}. \tag{2.2.7}$$

Solution. The equation is equivalent to

$$x^2 + y^2 = \left(\frac{xy}{z}\right)^2.$$

This means that $z \mid xy$ and that $x^2 + y^2$ is a perfect square. Then $x^2 + y^2 = t^2$ for some positive integer t, and the equation becomes

$$t = \frac{xy}{z}. \tag{2.2.8}$$

Let $d = \gcd(x, y, t)$. Then $x = ad$, $y = bd$, $t = cd$, where $a, b, c \in \mathbb{Z}_+$ with $\gcd(a, b, c) = 1$. Equation (2.2.8) reduces to

$$z = \frac{abd}{c}. \tag{2.2.9}$$

From the choice of t it follows that

$$a^2 + b^2 = c^2; \tag{2.2.10}$$

hence a, b, c are pairwise relatively prime. Then using (2.2.7), we deduce that $c \mid d$, i.e., $d = kc$, $k \in \mathbb{Z}_+$. We obtain

$$x = ad = kac, \quad y = bd = kbc, \quad t = cd = kc^2, \quad z = kab.$$

Taking into account (2.2.10) and the formulas (2.2.2), we have $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$, where the positive integers m and n satisfy the conditions in Theorem 2.2.1. The solutions to equation (2.2.7) are given by

$$x = k\Big(m^4 - n^4\Big), \quad y = 2kmn\Big(m^2 + n^2\Big), \quad z = 2kmn\Big(m^2 - n^2\Big),$$

where $k, m, n \in \mathbb{Z}_+$ and $m > n$.

Remark. If a, b, c are positive integers satisfying

$$\frac{1}{a^2} + \frac{1}{b^2} = \frac{1}{c^2},$$

then $a^4 + b^4 + c^4$ is a perfect square. Indeed,

$$a^2b^2 = b^2c^2 + c^2a^2$$

and

$$a^4 + b^4 + c^4 = a^4 + b^4 + c^4 + 2a^2b^2 - 2b^2c^2 - 2c^2a^2 = (a^2 + b^2 - c^2)^2.$$

Example 2. *Prove that there are no two positive integers such that the sum and the difference of their squares are also squares.*

Solution. The problem is equivalent to showing that the system of equations

$$\begin{cases} x^2 + y^2 = z^2, \\ x^2 - y^2 = w^2, \end{cases} \tag{2.2.11}$$

is not solvable in positive integers.

Assume, for the sake of contradiction, that (2.2.11) is solvable in positive integers and consider a pair (x, y) such that $x^2 + y^2$ is minimal. It is clear that $\gcd(x, y) = 1$. Adding the equations of the system yields

$$2x^2 = z^2 + w^2; \tag{2.2.12}$$

hence z and w have the same parity. It follows that $z + w$ and $z - w$ are both even. Write (2.2.12) in the form

$$x^2 = \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2.$$

Moreover, $\gcd\left(x, \frac{z+w}{2}, \frac{z-w}{2}\right) = 1$. Indeed, if

$$\gcd\left(x, \frac{z+w}{2}, \frac{z-w}{2}\right) = d \geq 2,$$

then $d \mid x$ and $d \Big| \left(\frac{z+w}{2} + \frac{z-w}{2}\right) = z$. From the first equation in (2.2.11) we then obtain $d \mid y$, in contradiction to $\gcd(x, y) = 1$.

Applying Theorem 2.2.1, we get

$$\frac{z-w}{2} = m^2 - n^2, \quad \frac{z+w}{2} = 2mn,$$

or

$$\frac{z-w}{2} = 2mn, \quad \frac{z+w}{2} = m^2 - n^2.$$

Since $2y^2 = z^2 - w^2$, in either case we have

$$2y^2 = 2(m^2 - n^2) \cdot 4mn,$$

and hence

$$y^2 = 4mn(m^2 - n^2).$$

It follows that $y = 2k$, for some positive integer k, and that

$$k^2 = mn(m+n)(m-n). \tag{2.2.13}$$

Since m and n are relatively prime and $m+n$ is odd, the integers $m, n, m+n, m-n$ are also pairwise relatively prime; hence from (2.2.13) we deduce that $m = a^2$, $n = b^2$, $m+n = c^2$, and $m-n = d^2$, for some positive integers a, b, c, d. But $a^2+b^2 = c^2$ and $a^2-b^2 = d^2$, i.e., (a, b, c, d) is also a solution to the system (2.2.11). Moreover,

$$a^2 + b^2 = m + n < 4mn(m^2 - n^2) = y^2 < x^2 + y^2,$$

in contradiction to the minimality of $x^2 + y^2$.

Example 3. *Solve the following equation in positive integers:*

$$x^2 + y^2 = 1997(x - y).$$

Solution. The solutions are

$$(x, y) = (170, 145) \quad \text{and} \quad (x, y) = (1827, 145).$$

We have

$$\begin{aligned} x^2 + y^2 &= 1997(x - y), \\ \Big(x + y\Big)^2 + \bigg(\Big(x - y\Big)^2 - 2 \cdot 1997(x - y)\bigg) &= 0 \\ \Big(x + y\Big)^2 + (1997 - x + y)^2 &= 1997^2. \end{aligned}$$

Since x and y are positive integers, $0 < x + y < 1997$ and $0 < 1997 - x + y < 1997$. Thus the problem reduces to solving $a^2 + b^2 = 1997^2$ in positive integers. Since 1997 is a prime, $\gcd(a, b) = 1$. By Pythagorean substitution, there are positive integers $m > n$ such that $\gcd(m, n) = 1$ and

$$1997 = m^2 + n^2, \quad a = 2mn, \quad b = m^2 - n^2.$$

Since $m^2, n^2 \equiv 0, 1, -1 \pmod 5$ and $1997 \equiv 2 \pmod 5$, $m, n = \pm 1 \pmod 5$. Since $m^2, n^2 \equiv 0, 1 \pmod 3$ and $1997 \equiv 2 \pmod 3$, $m, n \equiv \pm 1 \pmod 3$. Therefore $m, n \equiv 1, 4, 11, 14 \pmod{15}$. Since $m > n$, $1997/2 \le m^2 \le 1997$. Thus we need to consider only $m = 34, 41, 44$. The only solution is $(m, n) = (34, 29)$. Thus

$$(a, b) = (1972, 315),$$

which leads to our solution.

Example 4. *Find all quadruples (x, y, z, w) such that*

$$x^2 + y^2 + z^2 + xy + yz + zx = 2w^2.$$

Solution. Write the equation as

$$(x+y)^2+(y+z)^2+(z+x)^2=(2w)^2.$$

From Theorem 2.2.3,

$$x+y=\frac{l^2+m^2-n^2}{n},\quad y+z=2l,\quad z+x=2m,$$
$$2w=\frac{l^2+m^2+n^2}{n},$$

where $n \mid l^2+m^2$. It follows that all desired quadruples are

$$x=m-l+\frac{l^2+m^2-n^2}{2n},\quad y=l-m+\frac{l^2+m^2-n^2}{2n},$$
$$z=l+m-\frac{l^2+m^2-n^2}{2n},\quad w=\frac{l^2+m^2+n^2}{2n},$$

where the positive integers l, m, n are chosen such that x, y, z are all positive and $2n \mid l^2+m^2+n^2$.

Exercises and Problems

1. Prove that the system of equations

$$\begin{cases} x^2+y^2=u^2, \\ x^2+2y^2=v^2, \end{cases}$$

is not solvable in positive integers.

2. Let m and n be distinct positive integers. Show that none of the numbers $2(m^4+n^4),\ m^4+6m^2n^2+n^4$ is a perfect square.

3. Prove that the equation

$$x^2y^2=z^2\Big(z^2-x^2-y^2\Big)$$

has no solution in positive integers.

4. Prove that the equation $x^2 + y^2 = \left(a^2 + b^2\right)z^2$, where a and b are nonzero given integers, has infinitely many solutions.

5. Find all quadruples (x, y, z, w) of positive integers such that

$$xy + yz + zx = w^2.$$

6. Prove that there is no Pythagorean triangle whose area is a perfect square.

7. Prove that the number of primitive Pythagorean triangles with a given inradius r is a power of 2 if r is integer.

8. (a) Solve the equation $x^2 + y^2 + z^2 - xy - yz - zx = t^2$.

(b) Prove that the equation $u^2 + v^2 + w^2 = 2t^2$ has infinitely many solutions in positive integers.

(Titu Andreescu and Dorin Andrica)

2.3 Other Remarkable Equations

2.3.1. Some Quadratic Diophantine Equations and Related Problems

We begin by presenting a simple but useful equation that has numerous applications.

Theorem 2.3.1. *All integer solutions to the equation*

$$xy = zw$$

are $x = mn$, $y = pq$, $z = mp$, $w = nq$, *where* m, n, p, q *are integers and* $\gcd(n, p) = 1$.

Proof. Write the equation as $\frac{x}{z} = \frac{w}{y}$ and denote by $\frac{n}{p}$ the corresponding irreducible fraction. Then set

$$m = \frac{x}{n} = \frac{z}{p} \quad \text{and} \quad q = \frac{y}{p} = \frac{w}{n}. \qquad \square$$

Remarks. (1) For all positive integers x, y, z, w satisfying $xy = zw$, the integer $N = x + y + z + w$ is composite. Indeed,

$$xN = x^2 + xy + xz + xw = x^2 + zw + xz + xw = (x + z)(x + w)$$

and the conclusion follows.

(2) A special case is the equation $xy = z^2$. All integer solutions to this equation are $x = km^2$, $y = kn^2$, $z = kmn$, where k, m, n are integers and $\gcd(m, n) = 1$.

Example 1. *If there are two distinct unordered pairs (x, y) of positive integers satisfying the equation*

$$x^2 + y^2 = n,$$

then n is composite.

Solution. Let (a, b) and (c, d) be two such solutions. Then $a \neq c$ and $a \neq d$. We may assume without loss of generality that $a > c$. Then

$$(a + c)(a - c) = (d + b)(d - b),$$

so there are positive integers m, n, p, q such that

$$\gcd(n, p) = 1$$

and

$$a + c = mn, \quad a - c = pq, \quad d + b = mp, \quad d - b = nq.$$

Then

$$a = \frac{1}{2}(mn + pq), \quad b = \frac{1}{2}(nq - mp),$$

and

$$4n = 4(a^2 + b^2) = (mn + pq)^2 + (nq - mp)^2 = (m^2 + q^2)(n^2 + p^2).$$

Assume by way of contradiction that n is a prime. Then without loss of generality, $m^2 + q^2 = 2$ or $m^2 + q^2 = 4$. In the first case $m = q = 1$, implying $a = d$, a contradiction. The second case is clearly impossible. Thus n is composite.

Remark. All integer solutions to the equation

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

are

$$x = \frac{1}{2}(mn + pq), \quad y = \frac{1}{2}(mp - nq),$$

$$z = \frac{1}{2}(mp + nq), \quad w = \frac{1}{2}(mn - pq),$$

where m, n, p, q are integers.

We continue this section by examining the Diophantine equation

$$x^2 + axy + y^2 = z^2, \tag{2.3.1}$$

where a is a given integer. The Pythagorean equation is a special case of this equation ($a = 0$).

Theorem 2.3.2. *All integral solutions to (2.3.1) are given by*

$$\begin{cases} x = k(an^2 - 2mn), \\ y = k(m^2 - n^2), \\ z = \pm k(amn - m^2 - n^2), \end{cases} \qquad \begin{cases} x = k(m^2 - n^2), \\ y = k(an^2 - 2mn), \\ z = \pm k(amn - m^2 - n^2), \end{cases} \tag{2.3.2}$$

where $m, n \in \mathbb{Z}$ are relatively prime and $k \in \mathbb{Q}$ such that $(a^2 - 4)$ $k \in \mathbb{Z}$.

Proof. Note that the two families of solutions are given by the symmetry of (2.3.1) in x and y.

It is not difficult to check that the triples (x, y, z) in (2.3.2) satisfy equation (2.3.1).

Conversely, we need to show that all solutions to (2.3.1) are of the form (2.3.2). In this regard, note that equation (2.3.1) is equivalent to

$$x(x + ay) = (z - y)(z + y). \tag{2.3.3}$$

From Theorem 2.3.1 it follows that

$$x = np, \quad x + ay = mq, \quad z + y = nq, \quad z - y = mp,$$

for some integers m, n, p, q.

The result is clear in the case $y = z$, which corresponds to $x = 0$ or $x + ay = 0$. In all other cases (2.3.3) is equivalent to

$$\frac{x}{z - y} = \frac{z + y}{x + ay} = \frac{n}{m}$$

for some nonzero integers m and n. The last relations lead to the homogeneous system

$$\begin{cases} mx + ny - nz = 0, \\ nx + (n - am)y - mz = 0, \end{cases}$$

whose solutions are

$$x = \frac{an^2 - 2mn}{amn - m^2 - n^2} z, \quad y = \frac{m^2 - n^2}{amn - m^2 - n^2} z.$$

We choose $z = k\Big(amn - m^2 - n^2\Big)$, where $k \in \mathbb{Q}$, and get the solutions (2.3.2). □

If $k = p/q$ in lowest terms, then

$$q \mid \gcd\Big(an^2 - 2mn, m^2 - n^2, amn - m^2 - n^2\Big),$$

and hence

$$q \mid a\Big(an^2 - 2mn\Big) + 2\Big(m^2 - n^2\Big) + 2\Big(amn - m^2 - n^2\Big) = \Big(a^2 - 4\Big)n^2.$$

Since any prime dividing n cannot divide $m^2 - n^2$, it follows that $q \mid a^2 - 4$ or $\Big(a^2 - 4\Big)k \in \mathbb{Z}$.

Remarks. (1) Theorem 2.3.1 solves the third-degree Diophantine equation

$$x^2 + xyw + y^2 = z^2. \tag{2.3.4}$$

The general solution is (x, y, z, w), where $w = a$, $a \in \mathbb{Z}$ and x, y, z are given in (2.3.2).

(2) In a similar manner, we can prove that the equation

$$x^2 + axy + by^2 = z^2 \tag{2.3.5}$$

has infinitely many solutions, one family of which is

$$\begin{cases} x = k\Big(m^2 - bn^2\Big), \\ y = k\Big(an^2 - 2mn\Big), \\ z = \pm k\Big(amn - m^2 - bn^2\Big), \end{cases} \tag{2.3.6}$$

where $m, n \in \mathbb{Z}$ are relatively prime and $k \in \mathbb{Q}$ such that $(a^2 - 4b)k \in \mathbb{Z}$.

Generally, choosing $k \in \mathbb{Z}$ gives integer solutions, but not every integer solution corresponds to an integral k. For instance, for $a = 0$ and $b = -21$ the family (2.3.6) is

$$x = k\Big(m^2 + 21n^2\Big), \quad y = -2kmn, \quad z = k\Big(21n^2 - m^2\Big),$$

but the triple $(5, 1, 2)$ is not generated in this way. One reason is the following: equation (2.3.5) is equivalent to

$$(2x + ay)^2 - \Big(a^2 - 4b\Big)y^2 = (2z)^2,$$

and if a^2-4b is not a perfect square, the ring $\mathbb{Z}\left[\sqrt{a^2-4b}\right]$ is not necessarily a unique factorization domain (see Section 4.1).

(3) Using the above remark we can construct an infinite family of solutions to the Diophantine equation

$$x^2+uxy+vy^2=z^2.$$

The solutions are (x,y,z,u,v), where $u=a$, $v=b$, $a,b\in\mathbb{Z}$, and x,y,z are given in (2.3.6).

(4) The solutions in positive integers to equation (2.3.1) can be expressed as follows:

$$\begin{cases} x=k\Big(2mn+an^2\Big), \\ y=k\Big(m^2-n^2\Big), \\ z=k\Big|m^2+amn+n^2\Big|, \end{cases} \qquad \begin{cases} x=k\Big(m^2-n^2\Big), \\ y=k\Big(2mn+an^2\Big), \\ z=k\Big|m^2+amn+n^2\Big| \end{cases} \tag{2.3.7}$$

where $m,n\in\mathbb{Z}_+^*$ are relatively prime, $k\in\mathbb{Q}_+^*$ such that $\Big(a^2-4\Big)k\in\mathbb{Z}$, $n>0$, $2m+an>0$, and $|m|>n$.

Aside from the case $a=0$, for which we obtain the Pythagorean equation, the following two cases are of particular interest:

The case $a=1$. Equation (2.3.1) becomes

$$x^2+xy+y^2=z^2. \tag{2.3.8}$$

From (2.3.7) it follows that its positive integer solutions are given by

$$\begin{cases} x=k\Big(2mn+n^2\Big), \\ y=k\Big(m^2-n^2\Big), \\ z=k\Big(m^2+mn+n^2\Big), \end{cases} \qquad \begin{cases} x=k\Big(m^2-n^2\Big), \\ y=k\Big(2mn+n^2\Big), \\ z=k\Big(m^2+mn+n^2\Big), \end{cases} \tag{2.3.9}$$

where $m, n \in \mathbb{Z}_+^*$, $m > n$, are relatively prime and $k \in \mathbb{Q}_+^*$ such that $3k \in \mathbb{Z}$.

The solutions (2.3.9) give all triples of positive integers (x, y, z) that are the side lengths of a triangle whose opposite angle to z is $120°$.

The case $a = -1$. Equation (2.3.1) becomes

$$x^2 - xy + y^2 = z^2. \tag{2.3.10}$$

Its positive integral solutions are given by

$$\begin{cases} x = k\Big(2mn - n^2\Big), \\ y = k\Big(m^2 - n^2\Big), \\ z = k\Big(m^2 - mn + n^2\Big), \end{cases} \qquad \begin{cases} x = k\Big(m^2 - n^2\Big), \\ y = k\Big(2mn - n^2\Big), \\ z = k\Big(m^2 - mn + n^2\Big), \end{cases} \tag{2.3.11}$$

where $m, n \in \mathbb{Z}_+^*$, $m > n$, are relatively prime and $k \in \mathbb{Q}_+^*$, such that $3k \in \mathbb{Z}$.

The solutions (2.3.11) characterize all triples of positive integers (x, y, z) that are the side lengths of a triangle whose angle opposite the side of length z is $60°$.

Example 1. *Find all triples* (x, y, z) *of positive integers such that*

$$x^2 + xy + y^2 = 49^2.$$

Solution. From the general form of the solutions in (2.3.9), the problem reduces to finding all relatively prime positive integers m, n with $m > n$, and $k \in \mathbb{Q}_+$ with $3k \in \mathbb{Z}$ such that

$$k\Big(m^2 + mn + n^2\Big) = 49.$$

In the following table we give all pairs (m, n) satisfying the inequality $m^2 + mn + n^2 \leq 49$, where $m > n$.

m	n	$m^2 + mn + n^2$
2	1	7
3	1	13
4	1	21
5	1	31
6	1	43
3	2	19
4	2	28
5	2	39
4	3	37
5	3	49

If $k = 1$, from the above table we can see that $m^2 + mn + n^2 = 49$ holds if and only if $m = 5$ and $n = 3$. In this case we obtain the solutions $(x, y) = (39, 16)$ and $(x, y) = (16, 39)$.

If $k = 7$ we obtain that $m^2 + mn + n^2 = 7$ if and only if $m = 2$ and $n = 1$, yielding the solutions $(x, y) = (35, 21)$ and $(x, y) = (21, 35)$.

The cases $k = \frac{1}{3}$ and $k = \frac{49}{3}$ give $m = n$, which is impossible. If $k = \frac{7}{3}$, then we get $m = 4$ and $n = 1$, giving solutions $(x, y) = (35, 21)$, $(21, 35)$.

It is natural to ask in what situations the solutions (x, y) to equations (2.3.8) and (2.3.10) are perfect squares.

Theorem 2.3.2. *All nonnegative integral solutions to the equation*

$$x^4 + x^2y^2 + y^4 = z^2 \tag{2.3.12}$$

are $(x, y, z) = \left(k, 0, k^2\right)$, $(x, y, z) = \left(0, k, k^2\right)$, $k \in \mathbb{Z}_+$.

Proof. We may assume that $\gcd(x, y) = 1$. Then x and y have different parities, for otherwise $z^2 \equiv 3 \pmod 4$. Suppose that y is odd and minimal. Write the equation in the equivalent form

$$4z^2 - \left(2x^2 + y^2\right)^2 = 3y^4, \tag{2.3.13}$$

or $\left(2z + 2x^2 + y^2\right)\left(2z - 2x^2 - y^2\right) = 3y^4$.

We claim that $\gcd\left(2z+2x^2+y^2, 2z-2x^2-y^2\right) = 1$. Indeed, assume that d is a prime dividing both $2z+2x^2+y^2$ and $2z-2x^2-y^2$. Then d is odd and d divides both z and $2x^2 + y^2$. From (2.3.13) it follows that $d \mid 3y$. If $d > 3$, then $d \mid y$ and $d \mid 2x^2$, i.e., $\gcd(x, y) \geq d$, a contradiction. If $d = 3$, it follows that $3 \mid z$, and from (2.3.12) we obtain $3 \mid (2x^2 + y^2)$, so $3 \mid y$. Therefore $3 \mid x$, and so $\gcd(x, y) \geq 3$, a contradiction.

Hence, either $2z + 2x^2 + y^2 = a^4$, $2z - 2x^2 - y^2 = 3b^4$, $y = ab$ or $2z + 2x^2 + y^2 = 3a^4$, $2z - 2x^2 - y^2 = b^4$, $y = ab$, where a and b are both odd positive integers.

In the first situation,

$$4x^2 = a^4 - 2a^2b^2 - 3b^4 \equiv -4 \pmod{16},$$

a contradiction.

In the second case,

$$4x^2 = 3a^4 - 2a^2b^2 - b^4 = \left(a^2 - b^2\right)\left(3a^2 + b^2\right).$$

Since a and b are both odd, it follows that $a^2 - b^2 = c^2$ and $3a^2 + b^2 = 4d^2$, for some positive integers c and d. Then $a = p^2 + q^2$, $b = p^2 - q^2$, $p, q \in \mathbb{Z}_+$, and

$$p^4 + p^2q^2 + q^4 = d^2,$$

which contradicts the minimality of y.

Therefore $y = 1$, $a = b = 1$, and $x = 0$, yielding the solution $(0, 1, 1)$. Taking into account the symmetry in x and y, we also have the solution $(1, 0, 1)$, and the conclusion follows. □

Example 2. *Solve in positive integers the system of equations*

$$\begin{cases} 3u^2 + v^2 = 4s^2, \\ u^2 + 3v^2 = 4t^2. \end{cases}$$

Solution. Setting $u = x+y$ and $v = x-y$, we obtain the equivalent system

$$\begin{cases} x^2 + xy + y^2 = s^2, \\ x^2 - xy + y^2 = t^2. \end{cases}$$

Multiplying the two equations gives

$$x^4 + x^2y^2 + y^4 = (st)^2.$$

From Theorem 2.3.2 it follows that

$$(x, y, st) = \left(k, 0, k^2\right) \quad \text{or} \quad (x, y, st) = \left(0, k, k^2\right),$$

yielding the solutions

$$(u, v, s, t) = (k, k, k, k), \quad k \in \mathbb{Z}_+.$$

Theorem 2.3.3. *All nonnegative integral solutions to the equation*

$$x^4 - x^2y^2 + y^4 = z^2 \tag{2.3.14}$$

are $(x, y, z) = \left(k, 0, k^2\right), \left(0, k, k^2\right), \left(k, k, k^2\right)$, $k \in \mathbb{Z}_+$.

Proof. We may assume that $\gcd(x, y) = 1$ and that xy is minimal. Write the equation as

$$\left(x^2 - y^2\right)^2 + (xy)^2 = z^2.$$

Suppose first that x and y are not both odd. Then

$$x^2 - y^2 = a^2 - b^2, \quad xy = 2ab,$$

for some positive integers a and b, with $\gcd(a, b) = 1$. Let $d_1 = \gcd(x, b)$ and $d_2 = \gcd(y, a)$. We have

$$x = d_1 X, \quad b = d_1 B, \quad y = d_2 Y, \quad a = d_2 A, \quad XY = 2AB.$$

Since $\gcd(X, B) = 1$ and $\gcd(Y, A) = 1$, it follows that

$$(X, Y) = (2A, B) \quad \text{or} \quad (X, Y) = (A, 2B).$$

Hence

$$x = 2d_1 A, \quad b = d_1 B, \quad y = d_2 B, \quad a = d_2 A$$

or

$$x = d_1 A, \quad b = d_1 B, \quad y = 2d_2 B, \quad a = d_2 A.$$

In the first case,

$$4d_1^2 A^2 - d_2^2 B^2 = d_2^2 A^2 - d_1^2 B^2,$$

i.e.,

$$d_1^2\Big(4A^2 + B^2\Big) = d_2^2\Big(A^2 + B^2\Big). \tag{2.3.15}$$

The condition $\gcd(a, b) = 1$ implies $\gcd(A, B) = 1$. Let $\gcd\Big(4A^2 + B^2, A^2 + B^2\Big) = D$. Then $D \mid \Big(4A^2 + B^2 - A^2 - B^2\Big) = 3A^2$, and since $A^2 + B^2 \not\equiv 0 \pmod 3$, it follows that $\gcd(D, 3) = 1$; hence $D \mid A^2$ and $D \mid \Big(A^2 + B^2 - A^2\Big) = B^2$. The condition $\gcd(A, B) = 1$ now implies $D = 1$, and from (2.3.15) we obtain

$$A^2 + B^2 = C^2 \quad \text{and} \quad 4S^2 + B^2 = D^2 \tag{2.3.16}$$

for some positive integers C and D.

We may suppose that B is odd, since if B were even, we could set $B = 2B_1$ and have a similar pair of equations. Hence from the second Pythagorean equation in (2.3.16), $B = p^2 - q^2$, $A = pq$, and $p^4 - p^2q^2 + q^4 = C^2$. Also $pq \le a \le xy/2$, and so the method of descent applies, since p and q are not both odd. It follows that $xy = 0$, yielding the solutions $\left(k, 0, k^2\right)$, $\left(0, k, k^2\right)$, $k \in \mathbb{Z}_+$.

The other alternative gives

$$d_1^2A^2 - 4d_2^2B^2 = d_2^2A^2 - d_1^2B^2,$$

and so

$$d_1^2\left(A^2 + B^2\right) = d_2^2\left(A^2 + 4B^2\right).$$

Now $A = p^2 - q^2$, $B = pq$, and $pq \le b \le xy/2$, and so the method of descent applies to the product xy.

Suppose next that x and y are both odd. Then

$$xy = a^2 - b^2, \quad x^2 - y^2 = 2ab, \text{ with } \gcd(a, b) = 1,$$

and so a and b are not both odd. Then

$$a^4 - a^2b^2 + b^4 = \left(\frac{x^2 + y^2}{2}\right)^2.$$

Hence $ab = 0$, $x = y$, giving the solution $\left(k, k, k^2\right)$, $k \in \mathbb{Z}_+$. □

Example 3. *Prove that four distinct squares cannot form an arithmetic progression.*

Solution. Let the squares be a^2, b^2, c^2, d^2, arranged in increasing order. Then

$$a^2 + c^2 = 2b^2, \quad b^2 + d^2 = 2c^2.$$

Because of these relations, we may assume without loss of generality that a, b, c, d are all odd. We have

$$a^2\Big(2c^2 - b^2\Big) = d^2\Big(2b^2 - c^2\Big),$$

and so

$$2\Big(a^2c^2 - b^2d^2\Big) = a^2b^2 - c^2d^2.$$

Setting $ac = x$, $bd = y$, $ab + cd = 2z$, $ab - cd = 2w$, we obtain

$$x^2 - y^2 = 2zw, \quad xy = z^2 - w^2,$$

yielding

$$x^4 - x^2y^2 + y^4 = \Big(z^2 + w^2\Big)^2.$$

From Theorem 2.3.3 it follows that $xy = 0$ or $x = y$. The first alternative is impossible. The second implies $w = 0$, so $ab = cd$, which is in contradiction to $a < b < c < d$.

2.3.2. Some Higher-Degree Diophantine Equations

Theorem 2.3.4. *The equation*

$$x^4 + y^4 = z^2 \tag{2.3.17}$$

is not solvable in nonzero integers.

Proof. We need only consider $x, y, z > 0$. Assume that (2.3.17) is solvable and let (x_1, y_1, z_1) be a solution with z_1 minimal. We may suppose that $\gcd(x_1, y_1, z_1) = 1$, and taking into account that $\Big(x_1^2, y_1^2, z_1\Big)$ is a primitive Pythagorean triple, it follows that

$$\gcd(x_1, y_1) = \gcd(y_1, z_1) = \gcd(z_1, x_1) = 1$$

and that x_1 and y_1 are of different parities. Assume that x_1 is odd and that y_1 is even. Note that

$$\gcd\left(z_1 - x_1^2, z_1 + x_1^2\right) = 2. \tag{2.3.18}$$

Indeed, if $d \mid \left(z_1 - x_1^2\right)$ and $d \mid \left(z_1 + x_1^2\right)$, then $d \mid 2z_1$ and $d \mid 2x_1^2$. But $\gcd(z_1, x_1) = 1$ and z_1 is odd, so $d = 2$.

Since $y_1^4 = \left(z_1 - x_1^2\right)\left(z_1 + x_1^2\right)$, it follows that one of the numbers $z_1 - x_1^2$ and $z_1 + x_1^2$ is divisible by 2 and not by 4, and that the other is divisible by 8. Therefore $y_1 = 2ab$ and either

$$z_1 - x_1^2 = 2a^4, \quad z_1 + x_1^2 = 8b^4 \tag{2.3.19}$$

or

$$z_1 - x_1^2 = 8b^4, \quad z_1 + x_1^2 = 2a^4, \tag{2.3.20}$$

where in each case a is odd and $\gcd(a, b) = 1$.

The situation (2.3.19) is not possible, because it would imply $x_1^2 = -a^4 + 4b^4$, giving $1 \equiv -1 \pmod 4$, a contradiction. Therefore we have the second alternative, i.e., $z_1 = a^4 + 4b^4$, with $0 < a < z_1$, and

$$4b^4 = \left(a^2 - x_1\right)\left(a^2 + x_1\right).$$

Since $\gcd(a, b) = 1$, we have $\gcd(a, x_1) = 1$, and we see, as in the proof of (2.3.18), that $\gcd\left(a^2 - x_1, a^2 + x_1\right) = 2$. Consequently,

$$a^2 - x_1 = 2x_2^4 \quad \text{and} \quad a^2 + x_1 = 2y_2^4,$$

where $x_2 y_2 = b$. Setting $a = z_2$, we obtain

$$x_2^4 + y_2^4 = z_2^2,$$

with $0 < z_2 < z_1$, which contradicts the minimality of z_1. □

Corollary 2.3.5. *The equation*

$$x^4 + y^4 = z^4 \tag{2.3.21}$$

is not solvable in nonzero integers.

The study of the equation

$$x^3 + y^3 = z^3 \tag{2.3.22}$$

is much more complicated and was first done by Euler.

Let m and a be integers such that $m \neq 0$ and $\gcd(a, m) = 1$. We say that a is a quadratic residue modulo m if the congruence

$$x^2 \equiv a \pmod{m}$$

is solvable. If $p > 2$ is a prime and $\gcd(a, p) = 1$, we introduce the Legendre symbol $\left(\frac{a}{p}\right)$ by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue,} \\ -1 & \text{otherwise.} \end{cases}$$

The following result due to Euler will be useful in what follows: If $p > 2$ is a prime and $\gcd(a, p) = 1$, then

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Theorem 2.3.6. *Let n be a positive integer. The Diophantine equation*

$$x^2 + 3y^2 = n$$

is solvable if and only if all prime factors of n of the form $3k - 1$ have even exponents.

Proof. We note that a prime p can be written in the form $p = x^2 + 3y^2$ if and only if $p = 3$ or $p = 3k + 1$, $k \in \mathbb{Z}_+$. Indeed, we have $3 = 0^2 + 3 \cdot 1^2$. Assume $p > 3$ and $p = x^2 + 3y^2$. Then $\gcd(x, p) = 1$ and $\gcd(y, p) = 1$. Therefore, there exists an integer y' such that $yy' \equiv 1 \pmod{p}$. From the congruence $x^2 \equiv -3y^2 \pmod{p}$ it follows that $(xy')^2 \equiv -3 \pmod{p}$. We use the quadratic reciprocity law (see Theorem 4.3.2). But $\gcd(xy', 3) = 1$ implies $\left(\frac{-3}{p}\right) = 1$, or equivalently $(-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) = 1$, i.e., $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$.

From the quadratic reciprocity law we obtain

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}.$$

Since $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$, we have $\left(\frac{p}{3}\right) = 1$, i.e., $p \equiv 1 \pmod{3}$.

Conversely, consider p a prime of the form $3k + 1$. Then there exists an integer a such that $a^2 \equiv -3 \pmod{p}$. Moreover, there exist integers x, y such that $0 < x, y < \sqrt{p}$ and $p \mid \left(a^2x^2 - y^2\right)$. It is clear that $\gcd(a, p) = 1$, and if we set $b = [\sqrt{p}]$, then $(b + 1)^2 > p$. There exist $(b + 1)^2$ pairs $(u, v) \in \{0, 1, \ldots, b\} \times \{0, 1, \ldots, b\}$ and $(b + 1)^2$ integers of the form $au + v$, where $u, v \in \{0, 1, \ldots, b\}$. It follows that there exist pairs $(u_1, v_1) \neq (u_2, v_2)$ such that $au_1 + v_1 \equiv au_2 + v_2 \pmod{p}$. Assume $u_1 \geq u_2$ and define $x = u_1 - u_2$, $y = |v_1 - v_2|$. Therefore, $0 < x, y \leq b < \sqrt{p}$ and $ax + y \equiv 0 \pmod{p}$, i.e., $a^2x^2 - y^2 \equiv 0 \pmod{p}$ (see also Theorem 4.4.3). We obtain $p \mid \left(a^2 + 3\right)x^2 - \left(3x^2 + y^2\right)$, that is, $3x^2 + y^2 = lp$, where $l \in \mathbb{Z}_+$. From the inequalities $0 < x^2 < p$, $0 < y^2 < p$, it follows that $l \in \{1, 2, 3\}$.

If $l = 1$, we have $p = 3x^2 + y^2$.

If $l = 2$, the equality $2p = 3x^2 + y^2$ is not possible, since in this case the integers x, y have the same parity and we obtain $2p \equiv 0 \pmod 4$, a contradiction.

If $l = 3$, we have $3p = 3x^2 + y^2$, and therefore $y = 3y_1$ and $p = x^2 + 3y_1^2$.

Now let us note that if $p \geq 3$ is a prime of the form $3k - 1$ and $p \mid x^2 + 3y^2$, then $p \mid x$ and $p \mid y$. Indeed, if $p \nmid x$, we have $\gcd(p, x) = 1$, so there exists an integer y' with the property $yy' \equiv 1 \pmod p$. From $x^2 \equiv -3y^2 \pmod p$ it follows that $(xy')^2 \equiv -3 \pmod p$, i.e., $\left(\frac{-3}{p}\right) = 1$ and $p \equiv 1 \pmod 3$, a contradiction.

To prove the result in Theorem 2.3.6, consider $n = a^2 b$, where b is a square-free integer. It follows that $b = \prod_{i=1}^{m} p_i$, where $p_i = 3$ or $p_i \equiv 1 \pmod 3$. Then $p_i = x_i^2 + 3y_i^2$ and $b = p_1 p_2 \cdots p_m = x^2 + 3y^2$, since it is easy to see that if $n_1 = x_1^2 + 3y_1^2$, $n_2 = x_2^2 + 3y_2^2$, then $n_1 n_2 = (x_1 x_2 + 3y_1 y_2)^2 + 3(x_1 y_2 - x_2 y_1)^2$. Finally, $n = a^2 b = (ax)^2 + 3(ay)^2$. □

Lemma 2.3.7. *The Diophantine equation*

$$x^2 + 3y^2 = z^3 \tag{2.3.23}$$

has solution (x_0, y_0, z_0) *with* z_0 *odd and* $\gcd(x_0, y_0) = 1$ *if and only if there exist integers* α, β *such that* $\alpha \not\equiv \beta \pmod 2$, $\gcd(\alpha, 3\beta) = 1$, *and*

$$x_0 = \alpha\left(\alpha^2 - 9\beta^2\right), \quad y_0 = 3\beta\left(\alpha^2 - \beta^2\right), \quad z_0 = \alpha^2 + 3\beta^2.$$

Proof. Let (x_0, y_0, z_0) be a triple of integers satisfying the above conditions. From the identity

$$\alpha^2\left(\alpha^2 - 9\beta^2\right)^2 + 3\left(3\beta\left(\alpha^2 - \beta^2\right)\right)^2 = \left(\alpha^2 + 3\beta^2\right)^3$$

it follows that (x_0, y_0, z_0) is a solution to (2.3.23).

Since $\alpha \not\equiv \beta \pmod 2$ we obtain that z_0 is odd. From $\gcd(\alpha, 3\beta) = 1$, it follows that

$$\gcd\left(\alpha, 3\beta\left(\alpha^2 - \beta^2\right)\right) = \gcd\left(\alpha, \alpha^2 - \beta^2\right) = \gcd\left(\alpha, -\beta^2\right) = 1$$

and that

$$\gcd\left(\alpha^2 - 9\beta^2, 3\beta\right) = \gcd\left(\alpha^2, 3\beta\right) = 1.$$

Taking into account the condition $\alpha \not\equiv \beta \pmod 2$, we have

$$\gcd\left(\alpha^2 - 9\beta^2, \alpha^2 - \beta^2\right) = \gcd\left(-8\beta^2, \alpha^2 - \beta^2\right)$$
$$\gcd\left(\beta^2, \alpha^2 - \beta^2\right) = \gcd\left(\beta^2, \alpha^2\right) = 1.$$

To prove the converse implication, we will use induction on the number of prime factors of z_0, where the triple (x_0, y_0, z_0) is a solution to (2.3.23) such that z_0 is odd and $\gcd(x_0, y_0) = 1$.

If $z_0 = 1$, we have $x_0 = \pm 1$, $y_0 = 0$, and $\alpha = \pm 1$, $\beta = 0$. Consider $z_0 > 1$ and let p be a prime divisor of z_0. So $z_0 = pt$, where p and t are odd. From the equality

$$(pt)^3 = x_0^2 + 3y_0^2,$$

and using the relation $\gcd(x_0, y_0) = 1$ and the result in Theorem 2.3.6, it follows that $p = 6k + 1$ and there exist integers α_1, β_1 such that

$$p = \alpha_1^2 + 3\beta_1^2.$$

Since p is a prime and $p = 6k + 1$, we obtain $\gcd(\alpha_1, 3\beta_1) = 1$ and $\alpha_1 \not\equiv \beta_1 \pmod 2$.

From the above relation we get $p^3 = a^2 + 3b^2$, where

$$a = \alpha_1\Big(\alpha_1^2 - 9\beta_1^2\Big), \quad b = 3\beta_1\Big(\alpha_1^2 - \beta_1^2\Big).$$

It is not difficult to see that $a \not\equiv b \pmod 2$ and $\gcd(a, 3b) = 1$. We have

$$\begin{aligned} P^6t^3 = p^3z_0^3 &= \Big(a^2 + 3b^2\Big)\Big(x_0^2 + 3y_0^2\Big) = (ax_0 + 3by_0)^2 + 3(bx_0 - ay_0)^2 \\ &= (ax_0 - 3by_0)^2 + 3(bx_0 + ay_0)^2. \end{aligned}$$

Also

$$\begin{aligned} (bx_0 + ay_0)(bx_0 - ay_0) &= b^2x_0^2 - a^2y_0^2 = b^2x_0^2 - \Big(p^3 - 3b^2\Big)y_0^2 \\ &= b^2\Big(x_0^2 + 3y_0^2\Big) - p^3y_0^2 = b^2z_0^3 - p^3y_0^2 \\ &= b^2p^3t^3 - p^3y_0^2. \end{aligned}$$

Therefore $p^3 \mid (bx_0 + ay_0)(bx_0 - ay_0)$. Since $\gcd(abx_0y_0, p) = 1$, it follows that the relations $p \mid bx_0 + ay_0$ and $p \mid bx_0 - ay_0$ cannot be satisfied simultaneously.

Therefore, there exists $\varepsilon \in \{-1, 1\}$ such that $bx_0 - \varepsilon ay_0 = p^3d$. We obtain $ax_0 + 3\varepsilon by_0 = p^3c$, $t^3 = c^2 + 3d^2$, and

$$x_0 = ac + 3bd, \quad y_0 = \varepsilon(bc - ad).$$

If z_0 has in its decomposition n prime factors, then since $z_0 = pt$, it follows that t has $n - 1$ prime factors. From $\gcd(x_0, y_0) = 1$ we obtain $\gcd(c, d) = 1$. Taking into account that t is odd and that it satisfies the induction hypothesis for $n - 1$, we obtain integers α_2 and β_2 satisfying the properties $\alpha_2 \not\equiv \beta_2 \pmod 2$, $\gcd(\alpha_2, 3\beta_2) = 1$,

$c = \alpha_2\left(\alpha_2^2 - 9\beta_2^2\right)$, $d = 3\beta_2\left(\alpha_2^2 - \beta_2^2\right)$ and $t = \alpha_2^2 + 3\beta_2^2$. From the above relations it follows that

$$z_0 = pt = \left(\alpha_1^2+3\beta_1^2\right)\left(\alpha_2^2+3\beta_2^2\right) = (\alpha_1\alpha_2+3\beta_1\beta_2)^2+3(\alpha_1\beta_2-\alpha_2\beta_1)^2.$$

Writing

$$\alpha = \alpha_1\alpha_2 + 3\beta_1\beta_2, \quad \beta = \varepsilon(\alpha_2\beta_1 - \alpha_1\beta_2),$$

we obtain $z_0 = \alpha^2 + 3\beta^2$ and

$$x_0 = \alpha\left(\alpha^2 - 9\beta^2\right), \quad y_0 = 3\beta\left(\alpha^2 - \beta^2\right).$$

Finally, $\alpha - \beta \equiv \alpha_1\alpha_2 + \beta_1\beta_2 - (\alpha_1\beta_2 + \alpha_2\beta_1) \equiv (\alpha_1 - \beta_1)(\alpha_2 - \beta_2) \pmod 2$, so $\alpha \not\equiv \beta \pmod 2$. From $\gcd(x_0, y_0) = 1$ it follows that $\gcd(\alpha, 3\beta) = 1$. □

Theorem 2.3.8. *Equation (2.3.22) is not solvable in nonzero integers.*

Proof. Assume that (2.3.22) is solvable and let (x_0, y_0, z_0) be a solution with $x_0y_0z_0 \neq 0$ and $|x_0y_0z_0|$ minimal.

It is clear that two of the integers x_0, y_0, z_0 are odd. Let us assume that x_0 and y_0 have this property. Set

$$x_0 + y_0 = 2u \quad \text{and} \quad x_0 - y_0 = 2v,$$

and we can assume that $u > 0$.

We obtain $x_0 = u+v$, $y_0 = u-v$, and from (2.3.22) it follows that

$$2u\left(u^2 + 3v^2\right) = z_0^3. \tag{2.3.24}$$

Since x_0 is odd, we have that u and v are of different parities, i.e., $u^2 + 3v^2$ is odd. From $\gcd(x_0, y_0) = 1$ we obtain $\gcd(u, v) = 1$ and $\gcd\left(2u, u^2 + 3v^2\right) = \gcd\left(u, u^2 + 3v^2\right) = \gcd\left(u, 3v^2\right) = \gcd(u, 3)$.

Case 1. If $\gcd(u,3)=1$, then from (2.3.24) it follows that

$$2u=t^3,\quad u^2+3v^2=s^3,\quad \text{and}\quad ts=z_0.$$

From Lemma 2.3.7, we obtain that there exist integers α,β such that $\gcd(\alpha,3\beta)=1$, $\alpha\not\equiv\beta \pmod 2$, and

$$s=\alpha^2+3\beta^2,\quad u=\alpha\Big(\alpha^2-9\beta^2\Big),\quad v=3\beta\Big(\alpha^2-\beta^2\Big).$$

Therefore, $2u=t^3=(2\alpha)(\alpha-3\beta)(\alpha+3\beta)$. The factors 2α, $\alpha-3\beta$, $\alpha+3\beta$ are pairwise relatively prime, so

$$2\alpha=z^3,\quad \alpha-3\beta=X^3,\quad \alpha+3\beta=Y^3.$$

We obtain

$$X^3+Y^3=Z^3$$

and $XYZ\neq 0$, i.e., (X,Y,Z) is a nonzero integral solution to (2.3.22). Moreover,

$$\begin{aligned}|XYZ|&=\sqrt[3]{|2\alpha(\alpha^2-9\beta^2)|}=\sqrt[3]{2u}=\sqrt[3]{x_0+y_0}\\&<|\sqrt[3]{x_0y_0}|<|x_0y_0z_0|,\end{aligned}$$

which contradicts the minimality of $|x_0y_0z_0|$.

Case 2. If $\gcd(u,3)=3$, then $u=3u_1$, and from (2.3.24) it follows that $z_0=3z_1$ and

$$2u_1(3u_1^2+v^2)=3z_1^3. \tag{2.3.25}$$

Taking into account that $\gcd(u,v)=1$, we obtain $\gcd(v,3)=1$ and $\gcd\Big(3u_1^2+v^2,3\Big)=1$. From (2.3.25) it follows that $u_1=3u_2$, $u_2\in\mathbb{Z}$, and $2u_2\Big(3u_1^2+v^2\Big)=z_1^3$.

Since $\gcd\left(2u_2, 3u_1^2 + v^2\right) = 1$, we obtain

$$2u_2 = m^3 \quad \text{and} \quad 3u_1^2 + v^2 = n^3,$$

where n is an odd integer.

Applying Lemma 2.3.7, it follows that there exist integers α, β such that $\gcd(\alpha, 3\beta) = 1$, $\alpha \not\equiv \beta \pmod 2$, and $v = \alpha(\alpha^2 - 9\beta^2)$, $u_1 = 3\beta(\alpha^2 - \beta^2)$. Therefore $u_2 = \beta\left(\alpha^2 - \beta^2\right)$ and $m^3 = 2\beta(\alpha - \beta)(\alpha + \beta)$.

Taking into account that the integers 2β, $\alpha - \beta$, and $\alpha + \beta$ are pairwise relatively prime, we obtain $\alpha - \beta = X^3$, $\alpha + \beta = Z^3$, $2\beta = Y^3$, for some nonzero integers X, Y, Z. It follows that

$$X^3 + Y^3 = Z^3$$

and

$$|XYZ| = \sqrt[3]{\left|2\beta\left(\alpha^2 - \beta^2\right)\right|} < \left|\sqrt[3]{2u}\right| = \left|\sqrt[3]{x_0 + y_0}\right| < \left|x_0 y_0 z_0\right|,$$

which contradicts the minimality of $|x_0 y_0 z_0|$. □

Remarks. (1) Equations (2.3.21) and (2.3.22) are special cases of Fermat's equation

$$x^n + y^n = z^n, \tag{2.3.26}$$

where n is an integer greater than 2 and x, y, z are nonzero integers.

Fermat's last theorem states that equation (2.3.26) has no nonzero integer solutions for x, y, z when $n > 2$.

Around 1630, Fermat wrote a note in the margin of a page of Diophantus's *Arithmetica*:

"I have discovered a truly remarkable proof which this margin is too small to contain."

Fermat apparently had found a proof only for the case $n = 4$, but when his marginal note was published, this theorem became famous, capturing the attention of the mathematics world and remaining for centuries the last of Fermat's Theorems yet to be proved.

Through the years, many important mathematicians worked on special cases and solved them affirmatively. We mention here Euler ($n = 3$), Sophie Germain (n and $2n + 1$ are primes, $n < 100$, and x, y, z are not divisible by n), Dirichlet ($n = 5$, $n = 14$), and Lamé ($n = 7$). Liouville and Kummer developed important mathematical theories in their attempts to prove Fermat's last theorem.

Using techniques based on Kummer's work, Fermat's Last Theorem was proved true, with the help of computers, for n up to 4,000,000 by 1993.

In 1983, a major contribution was made by Gerd Faltings, who proved that for every $n > 2$ there are at most a finite number of relatively prime integers satisfying equation (2.3.26).

The proof of Fermat's last theorem was almost completed in 1993 by Andrew Wiles, a British mathematician working at Princeton in the USA. Wiles gave a series of three lectures at the Isaac Newton Institute in Cambridge, England, the first on Monday, June 21, and the second on June 22. In the final lecture on Wednesday, June 23, 1993, Wiles announced his proof of Fermat's last theorem as a corollary to his main results. His proof turned to be incomplete.

In October, 1994, Wiles sent a new proof to three colleagues, including Faltings. All accepted the new proof, which was essentially simpler than the earlier one.

Pierre de Fermat died in 1665. Today we think of Fermat as a number theorist, in fact as perhaps the most famous number theorist who ever lived. It is therefore surprising to find that Fermat was in fact a lawyer and only an amateur mathematician. Also surprising may be the fact that he published only one mathematical paper in his life, and that was an anonymous article written as an appendix to a colleague's book. But perhaps it is less surprising when we note that there were no mathematical journals at the time, and most scientific communication was carried on by private correspondance.

(2) Euler conjectured that the equation

$$x^n + y^n + z^n = w^n \tag{2.3.27}$$

has no integral solution if n is an integer greater than or equal to 4.

In 1988, Noam Elkies gave the following counterexample:

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Subsequently, Roger Frye (1988) found the smallest solution to (2.3.27):

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

Example 4. *The equation*

$$x^4 - y^4 = z^2 \tag{2.3.28}$$

is not solvable in nonzero integers.

Solution. We may assume that $x, y, z > 0$ and consider a solution (x, y, z) with $\gcd(x, y) = 1$ and x minimal. Then $\left(y^2, z, x^2\right)$ is a primitive Pythagorean triple, so we have the following two cases:

Case 1: $y^2 = a^2 - b^2$, $z = 2ab$, $x^2 = a^2 + b^2$,

where $a > b > 0$ and $\gcd(a, b) = 1$. It follows that

$$a^4 - b^4 = (xy)^2$$

and $a < x$, contradicting the minimality of x.

Case 2: $y^2 = 2ab$, $z = a^2 - b^2$, $x^2 = a^2 + b^2$,

where $a > b > 0$ and $\gcd(a, b) = 1$.

Since (a, b, x) is also a primitive Pythagorean triple, we may assume that a is even and b is odd. Then $a = 2p^2$ and $b = q^2$ for some positive integers p, q with $\gcd(p, q) = 1$ and $q \equiv 1 \pmod 2$. It follows that

$$x^2 = 4p^4 + q^4 \quad \text{and} \quad y = 2pq.$$

Hence $\left(2p^2, q^2, x\right)$ is itself a primitive Pythagorean triple, and so

$$p^2 = rs, \quad q^2 = r^2 - s^2$$

for some positive integers r, s with $r > s$ and $\gcd(r, s) = 1$.

Finally, $r = u^2$, $s = v^2$, for some positive integers u, v with $\gcd(u, v) = 1$. Then

$$u^4 - v^4 = q^2$$

and $u = \sqrt{r} \le p < 2p^2 < x$, which contradicts the minimality of x. □

Alternative Proof. We may assume that $x, y, z > 0$ and that $\gcd(x, y) = 1$. Write the equation as

$$\left(x^2 - y^2\right)\left(x^2 + y^2\right) = z^2.$$

It is not difficult to see that

$$\gcd\left(x^2 - y^2, x^2 + y^2\right) = 1 \quad \text{or} \quad \gcd\left(x^2 - y^2, x^2 + y^2\right) = 2.$$

In the first case, we obtain the system

$$\begin{cases} x^2 + y^2 = u^2, \\ x^2 - y^2 = v^2, \end{cases}$$

which, according to Example 2 in Section 2.2, is not solvable.

In the second case, we obtain

$$\begin{cases} x^2 - y^2 = 8r^2, \\ x^2 + y^2 = 2s^2, \end{cases}$$

hence

$$\begin{cases} s^2 + (2r)^2 = x^2, \\ s^2 - (2r)^2 = y^2, \end{cases}$$

which, by the same argument, is not solvable. □

Example 5. *Solve in integers the equation*

$$x^4 + y^4 = 2z^2.$$

Solution. Without loss of generality, we may assume that

$$\gcd(x, y) = 1.$$

Then x and y are both odd, and

$$z^4 - (xy)^4 = \left(\frac{x^4 - y^4}{2}\right)^2.$$

From Example 4 it follows that $xyz = 0$ or $x^4 - y^4 = 0$, and so $x = y = z = 0$ or $x^2 = y^2 = z$.

The solutions are $\left(k, k, k^2\right)$, $k \in \mathbb{Z}$.

Example 6. *Solve in integers the equation*

$$x^4 + 6x^2y^2 + y^4 = z^2.$$

Solution. Let (x, y, z) be a solution to the equation. Then

$$(2x)^4 + 6(2x)^2(2y)^2 + (2y)^4 = (4z)^2.$$

Setting $2x = u + v$, $2y = u - v$, where $u, v \in \mathbb{Z}$, we obtain the equation

$$(u+v)^4 + 6\Big(u^2 - v^2\Big)^2 + (u-v)^4 = 16z^2,$$

which is equivalent to

$$u^4 + v^4 = 2z^2.$$

From the previous example it follows that $(u, v, z) = \Big(k, k, k^2\Big)$, yielding the solutions $(x, y, z) = \Big(k, 0, k^2\Big)$ and $(x, y, z) = \Big(0, k, k^2\Big)$, $k \in \mathbb{Z}$.

Remark. Another variant of this problem was given in the second part of Problem 2 in Section 2.2.

Exercises and Problems

1. Let p be a prime. Find all solutions to the equation

$$a + b - c - d = p,$$

where a, b, c, d are positive integers such that $ab = cd$.

(Mathematical Reflections)

2. Let a, b, c be integers such that

$$\gcd(a, b, c) = 1 \text{ and } ab + bc + ca = 0.$$

Prove that $|a + b + c|$ can be expressed in the form $x^2 + xy + y^2$, where x, y are integers.

3. Prove that the equation $x^2 + xy + y^2 = 36^2$ is not solvable in positive integers.

4. Find all pairs of positive integers such that

$$x^2 - xy + y^2 = 727.$$

(Turkish Mathematical Olympiad)

5. We say that the positive integer z satisfies property (P) if $z = x^2 + xy + y^2$, for some positive integers x and y. Prove that:

(a) if z satisfies property (P), then so does z^2;

(b) if z^2 satisfies property (P) with the additional condition that $\gcd(x, y) = 1$, then so does z.

(Dorin Andrica)

6. Solve in integers the equation $x^2 + 3y^2 = 4z^2$.

7. Find all triples (x, y, z) of nonnegative integers satisfying the equation $x^4 + 14x^2y^2 + y^4 = z^2$.

(Ion Cucuruzeanu)

8. Solve in positive integers the equation

$$3x^4 + 10x^2y^2 + 3y^4 = z^2.$$

9. Find all distinct squares a^2, b^2, c^2 that form an arithmetic progression.

10. Solve in integers the equation $xy\Big(x^2 + y^2\Big) = 2z^2$.

(Titu Andreescu)

11. Find all integral triples (x, y, z) satisfying the equation

$$x^4 - 6x^2y^2 + y^4 = z^2.$$

12. If a and b are distinct positive integers, then $2a(a^2 + 3b^2)$ is not a cube.

13. Prove that equation $x^6 - y^6 = 4z^3$ is not solvable in positive integers.

(Titu Andreescu)

14. Prove that the system of equations

$$\begin{cases} x + y = z^2, \\ xy = \dfrac{z^4 - z}{3}, \end{cases}$$

is not solvable in nonzero integers.

(Titu Andreescu)

http://www.springer.com/978-0-8176-4548-9

An Introduction to Diophantine Equations
A Problem-Based Approach
Andreescu, T.; Andrica, D.; Cucurezeanu, I.
2010, XI, 345 p., Hardcover
ISBN: 978-0-8176-4548-9
A product of Birkhäuser Basel