Some solved exercises with linear Diophantine equations, including problems ("maths word problems") whose solving comes down to solving such equations, can be found in [1, 228, 335].

10.2 Pythagorean triangles

Definition 10.2. *An ordered triple of positive integers (x, y, z) is called a* Pythagorean triple *if x and y are the leg lengths, and z the hypotenuse length of a right-angled triangle, i.e. if*

$$x^2 + y^2 = z^2. \tag{10.8}$$

If x, y, z are relatively prime, we then say that (x, y, z) is a primitive Pythagorean triple. *We call such a triangle a (primitive) Pythagorean triangle. Note that from $\gcd(x, y, z) = 1$ and (10.8) it follows that $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$.*

A very interesting booklet [370] whose author is the Polish mathematician Wacław Sierpiński (1882 – 1969) deals with Pythagorean triangles. That topic is, of course, present in many other books on number theory, and also in books written for a wide audience, such as the beautifully written book in "recreational mathematics" [32]. The two mentioned books were basic references for the paper [110], which we will follow in this section.

An important step in considering Pythagorean triples is determining formulas which provide all solutions of Diophantine equation (10.8). Let us first solve a few examples for which it is not necessary to know these formulas.

Example 10.4. *Prove that in every Pythagorean triangle:*

a) the length of at least one leg is divisible by 3,

b) the length of at least one leg is divisible by 4,

c) the length of at least one side is divisible by 5.

Solution: Without loss of generality, we can assume that the Pythagorean triple (x, y, z) is primitive.

a) Note that the square of an integer which is not divisible by 3 is congruent to 1 modulo 3. Indeed, $(3k \pm 1)^2 = 3(3k^2 \pm 2k) + 1$. Therefore, if neither x nor y were divisible by 3, then z^2 would be congruent to 2 modulo 3, which is impossible because we have just shown that the square of an integer is congruent to 0 or 1 modulo 3.

b) We showed in Example 5.15 that the square of an odd number is congruent to 1 modulo 8. From this, it follows that x and y cannot both be odd because, otherwise, the number z^2 would be congruent to 2 modulo 8, i.e. it would be even, but it would not be divisible by 4. Hence, due to primitivity, we can assume that x is odd, and y is even. Now, z is odd, so from $y^2 = z^2 - x^2$, we conclude that y^2 is divisible by 8 and that y is divisible by 4.

c) From Example 4.1, we know that the square of an integer is congruent to 0, 1 or 4 modulo 5. Let us now assume that neither x nor y are divisible by 5. This means that the number $x^2 + y^2$ is congruent to 0, 2 or 3 modulo 5. However, z^2 as the square of an integer, cannot be congruent to 2 or 3 modulo 5, so we conclude that z^2 is divisible by 5, so z is also divisible by 5. ♢

Example 10.5.

a) Find all Pythagorean triples which consist of three consecutive positive integers.

b) Find all Pythagorean triples which consist of three consecutive elements of an arithmetic progression.

Solution:

a) From the condition $(n-1)^2 + n^2 = (n+1)^2$, we obtain $n^2 = 4n$ and $n = 4$. Therefore, the only Pythagorean triple with the required property is the triple $(3, 4, 5)$.

b) Let $(n-k, n, n+k)$ be a Pythagorean triple with the required property. Then $(n-k)^2 + n^2 = (n+k)^2$, which implies that $n = 4k$. Hence, required triples have the form $(3k, 4k, 5k)$ for a positive integer k. ♢

Let us now move on to solving equation (10.8). It is sufficient to consider the case when x, y and z are relatively prime, because if they have a common factor $d > 1$, then equation (10.8) can be divided by d^2. Let us also notice that, by example 10.4.b), in every Pythagorean triangle, the length of at least one leg has to be even, while in every primitive Pythagorean triangle, the length of one leg is even and the other is odd.

Theorem 10.4. *All primitive Pythagorean triples (x, y, z), in which y is even, are given by the formulas*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2, \tag{10.9}$$

where $m > n$ and m, n are relatively prime positive integers of different parity.

Proof: Equation (10.8) can be written in the form $y^2 = (z+x)(z-x)$. Let $y = 2c$. The numbers $z+x$ and $z-x$ are even, so there are positive integers a and b such that $z+x = 2a$, $z-x = 2b$. Now,

$$c^2 = ab.$$

Since $z = a+b$, $x = a-b$ and $\gcd(x,z) = 1$, we conclude that $\gcd(a,b) = 1$. By Proposition 2.14 (which is a consequence of the fundamental theorem of arithmetic), we conclude that there are $m, n \in \mathbb{N}$, $\gcd(m,n) = 1$, such that $a = m^2$, $b = n^2$. From this,

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

The numbers m and n have to be of different parity because the number $x = m^2 - n^2$ is odd.

It is easily checked that the numbers x, y, z, defined by (10.9), satisfy (10.8). It also needs to be checked that they are relatively prime. Let us assume that $\gcd(x,z) = d > 1$. Then d is odd, $d \mid (m^2+n^2)+(m^2-n^2) = 2m^2$ and $d \mid (m^2+n^2)-(m^2-n^2) = 2n^2$. However, this is a contradiction to the assumption that m and n, and therefore also m^2 and n^2, are relatively prime. Hence, $\gcd(x,z) = 1$ and $\gcd(x,y,z) = 1$. □

From Theorem 10.4, it follows that all Pythagorean triples are given by the identity

$$(d(m^2-n^2))^2 + (2dmn)^2 = (d(m^2+n^2))^2. \tag{10.10}$$

Let us now list Pythagorean triples whose all elements are ≤ 50:

$$\begin{array}{ccccc}
(3,4,5), & (6,8,10), & (5,12,13), & (9,12,15), & (8,15,17),\\
(12,16,20), & (15,20,25), & (7,24,25), & (10,24,26), & (20,21,29),\\
(18,24,30), & (16,30,34), & (21,28,35), & (12,35,37), & (15,36,39),\\
(24,32,40), & (9,40,41), & (27,36,45), & (30,40,50), & (14,48,50).
\end{array}$$

We see that there are 20 such triples (if we consider the triples (x,y,z) and (y,x,z) to be equal). There are 7 primitive triples among them. Let us mention that in 1900, Lehmer proved that the number $P_h(n)$ of primitive Pythagorean triangles with the hypotenuse length $\leq n$ is approximately equal to $\frac{n}{2\pi}$ (see [398, Chapter 13.1]).

Example 10.6. If we choose $m = n+1$ in (10.9), we obtain:

$$x = 2n+1, \quad y = 2n(n+1), \quad z = 2n(n+1)+1.$$

If we put here $n = 10^s$, we obtain:

$$x = 2 \cdot 10^s + 1, \quad y = 2 \cdot 10^{2s} + 2 \cdot 10^s, \quad z = 2 \cdot 10^{2s} + 2 \cdot 10^s + 1.$$

In this manner, we have a simple method for generating Pythagorean triples such that $z = y + 1$:

$$(21, 220, 221),$$

$$(201, 20200, 20201),$$

$$(2001, 2002000, 2002001),$$

$$(20001, 200020000, 200020001), \ldots$$

Example 10.7. *Find all Pythagorean triangles such that the length of one side is equal to*

a) 39*,*

b) 1999*.*

Solution:

a) All Pythagorean triples are given by identity (10.10). In this case, we have three possibilities: $d = 1$, $d = 3$, $d = 13$. Namely, the possibility $d = 39$ can be discarded because the equations $m^2 - n^2 = 1$ and $m^2 + n^2 = 1$ do not have solutions in positive integers.

If $d = 1$, then $m^2 + n^2 \neq 39$ by Theorem 5.7, so it has to be $m^2 - n^2 = (m-n)(m+n) = 39$. This yields $m - n = 1$, $m + n = 39$ or $m - n = 3$, $m + n = 13$, and we get $m = 20$, $n = 19$ or $m = 8$, $n = 5$. In this way, we obtain Pythagorean triples $(39, 760, 761)$ and $(39, 80, 89)$.

If $d = 3$, then $m^2 - n^2 = 13$ or $m^2 + n^2 = 13$, which gives $m = 7$, $n = 6$ or $m = 3$, $n = 2$. The obtained triples are $(39, 252, 255)$ and $(15, 36, 39)$.

If $d = 13$, then $m^2 - n^2 = 3$. We obtain $m = 2$, $n = 1$, which gives the triple $(39, 52, 65)$.

b) The number 1999 is prime, so the only possibility is $d = 1$. The equation $m^2 + n^2 = 1999$ does not have solutions because $1999 \equiv 3 \pmod 4$, while from $m^2 - n^2 = 1999$, it follows that $m = 1000$, $n = 999$ and the only triple is $(1999, 1998000, 1998001)$. ♢

Example 10.8. *Find all primitive Pythagorean triangles for which the lengths of all three sides are between* 2000 *and* 3000*.*

Solution: Let (x, y, z) be a Pythagorean triple with the required property. Then $2000^2 + x^2 \leq 3000^2$, so $2000 \leq x \leq 2236$. Similarly, $2000 \leq y \leq 2236$. We also have $z^2 \geq 2000^2 + 2000^2$, so $2829 \leq z \leq 3000$. By Theorem 10.4, there are positive integers m and n such that $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$. From considerations so far, we have:

$$2829 \leq m^2 + n^2 \leq 3000, \tag{10.11}$$

$$2000 \leq m^2 - n^2 \leq 2236, \tag{10.12}$$

$$2000 \leq 2mn \leq 2236. \tag{10.13}$$

By adding (10.11) and (10.12), we obtain $50 \leq m \leq 51$. If we insert this in (10.13), we obtain $20 \leq n \leq 22$. Finally, from (10.11), we obtain $m^2 \leq 3000 - 20^2 = 2600 < 2601 = 51^2$. Hence, $m = 50$, so the number n has to be odd, which means that $n = 21$. Thus, the only such Pythagorean triple is $(2059, 2100, 2941)$. ♢

In a Pythagorean triangle, by definition, the lengths of sides are positive integers. The question arises of whether some other elements of that triangle can also be positive integers.

The following example is one of the exercises from the sixth part of Diophantus' book *Arithmetics*. It can be found in English translation in [213].

Example 10.9. *Find a Pythagorean triangle such that the length of the bisector segment of an acute angle is a positive integer.*

Solution: Let triangle ABC satisfy the conditions and let the bisector of the angle α intersect the line segment $\overline{BC}$ at the point D. Let us introduce the following notation: $|\overline{BC}| = x$, $|\overline{AC}| = y$, $|\overline{AB}| = z$, $|\overline{AD}| = s$, $|\overline{CD}| = u$. Since the angle bisector divides the opposite side into parts proportional to the adjacent sides (see [209, Book III, Chapter 1], [336, Chapter 3.2.2.4]), we obtain the system of equations:

$$x^2 + y^2 = z^2, \tag{10.14}$$

$$u^2 + y^2 = s^2, \tag{10.15}$$

$$\frac{u}{x - u} = \frac{y}{z}. \tag{10.16}$$

By the assumptions, numbers x, y, z, s are positive integers. From (10.16), the number u is rational, so from (10.15), we conclude that u is also a positive integer. Let (p, q, r) be a primitive Pythagorean triple such that $u =$

pt, $y = qt$, $s = rt$. From (10.16), it follows that $z = \frac{q(x-pt)}{p}$. If we substitute this in (10.14), we obtain

$$x^2 + q^2t^2 = \frac{q^2x^2 - 2pq^2xt + p^2q^2t^2}{p^2}$$

and

$$p^2x = q^2x - 2pq^2t.$$

From this, we obtain $t = \frac{q^2-p^2}{2pq^2}x$. For this number to be an integer, it suffices that $x = 2pq^2k$, for $k \in \mathbb{N}$. Then $t = (q^2 - p^2)k$, so $y = q(q^2 - p^2)k$, $z = q(q^2 + p^2)k$, $s = r(q^2 - p^2)k$. In particular, if we choose $p = 3$, $q = 4$, $r = 5$, $k = 1$ (as it was done by Diophantus), we obtain the Pythagorean triple $(28, 96, 100)$ with a corresponding bisector segment of the length 35. □

From Example 10.4.b), it follows that the area of each Pythagorean triangle is a positive integer. We come to the question of whether there is a Pythagorean triangle whose area is a perfect square. Before we answer this question, let us consider the problem of the existence of Pythagorean triples in which the length of one or more sides is a perfect square. We will see that these two problems are closely related.

Example 10.10. *Prove that there are infinitely many primitive Pythagorean triangles whose:*

a) length of the hypotenuse,

b) length of one leg

is a perfect square.

Solution:

a) Let (n, m, p), where $n < m < p$, be a primitive Pythagorean triple. If numbers x, y and z are defined by formula (10.9), then by Theorem 10.4, (x, y, z) is a primitive Pythagorean triple such that

$$z = m^2 + n^2 = p^2.$$

b) Statement b) is a direct consequence of the identity

$$(k^4 - 4)^2 + (4k^2)^2 = (k^4 + 4)^2.$$ ♢

Theorem 10.5. *The equation $x^4 + y^4 = z^2$ does not have solutions in positive integers. In other words, there does not exist a right-angled triangle whose lengths of legs are squares of positive integers.*

Proof: Let us assume that such a triangle exists and choose among all such triangles the one with the shortest hypotenuse. In this manner, we obtain a Pythagorean triple (x^2, y^2, z). Let us show that x and y are relatively prime. Otherwise, it would be $x = ad$, $y = bd$ with $d > 1$. Then, from $z^2 = d^4(a^4 + b^4)$, it would follow that there exists $c \in \mathbb{N}$ such that $z = cd^2$, and we would obtain the Pythagorean triple (a^2, b^2, c) whose length of the hypotenuse is less than z, which is a contradiction.

Therefore, (x^2, y^2, z) is a primitive Pythagorean triple, so by Theorem 10.4 (if we choose that y is even), there are relatively prime positive integers m, n of different parity such that

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

From $x^2 + n^2 = m^2$, it follows that n is even and m is odd. If we put $n = 2k$, $y = 2t$, we obtain

$$t^2 = mk.$$

This implies that there are positive integers r and s such that $m = r^2$ and $k = s^2$. Since (x, n, m) is a primitive Pythagorean triple, by Theorem 10.4, there are u, v such that $\gcd(u, v) = 1$, $n = 2uv$, $m = u^2 + v^2$. Now from $n = 2s^2$, it follows that $s^2 = uv$, so there are $a, b \in \mathbb{N}$ such that $u = a^2$, $v = b^2$. Therefore, $a^4 + b^4 = r^2$, so (a^2, b^2, r) is a Pythagorean triple whose hypotenuse length satisfies $r < r^2 = m < m^2 + n^2 = z$, which is a contradiction to the minimality of z. □

Remark 10.1. From Theorem 10.5, it follows that the equation $x^4 + y^4 = z^4$ does not have solutions in positive integers. This is a special case of the famous Fermat's Last Theorem, which states that the equation $x^n + y^n = z^n$ does not have solutions in positive integers for $n \geq 3$. This theorem was proved by Andrew Wiles in 1995 (more about the proof can be found in [214] and [319, Chapter 24]).

Proposition 10.6. *There does not exist a Pythagorean triangle whose length of the hypotenuse and length of one leg are perfect squares.*

Proof: Suppose the contrary, and let (x, y, z) be a Pythagorean triple with the shortest hypotenuse which has the given property. It is clear that the triple (x, y, z) is primitive. Let $x = a^2$, $z = c^2$.

If y is even, then there are $m, n \in \mathbb{N}$ such that

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

From this, we get $(ac)^2 = m^4 - n^4$, so in the Pythagorean triple (n^2, ac, m^2), the length of the hypotenuse is $m^2 < z$, which is a contradiction.

Accordingly, y has to be odd, which means that a is even. From $y^2 = c^4 - a^4 = (c^2 - a^2)(c^2 + a^2)$, it follows that there are positive integers r, s such that

$$c^2 - a^2 = r^2, \quad c^2 + a^2 = s^2.$$

This implies $2c^2 = r^2 + s^2$ and $c^2 = (\frac{s+r}{2})^2 + (\frac{s-r}{2})^2$. Thus, there are $m, n \in \mathbb{N}$ such that

$$\frac{s \pm r}{2} = m^2 - n^2, \quad \frac{s \mp r}{2} = 2mn, \quad c = m^2 + n^2,$$

so $2a^2 = s^2 - r^2 = 8mn(m-n)(m+n)$. Since m and n are relatively prime numbers of different parity, the numbers m, n, $m-n$ and $m+n$ are pairwise coprime. Therefore, there exist $k, l, p, q \in \mathbb{N}$ such that

$$m = k^2, \quad n = l^2, \quad m - n = p^2, \quad m + n = q^2.$$

From this, we have $k^4 - l^4 = (pq)^2$, so we obtained the Pythagorean triple (l^2, pq, k^2) with the length of the hypotenuse $k^2 = m < m^2 + n^2 = c < c^2 = z$, which is a contradiction. □

Corollary 10.7. *There does not exist a Pythagorean triangle whose area is a perfect square.*

Proof: Suppose that such a triangle (x, y, z) exists. Then

$$x^2 + y^2 = z^2 \quad \text{and} \quad xy = 2P.$$

By the assumption, there is $u \in \mathbb{N}$ such that $P = u^2$, i.e. $2xy = (2u)^2$. Now,

$$z^2 + (2u)^2 = (x + y)^2, \quad z^2 - (2u)^2 = (x - y)^2.$$

From this, we get $z^4 = (2u)^4 + (x^2 - y^2)^2$. Hence, we obtained a Pythagorean triangle whose hypotenuse is of length z^2, and one leg of length $(2u)^2$, which is a contradiction with Proposition 10.6. □

Numerous generalizations of the Pythagorean equation have been studied (for a detailed overview of results until the beginning of the 20th century, see [105]). In the following theorem, we will consider one such generalization (according to [73, Chapter 10]).

Theorem 10.8. *All solutions of the equation*

$$x^2 + y^2 + z^2 = u^2 \tag{10.17}$$

in relatively prime positive integers are given by the identity

$$(a^2 + b^2 - c^2 - d^2)^2 + (2(ad \mp bc))^2 + (2(ac \pm bd))^2 = (a^2 + b^2 + c^2 + d^2)^2.$$

Proof: Since $u^2 \equiv 0$ or $1 \pmod 4$, we conclude that exactly one of the numbers x, y, z is odd, so u is odd. Let x be odd, while y and z are even. Write equation (10.17) in the form

$$y^2 + z^2 = (u^2 - x^2) = (u + x)(u - x).$$

Assume that a prime number $p \equiv 3 \pmod 4$ divides $u + x$ and $u - x$. Then $p \mid x$, $p \mid u$, while from $p \mid (y^2 + z^2)$ and Proposition 5.2, it follows that $p \mid y$, $p \mid z$, which is a contradiction to the assumption that $\gcd(x, y, z, u) = 1$. If p divides one of the numbers $u + x$, $u - x$, then, by Theorem 5.7, it divides it to an even power. Now, again by applying Theorem 5.7, we conclude that numbers $(u + x)/2$ and $(u - x)/2$ are sums of two squares. Therefore, there are integers a', b', c', d' such that

$$u + x = 2(a'^2 + b'^2), \quad u - x = 2(c'^2 + d'^2).$$

From this, we have $u = a'^2 + b'^2 + c'^2 + d'^2$, $x = a'^2 + b'^2 - c'^2 - d'^2$ and with the notation $y = 2y_1$, $z = 2z_1$, we get

$$y_1^2 + z_1^2 = (a'^2 + b'^2)(c'^2 + d'^2).$$

Let r_1 be the product of all prime numbers $p \equiv 3 \pmod 4$ which divide a' and b', and let r_2 be the product of all prime numbers $p \equiv 3 \pmod 4$ which divide c' and d'. Let us denote $a' = r_1 a_1$, $b' = r_1 b_1$, $c' = r_2 c_1$, $d' = r_2 d_1$ $y_1 = r_1 r_2 y_2$, $z_1 = r_1 r_2 z_2$, so that

$$y_2^2 + z_2^2 = (a_1^2 + b_1^2)(c_1^2 + d_1^2). \tag{10.18}$$

All prime factors of $(a_1^2 + b_1^2)$ and $(c_1^2 + d_1^2)$ in (10.18) are $\equiv 1 \pmod 4$. We claim that

$$y_2 = a_2 d_2 \mp b_2 c_2, \quad z_2 = a_2 c_2 \pm b_2 d_2 \tag{10.19}$$

for some a_2, b_2, c_2, d_2 such that $a_2^2 + b_2^2 = a_1^2 + b_1^2$, $c_2^2 + d_2^2 = c_1^2 + d_1^2$.

When we prove this claim, the proof of the theorem will be complete. Indeed, if we denote $a = r_1a_2$, $b = r_1b_2$, $c = r_2c_2$, $d = r_2d_2$, then

$$u = a'^2 + b'^2 + c'^2 + d'^2 = r_1^2(a_1^2 + b_1^2) + r_2^2(c_1^2 + d_1^2) = a^2 + b^2 + c^2 + d^2,$$
$$x = a'^2 + b'^2 - c'^2 - d'^2 = r_1^2(a_1^2 + b_1^2) - r_2^2(c_1^2 + d_1^2) = a^2 + b^2 - c^2 - d^2,$$
$$y = 2r_1r_2y_2 = 2r_1r_2(a_2d_2 \mp b_2c_2) = 2(ad \mp bc),$$
$$z = 2r_1r_2z_2 = 2r_1r_2(a_2c_2 \pm b_2d_2) = 2(ac \pm bd).$$

Therefore, it remains to prove (10.19). We will prove this statement by the induction on the number of prime factors of $a_1^2 + b_1^2$. Recall that a prime number $\equiv 1 \pmod 4$ has a unique representation in the form of a sum of two squares (Proposition 5.6). If $a_1^2 + b_1^2$ is prime, then from (10.18) we obtain

$$c_1^2 + d_1^2 = \Big(\frac{y_2a_1 \mp z_2b_1}{a_1^2 + b_1^2}\Big)^2 + \Big(\frac{y_2b_1 \pm z_2a_1}{a_1^2 + b_1^2}\Big)^2.$$

Since $(y_2a_1 - z_2b_1)(y_2a_1 + z_2b_1) = y_2^2a_1^2 - z_2^2b_1^2 \equiv a_1^2(y_2^2 + z_2^2) \equiv 0 \pmod{a_1^2 + b_1^2}$, for one of the choices of signs, the numbers $u = \frac{y_2a_1 \mp z_2b_1}{a_1^2 + b_1^2}$, $v = \frac{y_2b_1 \pm z_2a_1}{a_1^2 + b_1^2}$ are integers and $u^2 + v^2 = c_1^2 + d_1^2$, $a_1u + b_1v = y_2$, $a_1v - b_1u = \pm z_2$, so we proved the basis of induction.

Let us now assume that the statement holds if $a_1^2 + b_1^2$ has $k - 1$ prime factors. Let $a_1^2 + b_1^2 = p_1 \cdot \ldots \cdot p_{k-1}p_k$ and let $p_1 \cdot \ldots \cdot p_{k-1} = A_1^2 + B_1^2$, $p_k = A_2^2 + B_2^2$ and $p_1 \cdot \ldots \cdot p_{k-1}(c_1^2 + d_1^2) = g^2 + h^2$. From $y_2^2 + z_2^2 = p_k(g^2 + h^2)$ and previously proved, it follows that $y_2 = A_2g_1 \pm B_2h_1$, $z_2 = A_2h_1 \mp B_2g_1$, where $g_1^2 + h_1^2 = g^2 + h^2$. By the inductive assumption, we have $g_1 = A_3e \pm B_3f$, $h_1 = A_3f \mp B_3e$, where $A_3^2 + B_3^2 = A_1^2 + B_1^2$, $e^2 + f^2 = c_1^2 + d_1^2$. Let us choose one of the signs (for other choices, the analogous result is obtained) and we calculate: $y_2 = A_2(A_3e + B_3f) + B_2(A_3f - B_3e) = e(A_2A_3 - B_2B_3) + f(A_2B_3 + B_2A_3)$, $z_2 = A_2(A_3f - B_3e) - B_2(A_3e + B_3f) = f(A_2A_3 - B_2B_3) - e(A_2B_3 + B_2A_3)$. Now, (10.19) follows from

$$(A_2A_3 - B_2B_3)^2 + (A_2B_3 + B_2A_3)^2 = (A_2^2 + B_2^2)(A_3^2 + B_3^2) = a_1^2 + b_1^2$$

and $e^2 + f^2 = c_1^2 + d_1^2$. □

In much the same way as the Pythagorean equation $x^2 + y^2 = z^2$ motivated Fermat to show that equation $x^4 + y^4 = z^4$ does not have solutions in positive integers and to make a conjecture regarding the more general equation $x^k + y^k = z^k$, by considering equation (10.17) the question of the existence of solutions of the equation

$$x^4 + y^4 + z^4 = u^4 \tag{10.20}$$

arises. Euler made a conjecture that this equation does not have solutions in positive integers and also a more general one that equation $x_1^k + x_2^k + \cdots + x_n^k = y^k$ does not have solutions for $n < k$. It is known that these conjectures do not hold. The first counterexample for $k = 5$ was found by Lander and Parkin in 1966,

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5,$$

while in 1988, Elkies [170] found a counterexample for $k = 4$; namely, he found the following solution of equation (10.20)

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

Elkies' construction actually shows that equation (10.20) has infinitely many solutions. They correspond to rational points on the curve $u^2 = -31790v^4 + 36941v^3 - 56158v^2 + 28849v + 22030$, for which, through its connection with elliptic curves (about which we will provide more information later on, see for example Proposition 15.1), it is shown that it has infinitely many rational points (it has positive "rank", to be more precise, the rank is 3), out of which the simplest point is the one with coordinates $(v, u) = (-31/467, 30731278/218089)$, and each point gives a rational solution (and after multiplication with a common denominator also an integer solution) of equation (10.20) through the identity

$$(85v^2 + 484v - 313)^4 + (68v^2 - 586v + 10)^4 + (2u)^4 = (357v^2 - 204v + 363)^4.$$

10.3 Pell's equation

A Diophantine equation of the form

$$x^2 - dy^2 = 1, \tag{10.21}$$

where d is a positive integer which is not a perfect square, is called *Pell's equation*. We exclude the case when d is a perfect square because it is obvious that in that case, equation (10.21) has only trivial solutions $x = \pm 1$, $y = 0$. Indeed, if $d = \delta^2$, then from $(x - \delta y)(x + \delta y) = 1$, it follows that $x - \delta y = x + \delta y = \pm 1$. The equation is named after the English mathematician John Pell, to whom Euler, it seems mistakenly, attributed a solution method. Some particular equations of this type can be found in texts of ancient Greek mathematicians (Archimedes, Diophantus), but they were first systematically studied by medieval Indian mathematicians (Brahmagupta).