

Diophantine equations

Project is prepared and presented by:

I. Klimanova, P. Kozlov, A. Miroshnikov, E. Veretennikov.

Abstract

In this project you can get acquainted with some remarkable equations and problems arising from the theory of Diophantine equations. This project consists of several sections and it is highly recommended to solve problems step by step.

In section 1 we consider the Diophantine equation $x^2 - Dy^2 = n$ and we suggest that you are already familiar with the structure of solutions of equation $x^2 - Dy^2 = 1$. The theory of continued fractions helps to solve the given equation with a small n . Also, we provide a relatively little-known method that reduces equation $x^2 - Dy^2 = n$ to another one $t^2 - Du^2 = m$ with a smaller m .

Section 2 is devoted to special cases of the equations $x^4 - Dy^2 = 1$ and $x^2 - Dy^4 = 1$. While solving problems in this section, you will learn the structure of solutions to some equations $x^2 - Dy^2 = n$ with a small n . Understanding this structure is also quite useful for many other problems.

In section 3 we show the connection between the old problem on existence of Diophantine quadruples and the number of classes of solutions to equation $x^2 - (k^2 + 1)y^2 = k^2$.

1 On the diophantine equation $x^2 - Dy^2 = n$

Let α be an irrational number. We can represent α as an infinite continued fraction $[a_0; a_1, a_2, \dots]$. A continued fraction formed from $[a_0; a_1, a_2, \dots]$ by neglecting all terms after a given term is called a *convergent* to α . We can represent k -th convergent $[a_0, \dots, a_k]$ as an irreducible fraction with a numerator p_k and a denominator q_k . Denote a continued fraction by $[a_k, a_{k+1}, \dots]$ by α_k .

Properties of convergents:

- a) $p_k = a_k p_{k-1} + p_{k-2}$, $q_k = a_k q_{k-1} + q_{k-2}$.
- b) $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1}$, $p_k q_{k-2} - p_{k-2} q_k = (-1)^k a_k$.
- c) p_{2k}/q_{2k} is an increasing sequence, p_{2k-1}/q_{2k-1} is a decreasing sequence.
- d) $\alpha = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}}$.

Problem 1.1. a) Prove the equalities:

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1}, \quad p_k q_{k-2} - p_{k-2} q_k = (-1)^k a_k.$$

b) Prove the inequalities:

$$\frac{1}{q_{k+1} + q_k} < |q_k \alpha - p_k| < \frac{1}{q_{k+1}}.$$

c) Prove that a sequence $\{|q_k \alpha - p_k|\}_{k=0}^{\infty}$ is strictly decreasing.

Solution. a) These equations can be easily proved by induction.

b) Since

$$\alpha = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}},$$

we have by a)

$$|q_k\alpha - p_k| = \frac{|p_{k-1}q_k - p_kq_{k-1}|}{\alpha_{k+1}q_k + q_{k-1}}.$$

As $\alpha_{k+1} = a_{k+1} + 1/\alpha_{k+2}$, the following inequality is true:

$$a_{k+1} < \alpha_{k+1} < a_{k+1} + 1.$$

Therefore

$$q_{k+1} = a_{k+1}q_k + q_{k-1} < \alpha_{k+1}q_k + q_{k-1} < (a_{k+1} + 1)q_k + q_{k-1} = q_{k+1} + q_k$$

and

$$\frac{1}{q_{k+1} + q_k} < |q_k\alpha - p_k| < \frac{1}{q_{k+1}}.$$

c) By b)

$$|q_{k+1}\alpha - p_{k+1}| < \frac{1}{q_{k+2}} \leq \frac{1}{q_{k+1} + q_k} < |q_k\alpha - p_k|.$$

■

Problem 1.2. Prove that of any two consecutive convergents to α , at least one satisfies the inequality

$$\left| \alpha - \frac{a}{b} \right| < \frac{1}{2b^2}.$$

Solution. Suppose

$$\left| \alpha - \frac{p_k}{q_k} \right| \geq \frac{1}{2q_k^2} \quad \text{and} \quad \left| \alpha - \frac{p_{k+1}}{q_{k+1}} \right| \geq \frac{1}{2q_{k+1}^2}.$$

As α is irrational, we have

$$\left| \alpha - \frac{p_k}{q_k} \right| > \frac{1}{2q_k^2} \quad \text{and} \quad \left| \alpha - \frac{p_{k+1}}{q_{k+1}} \right| > \frac{1}{2q_{k+1}^2}.$$

Since the convergents are alternately less or greater than α , by Problem 1.1

$$\begin{aligned} \frac{1}{q_k q_{k+1}} &= \left| \frac{p_k}{q_k} - \frac{p_{k+1}}{q_{k+1}} \right| = \left| \frac{p_k}{q_k} - \alpha + \alpha - \frac{p_{k+1}}{q_{k+1}} \right| = \\ &= \left| \frac{p_k}{q_k} - \alpha \right| + \left| \alpha - \frac{p_{k+1}}{q_{k+1}} \right| > \frac{1}{2q_k^2} + \frac{1}{2q_{k+1}^2}. \end{aligned}$$

From this inequality we see that

$$q_{k+1}^2 - 2q_k q_{k+1} + q_k^2 = (q_{k+1} - q_k)^2 < 0$$

which is impossible. ■

Problem 1.3. Prove that of any three consecutive convergents to α , at least one satisfies the inequality

$$\left| \alpha - \frac{a}{b} \right| < \frac{1}{\sqrt{5}b^2}.$$

Solution. Suppose

$$\left| \alpha - \frac{p_k}{q_k} \right| \geq \frac{1}{\sqrt{5}q_k^2}, \quad \left| \alpha - \frac{p_{k+1}}{q_{k+1}} \right| \geq \frac{1}{\sqrt{5}q_{k+1}^2} \quad \text{and} \quad \left| \alpha - \frac{p_{k+2}}{q_{k+2}} \right| \geq \frac{1}{\sqrt{5}q_{k+2}^2}.$$

The convergents p_k/q_k and p_{k+1}/q_{k+1} are alternately less or greater than α , as well as p_{k+1}/q_{k+1} and p_{k+2}/q_{k+2} . As in the solution of the previous problem we get that

$$\frac{1}{q_k q_{k+1}} > \frac{1}{\sqrt{5}q_k^2} + \frac{1}{\sqrt{5}q_{k+1}^2} \quad \text{and} \quad \frac{1}{q_{k+1} q_{k+2}} > \frac{1}{\sqrt{5}q_{k+1}^2} + \frac{1}{\sqrt{5}q_{k+2}^2}.$$

Denote q_{k+1}/q_k by r_k . It follows from the previous inequalities that

$$r_k^2 - \sqrt{5}r_k + 1 < 0 \quad \text{and} \quad r_{k+1}^2 - \sqrt{5}r_{k+1} + 1 < 0$$

then $r_k, r_{k+1} < \varphi$, where $\varphi = \frac{\sqrt{5}+1}{2}$ is the largest root of equation $x^2 - \sqrt{5}x + 1 = 0$.

After dividing the equality $q_{k+2} = a_{k+2}q_{k+1} + q_k$ by q_{k+1} we get

$$r_{k+1} = a_{k+2} + \frac{1}{r_k}.$$

Now a contradiction follows:

$$\varphi > r_{k+1} = a_{k+2} + \frac{1}{r_k} \geq 1 + \frac{1}{r_k} > 1 + \frac{1}{\varphi} = 1 + \frac{2}{\sqrt{5}+1} = \frac{\sqrt{5}+1}{2} = \varphi.$$

■

Problem 1.4. Consider a positive integer k and integers p, q with $q > 0$ such that

$$|q\alpha - p| < |q_k\alpha - p_k|.$$

a) Prove that there are integers u, v such that

$$p_k u + p_{k+1} v = p, \quad q_k u + q_{k+1} v = q.$$

b) Prove that $q \geq q_{k+1}$.

Solution. a) Choose

$$u = (-1)^k(qp_{k+1} - pq_{k+1}), \quad v = (-1)^k(pq_k - qp_k).$$

These integers are valid by Problem 1.1.a.

b) Take the integers u, v from a). If $u \geq 0, v \geq 1$ then

$$q = q_k u + q_{k+1} v \geq q_{k+1} v \geq q_{k+1}.$$

The cases $u, v < 0$ or $v = 0$ are trivially impossible.

It remains to check the case when u, v are of different signs. Notice that the numbers $q_k \alpha - p_k$ and $q_{k+1} \alpha - p_{k+1}$ are also of different signs. It means that the numbers $u(q_k \alpha - p_k)$ and $v(q_{k+1} \alpha - p_{k+1})$ are of the same sign. Hence

$$|q \alpha - p| = |(q_k u + q_{k+1} v) \alpha - (p_k u + p_{k+1} v)| = |u| |q_k \alpha - p_k| + |v| |q_{k+1} \alpha - p_{k+1}| \geq |q_k \alpha - p_k|$$

which contradicts the condition of the problem. ■

Using the previous problem one can show that the convergents form a sequence of «best» approximations to α .

Problem 1.5. If a/b is a rational number such that

$$\left| \alpha - \frac{a}{b} \right| < \frac{1}{2b^2}$$

then a/b is one of the convergents to α .

Solution. It is enough to prove the statement of the problem only for coprime a, b .

Let k be an integer such that $q_k \leq b < q_{k+1}$. As $b < q_{k+1}$ inequality $|q_k \alpha - p_k| \leq |b \alpha - a|$ is true by Problem 1.4. It follows that

$$\left| \alpha - \frac{p_k}{q_k} \right| \leq \frac{|b \alpha - a|}{q_k} < \frac{1}{2bq_k}.$$

Suppose, $a/b \neq p_k/q_k$. Hence

$$\frac{1}{bq_k} \leq \left| \frac{a}{b} - \frac{p_k}{q_k} \right| \leq \left| \frac{a}{b} - \alpha \right| + \left| \alpha - \frac{p_k}{q_k} \right| < \frac{1}{2b^2} + \frac{1}{2bq_k}$$

which contradicts to inequality $q_k \leq b$. It means $a/b = p_k/q_k$. ■

Further, throughout the project, D is a squarefree positive integer number.

Problem 1.6. Let n be an integer that is less than $\sqrt{D}$ in absolute value. Assume that equation $x^2 - Dy^2 = n$ has a solution x_0, y_0 in positive integers. Prove that x_0/y_0 is one of convergents to $\sqrt{D}$ if:

- a) n is positive;
- b) n is negative.

Solution. a) The equality

$$(x_0 - y_0\sqrt{D})(x_0 + y_0\sqrt{D}) = n,$$

implies that $x_0 > y_0\sqrt{D}$.

Therefore

$$0 < \frac{x_0}{y_0} - \sqrt{D} = \frac{n}{y_0(x_0 + y_0\sqrt{D})} < \frac{n}{y_0(y_0\sqrt{D} + y_0\sqrt{D})} < \frac{\sqrt{D}}{2y_0^2\sqrt{D}} = \frac{1}{2y_0^2},$$

it follows from Problem 1.5 that x_0/y_0 is a convergent to $\sqrt{D}$.

b) Analogously to the proof of a), we find that y_0/x_0 is a convergent to $1/\sqrt{D}$. Hence x_0/y_0 is a convergent to $\sqrt{D}$. ■

Definition. A real irrational number which is a root of a quadratic equation with integral coefficients is called a *quadratic irrational*.

An infinite continued fraction is said to be *periodic* if it is of form $[a_0; a_1, \dots, a_l, \overline{b_1, \dots, b_m}]$. If it is of the form $[\overline{b_1, \dots, b_m}]$ it is said to be *purely periodic*. The smallest positive integer m satisfying the above relationship is called the *period* of the expansion.

Problem 1.7. a) Prove that if α is a quadratic irrational and a, b, c, d are rational with not both c and d zero then number

$$\beta = \frac{a + b\alpha}{c + d\alpha}$$

is either rational or a quadratic irrational.

b) Prove that each periodic continued fraction is a quadratic irrational.

Solution. a) It is easy to see that

$$\alpha = \frac{a' + b'\beta}{c' + d'\beta}$$

for some integers a', b', c', d' , and not both c' and d' are zero. Let α be a root of the quadratic equation $kx^2 + lx + m = 0$ with integer coefficients k, l, m . Then β is a root of the quadratic or linear equation

$$k(a' + b'x)^2 + l(a' + b'x)(c' + d'x) + m(c' + d'x)^2 = 0$$

with integer coefficients.

b) Let $\alpha = [a_0; a_1, \dots, a_l, \overline{b_1, \dots, b_m}]$. Then

$$\alpha_{l+1} = [\overline{b_1, \dots, b_m}] = [b_1, \dots, b_m, \alpha_{l+1}].$$

If p'_k/q'_k is the k -th convergent to α_{l+1} then

$$\alpha_{l+1} = \frac{p'_m \alpha_{l+1} + p'_{m-1}}{q'_m \alpha_{l+1} + q'_{m-1}}$$

so that

$$q'_m \alpha_{l+1}^2 + (q'_{m-1} - p'_m) \alpha_{l+1} - p'_{m-1} = 0.$$

Thus, since α_{l+1} is not rational (the continued fraction expansion is infinite), α_{l+1} is a quadratic irrational.

If p_k/q_k is the k -th convergent to α then

$$\alpha = \frac{\alpha_{l+1}p_l + p_{l-1}}{\alpha_{l+1}q_l + q_{l-1}}.$$

It follows from a) that α is either rational or a quadratic irrational. Since α is an infinite simple continued fraction, α is a quadratic irrational. ■

The converse to previous problem is also true.

Problem 1.8. a) Suppose α is a real, irrational root of $ax^2 + bx + c = 0$, where a, b, c are integers and $a \neq 0$. Prove that α_{k+1} is a root of the polynomial

$$A_k x^2 + B_k x + C_k = 0,$$

where

$$\begin{aligned} A_k &= ap_k^2 + bp_k q_k + cq_k^2, \\ B_k &= 2ap_k p_{k-1} + b(p_k q_{k-1} + p_{k-1} q_k) + 2cq_k q_{k-1}, \\ C_k &= ap_{k-1}^2 + bp_{k-1} q_{k-1} + cq_{k-1}^2 \end{aligned}$$

and

$$B_k^2 - 4A_k C_k = b^2 - 4ac.$$

b) Prove that there is a number M such that $|A_k|, |B_k|, |C_k| < M$ for any positive integer k .

c) Prove that each quadratic irrational has a periodic expansion as a continued fraction.

Solution. a) It follows from properties of continued fractions that

$$\alpha = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}}.$$

If we substitute this value of α into $a\alpha^2 + b\alpha + c = 0$ and rearrange the coefficients, we obtain

$$A_k \alpha_{k+1}^2 + B_k \alpha_{k+1} + C_k = 0,$$

where A_k, B_k, C_k are as given in the statement of the problem. By direct computation we obtain

$$B_k^2 - 4A_k C_k = (b^2 - 4ac) (p_k q_{k-1} - q_k p_{k-1})^2 = b^2 - 4ac.$$

b) By Problem 1.1.b we have

$$|\alpha q_k - p_k| < \frac{1}{q_k}$$

so we can write

$$p_k = \alpha q_k + \frac{\varepsilon}{q_k} \quad |\varepsilon| < 1,$$

where ε , of course, depends on k . Substituting this into the expression for A_k , we obtain

$$\begin{aligned} A_k &= a \left(\alpha q_k + \frac{\varepsilon}{q_k} \right)^2 + b \left(\alpha q_k + \frac{\varepsilon}{q_k} \right) q_k + c q_k^2 \\ &= (a\alpha^2 + b\alpha + c) q_k^2 + \left(2a\alpha + b + \frac{a\varepsilon}{q_k^2} \right) \cdot \varepsilon \\ &= \left(2a\alpha + b + \frac{a\varepsilon}{q_k^2} \right) \cdot \varepsilon. \end{aligned}$$

Thus,

$$|A_k| < |2a\alpha + b| + |a|$$

which implies that all of the A_k must come from a finite set of integers. As $C_k = A_{k-1}$, a similar result is true for the C_k . Since

$$B_k^2 - 4A_k C_k = b^2 - 4ac,$$

we have

$$B_k^2 = |4A_k C_k + b^2 - 4ac| < 4\{|2a\alpha + b| + |a|\}^2 + |b^2 - 4ac|$$

and B_k is also bounded.

c) Since a quadratic equation can have at most two distinct roots, it follows from b) that there are at least two equal numbers in the sequence of α_k . It means α is periodic. ■

Definition. Let $\alpha = a + b\sqrt{D}$, where a, b are rational and $\sqrt{D}$ is irrational. The *conjugate* of α , denoted by α' , is the number $a - b\sqrt{D}$.

Problem 1.9. Let α be a quadratic irrational.

- a) Prove that if the continued fraction of α is purely periodic then $\alpha > 1$ and $-1 < \alpha' < 0$.
- b) Prove that if $\alpha > 1$ and $-1 < \alpha' < 0$ then the continued fraction of α is purely periodic.

Solution. a) Let $\alpha = [\overline{a_1, \dots, a_m}] = [a_1, \dots, a_m, \alpha]$. Since $a_i \geq 1$ for any positive integer i , we obtain $\alpha > 1$.

If p_k/q_k is the k -th convergent to α then

$$\alpha = \frac{\alpha p_m + p_{m-1}}{\alpha q_m + q_{m-1}}$$

so that α is a root of

$$f(x) = q_m x^2 + (q_{m-1} - p_m)x - p_{m-1} = 0.$$

Since

$$f(-1) = (q_m - q_{m-1}) + (p_m - p_{m-1}) > 0$$

and

$$f(0) = -p_{m-1},$$

we obtain that α' , the other root of $f(x) = 0$, must be between -1 and 0 .

b) Suppose α is a quadratic irrational, $\alpha > 1$ and $-1 < \alpha' < 0$. Let $\alpha_1 = \alpha$ and define α_k inductively

$$\alpha_{k-1} = a_{k-1} + \frac{1}{\alpha_k}.$$

We know that α_k is a root of equation $f_k(x) = p_k x^2 + q_k x + r_k = 0$ for some integer p_k, q_k, r_k . Note that $1/\alpha_{k+1} = \alpha_k - a_k$ is a root of equation

$$f_{k-1}(a_{k-1} + x) = p_{k-1} x^2 + (2p_{k-1} a_{k-1} + q_{k-1})x + f_{k-1}(a_{k-1}) = 0.$$

It follows that

$$\frac{1}{\alpha_k} + \frac{1}{\alpha'_k} = \frac{1}{\alpha_k} + \left(\frac{1}{\alpha_k}\right)' = -\frac{2p_{k-1}a_{k-1} + q_{k-1}}{p_{k-1}} = -2a_{k-1} + \alpha_{k-1} + \alpha'_{k-1},$$

and

$$\alpha'_{k-1} = a_{k-1} + \frac{1}{\alpha'_k}.$$

It can be proved by mathematical induction that

$$-1 < \alpha'_k < 0$$

for any positive k and, as a consequence,

$$a_{k-1} = \left[-\frac{1}{\alpha'_k}\right].$$

Since $\alpha = [a_1, \dots, a_k, \alpha_{k+1}]$ and α is a quadratic irrational, by Problem 1.8 there exist positive integers k and l such that $\alpha_{k+1} = \alpha_{k+t+1}$. Thus,

$$a_k = \left[-\frac{1}{\alpha'_{k+1}}\right] = \left[-\frac{1}{\alpha'_{k+t+1}}\right] = a_{k+t}$$

and

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}} = a_{k+t} + \frac{1}{\alpha_{k+t+1}} = \alpha_{k+t}.$$

If we apply this process k times, we obtain

$$\alpha = \alpha_1 = \alpha_{t+1}.$$

Finally,

$$\alpha = [a_1, \dots, a_t, \alpha] = [\overline{a_1, \dots, a_t}].$$

■

Problem 1.10. Write the continued fraction $[a_0; a_1, a_2, \dots, a_k, \alpha_{k+1}]$ of $\sqrt{D}$.

a) Prove that α_k is purely periodic for any positive integer k .

b) Prove that there exist positive integers b_k, c_k such that

$$\alpha_{k+1} = \frac{b_k + \sqrt{D}}{c_k}$$

and

$$p_k^2 - Dq_k^2 = (-1)^{k+1} c_k.$$

Solution. a) Let $[a_0; a_1, \dots]$ be the continued fraction of $\sqrt{D}$. Consider the quadratic irrational $\alpha = a_0 + \sqrt{D}$. Since $a_0 = [\sqrt{D}]$, it follows that α' is in bounds $-1 < \alpha' < 0$. Then by Problem 1.9.b the continued fraction of α is purely periodic. Thus,

$$\sqrt{D} = \alpha - a_0 = [2a_0, a_1, \dots, a_n] - a_0 = [a_0, \overline{a_1, \dots, a_n, 2a_0}].$$

The statement of the problem follows.

b) Since

$$\sqrt{D} = \frac{p_k \alpha_{k+1} + p_{k-1}}{q_k \alpha_{k+1} + q_{k-1}},$$

we have

$$\alpha_{k+1} = \frac{q_{k-1} \sqrt{D} - p_{k-1}}{p_k - q_k \sqrt{D}}.$$

Now we rationalize the denominator:

$$\begin{aligned} \alpha_{k+1} &= \frac{q_{k-1} \sqrt{D} - p_{k-1}}{p_k - q_k \sqrt{D}} = \frac{(q_{k-1} \sqrt{D} - p_{k-1})(p_k + q_k \sqrt{D})}{p_k^2 - Dq_k^2} = \\ &= \frac{(Dq_k q_{k-1} - p_k p_{k-1}) + (p_k q_{k-1} - p_{k-1} q_k) \sqrt{D}}{p_k^2 - Dq_k^2} = \frac{(Dq_k q_{k-1} - p_k p_{k-1}) + (-1)^{k+1} \sqrt{D}}{p_k^2 - Dq_k^2}. \end{aligned}$$

Take $b_k = (-1)^{k+1}(Dq_k q_{k-1} - p_k p_{k-1})$. To complete the proof, it's enough to check that b_k and c_k are positive for any k .

First, c_k is positive since $\text{sign}(p_k^2 - Dq_k^2) = \text{sign}\left(\frac{p_k}{q_k} - \sqrt{D}\right) = (-1)^{k+1}$.

Secondly, b_k is positive because c_k is positive and $2b_k/c_k = \alpha_k + \alpha'_k > 0$. The latter follows from a) and the Problem 1.9.a. ■

It follows from the previous problem that sequence $p_k^2 - Dq_k^2$ is periodic with a period equal to or twice as large as the period of continued fraction for $\sqrt{D}$. This fact together with result of Problem 1.6 describes all the solutions to equation $x^2 - Dy^2 = n$ with $|n| < \sqrt{D}$.

In the sequel, we consider only solutions to equation $x^2 - Dy^2 = n$ with $x + y\sqrt{D} > 0$, because $(-x, -y)$ is also a solution whenever (x, y) is a solution.

It is easy to see that if the equation $x^2 - Dy^2 = n$ has an integer solution (x_0, y_0) then it has an infinite number of such solutions (x_k, y_k) defined by

$$x_k + y_k \sqrt{D} = (x_0 + y_0 \sqrt{D})(s + t \sqrt{D})^k,$$

where (s, t) is the minimal positive solution to the corresponding Pell's equation.

Definition. Two solutions (x_1, y_1) and (x_2, y_2) to equation $x^2 - Dy^2 = n$ are said to be *in the same class* if there is an integer n such that

$$x_2 + y_2 \sqrt{D} = (x_1 + y_1 \sqrt{D})(s + t \sqrt{D})^k,$$

where (s, t) is the minimal positive solution to the corresponding Pell's equation.

We say that (x, y) is the *minimal* solution in the class if $1 < x + y\sqrt{D} \leq s + t\sqrt{D}$.

Problem 1.11. How many classes of solutions does an equation

$$x^2 - (m^2 - 2)y^2 = 2$$

have for any integer $m > 1$?

Solution. Notice that $(m^2 - 1, m)$ is the minimal solution to the corresponding Pell's equation $x^2 - (m^2 - 2)y^2 = 1$. Consider some class of solutions to equation $x^2 - (m^2 - 2)y^2 = 2$ with minimal solution (u, v) . By definition,

$$1 < \alpha = u + v\sqrt{m^2 - 2} \leq \beta = m^2 - 1 + m\sqrt{m^2 - 2}.$$

Since

$$\alpha^2/2 = u^2 - 1 + uv\sqrt{m^2 - 2},$$

$(u^2 - 1, uv)$ is another solution to Pell's equation $x^2 - (m^2 - 2)y^2 = 1$. It means that $\alpha^2/2 = \beta^l$ for some integer l . From the inequalities $1 < \alpha^2/2 \leq \beta^2/2 < \beta^2$ it follows that $l = 1$. Hence $\alpha = \sqrt{2\beta} = m + \sqrt{m^2 - 2}$ and equation $x^2 - (m^2 - 2)y^2 = 2$ has the only one class of solutions with the minimal solution $(m, 1)$. ■

Definition. A solution (x_0, y_0) of $x^2 - Dy^2 = n$ is said to be *primitive* if x_0 and y_0 are relatively prime.

It is obviously sufficient to find only primitive solutions, because if $\gcd(x_0, y_0) = d > 1$ then $(x_0/d, y_0/d)$ is a primitive solution to

$$x^2 - Dy^2 = \frac{n}{d^2}.$$

Problem 1.12. If (x_0, y_0) is a primitive solution to equation $x^2 - Dy^2 = n$ then there exists an integer k such that

$$x_0 \equiv ky_0 \pmod{n}$$

and

$$k^2 \equiv D \pmod{n}.$$

Solution. Since x_0 and y_0 are relatively prime, so are y_0 and n . Thus, there exists an integer k such that

$$x_0 \equiv ky_0 \pmod{n}$$

Therefore

$$x_0^2 - Dy_0^2 \equiv k^2y_0^2 - Dy_0^2 \equiv y_0^2(k^2 - D) \pmod{n}$$

which in view of $\gcd(y_0^2, n) = 1$ implies that

$$k^2 \equiv D \pmod{n}.$$

■

It follows from the previous problem that if D is a quadratic nonresidue modulo n then the Diophantine equation

$$x^2 - Dy^2 = n$$

has no primitive solutions.

Definition. We say that a primitive solution (x_0, y_0) to the equation $x^2 - Dy^2 = n$ belongs to the integer k if

$$x_0 \equiv ky_0 \pmod{n}$$

and

$$k^2 \equiv D \pmod{n}.$$

Problem 1.13. Prove that two primitive solutions to equation $x^2 - Dy^2 = n$ are in the same class if and only if they belong to the same integer.

Solution. Suppose (x_1, y_1) and (x_2, y_2) are two primitive solutions to equation $x^2 - Dy^2 = n$ such that

$$x_2 + y_2\sqrt{D} = (x_1 + y_1\sqrt{D})(s + t\sqrt{D})^k,$$

where (s, t) is the minimal positive solution to the corresponding Pell's equation. Of course, $(s + t\sqrt{D})^k = u + v\sqrt{D}$, where (u, v) is another solution to Pell's equation. Then

$$x_2 = x_1u + y_1vD, \quad y_2 = x_1v + y_1u.$$

Assume that the solution (x_1, y_1) belongs to the integer k . Then

$$y_2k = x_1vk + y_1uk \equiv y_1kvk + x_1u \equiv y_1vD + x_1u = x_2,$$

Thus the solution (x_2, y_2) belongs to the same integer k .

Conversely, let solutions (x_1, y_1) and (x_2, y_2) belong to an integer k . Then

$$\begin{aligned} \frac{x_2 + y_2\sqrt{D}}{x_1 + y_1\sqrt{D}} &= \frac{(x_2 + y_2\sqrt{D})(x_1 - y_1\sqrt{D})}{(x_1 + y_1\sqrt{D})(x_1 - y_1\sqrt{D})} = \\ &= \frac{x_1x_2 - y_1y_2D}{n} + \frac{x_1y_2 - x_2y_1}{n}\sqrt{D}. \end{aligned}$$

Since

$$x_1 \equiv y_1k, \quad x_2 \equiv y_2k, \quad k^2 \equiv D \pmod{n},$$

we have

$$x_1x_2 \equiv y_1y_2k^2 \equiv y_1y_2D \pmod{n}$$

and

$$x_1y_2 \equiv y_1y_2k \equiv x_2y_1 \pmod{n}.$$

Thus

$$\frac{x_1x_2 - y_1y_2D}{n} = u, \quad \frac{x_1y_2 - x_2y_1}{n} = v$$

for some integers u, v and so

$$\frac{x_2 + y_2\sqrt{D}}{x_1 + y_1\sqrt{D}} = u + v\sqrt{D}.$$

Similarly

$$\frac{x_2 - y_2\sqrt{D}}{x_1 - y_1\sqrt{D}} = u - v\sqrt{D}.$$

Therefore

$$\begin{aligned} u^2 - v^2D &= (u + v\sqrt{D})(u - v\sqrt{D}) = \\ &= \frac{x_2 + y_2\sqrt{D}}{x_1 + y_1\sqrt{D}} \cdot \frac{x_2 - y_2\sqrt{D}}{x_1 - y_1\sqrt{D}} = \frac{n}{n} = 1 \end{aligned}$$

which means that (u, v) is a solution to Pell's equation. Hence (x_1, y_1) and (x_2, y_2) are two solutions lying in the same class. ■

It follows from the previous problem that there exists only a finite number of classes for any Diophantine equation $x^2 - Dy^2 = n$.

Let (x_0, y_0) be a solution to equation $x^2 - Dy^2 = n$ that belongs to some integer k . It follows from definition that there are integers u_0, m such that

$$x_0 = y_0k - u_0n, \quad D = k^2 - mn.$$

Problem 1.14. Prove that there is an integer t_0 such that (t_0, u_0) is a solution to equation $t^2 - Du^2 = m$ belonging to the integer $\pm k$. Express x_0, y_0 in terms of t_0, u_0 .

Solution. If we substitute the above expressions for x_0 and D into $x_0^2 - Dy_0^2 = n$ and simplify, we obtain

$$y_0^2m - 2y_0ku_0 + (u_0^2n - 1) = 0$$

which implies that

$$y_0 = \frac{ku_0 \pm \sqrt{k^2u_0^2 - mu_0^2n + m}}{m} = \frac{ku_0 \pm \sqrt{Du_0^2 + m}}{m}.$$

Since y_0 is an integer, the value of the radical $\sqrt{Du_0^2 + m}$ must be an integer, say t_0 , implying that (t_0, u_0) is a solution to the Diophantine equation

$$t^2 - u^2D = m.$$

For the same reason we must have

$$ku_0 \pm t_0 \equiv 0 \pmod{m},$$

so (t_0, u_0) is the solution belonging to the integer $\pm k$. Finally, from

$$y_0 = \frac{ku_0 \pm t_0}{m}$$

it follows that

$$x_0 = y_0k - u_0n = \frac{Du_0 \pm t_0k}{m}.$$

■

The number m from the previous problem depends on k . Notice that the choice of k is not fixed, it is fixed only modulo n .

Problem 1.15. If $|n| > \sqrt{D}$, the number m (from the previous problem) can be chosen to satisfy inequality $|m| \leq \max\{\sqrt{D}, |n|/4\}$.

Solution. Choose k such that $|k| \leq n/2$. If $k^2 < D$ then

$$|m| \leq \frac{D}{|n|} < \sqrt{D}.$$

If $k^2 > D$ then

$$|m| < \frac{k^2}{|n|} \leq |n|/4.$$

■

By applying the method from the previous two problems repeatedly, we eventually obtain equations

$$t'^2 - Du'^2 = m',$$

where $|m'| < \sqrt{D}$, which have only those integer solutions that we obtain from the numerators and denominators of convergents to $\sqrt{D}$. A word of caution: in applying the method repeatedly we can pick different values of k at each step.

Problem 1.16. Determine all the classes of solutions to the following equations:

- a) $x^2 - 82y^2 = 23$,
- b) $x^2 - 23y^2 = 41$.

Solution. a) We find that $k = \pm 6$ are the only values of k in the range

$$0 \leq |k| \leq \frac{23}{2},$$

such that $k^2 \equiv 82 \pmod{23}$. Thus

$$m = \frac{k^2 - D}{n} = \frac{36 - 82}{23} = -2.$$

Since $\sqrt{82} = [9, \overline{18}]$, by Problem 1.6 the only equations of form

$$t^2 - 82u^2 = n \quad (0 < |n| < \sqrt{82})$$

that have solutions are

$$t^2 - 82u^2 = p_l^2 - 82q_l^2 = \pm 1.$$

Thus, the equation $t^2 - 82u^2 = m = -2$ has no integer solutions, and, by Problem 1.14, the equation $x^2 - 82y^2 = 23$ has no integer solutions too.

b) The only values of k in the range

$$0 \leq |k| \leq \frac{41}{2}$$

such that $k^2 \equiv 23 \pmod{41}$ are $k = \pm 8$. Thus

$$m = \frac{k^2 - D}{n} = \frac{64 - 23}{41} = 1.$$

The equation $t^2 - 23u^2 = m = 1$ has a particular solution $t_0 = 1, u_0 = 0$. Hence $x_0 = \pm 8, y_0 = \pm 1$, where x_0 should be equal to 8 to satisfy $x_0 + y_0\sqrt{23} > 0$. So the equation $x^2 - 23y^2 = 41$ has two classes of solutions with minimal solutions $(8, 1)$ and $(8, -1)$ respectively. ■

Problem 1.17. Prove that equation $x^2 - 229y^2 = 3$

- a) has no integer solutions,
- b) has a solution modulo every prime p .

Solution. a) The continued fraction expansion of $\sqrt{229}$ is $[15; \overline{7, 1, 1, 7, 30}]$ with the period equal to 5. Calculate the first five values of $p_n^2 - 229q_n^2$:

$$\begin{aligned} p_0^2 - 229q_0^2 &= 15^2 - 229 \cdot 1^2 = -4, \\ p_1^2 - 229q_1^2 &= 106^2 - 229 \cdot 7^2 = 15, \\ p_2^2 - 229q_2^2 &= 121^2 - 229 \cdot 8^2 = -15, \\ p_3^2 - 229q_3^2 &= 227^2 - 229 \cdot 15^2 = 4, \\ p_4^2 - 229q_4^2 &= 1710^2 - 229 \cdot 113^2 = -1. \end{aligned}$$

By Problem 1.10 the sequence $|p_n^2 - 229q_n^2|$ is periodic with the period equal to 5. Hence by Problem 1.6 the only equations of form

$$x^2 - 229y^2 = n \quad (0 < |n| < \sqrt{229})$$

that have solutions are

$$x^2 - 229y^2 = \pm 1, \pm 4, \pm 15,$$

thus equation $x^2 - 229y^2 = 3$ has no integer solutions.

b) It is easy to see that equation $x^2 - 229y^2 = 3$ has a solution modulo 2. As 3 is a quadratic residue modulo 229, this equation has a solution modulo 229. Consider an odd prime p distinct from 229. Each of functions x^2 and $3 + 229y^2$ has $(p+1)/2$ values modulo p . Hence by Dirichlet's principle they are equal modulo p at some point and the equation $x^2 - 229y^2 = 3$ has a solution modulo p . ■

2 On the equations $x^4 - Dy^2 = 1$ and $x^2 - Dy^4 = 1$

To solve the problems in this section, it is helpful to solve the problems from the first section, though not mandatory. To understand the formulation of some problems, it is necessary to get acquainted with the definition of «class of solutions» and «minimal solution» in the class of solutions to equation $x^2 - Dy^2 = n$ from the first section (before Problem 1.11).

Definition. Suppose equation $x^2 - Dy^2 = n$ has a single class of solutions. We say that a number $\alpha = u + v\sqrt{D} > 0$ generates the fundamental solution to $x^2 - Dy^2 = n$ if (u, v) is the minimal solution in this class.

Problem 2.1. Prove that if equation $x^2 - Dy^2 = -1$ has a solution then it has a single class of solutions. Prove that if $\alpha = u + v\sqrt{D}$ generates the fundamental solution to $x^2 - Dy^2 = -1$ then the fundamental solution to $x^2 - Dy^2 = 1$ is given by $\beta = \alpha^2$.

Solution. Consider some class of solutions to equation $x^2 - Dy^2 = -1$ with minimal solution (u, v) . By definition,

$$1 < \alpha = u + v\sqrt{D} \leq \beta.$$

Notice that $\alpha^2 = (u + v\sqrt{D})^2 = u^2 + Dv^2 + 2uv\sqrt{D}$ generates a solution $(u^2 + Dv^2, 2uv)$ to Pell's equation $x^2 - Dy^2 = 1$ because

$$\begin{aligned} (u^2 + Dv^2)^2 - D(2uv)^2 &= (u^2 + Dv^2 + 2uv\sqrt{D})(u^2 + Dv^2 - 2uv\sqrt{D}) = \\ &= (u + v\sqrt{D})^2(u - v\sqrt{D})^2 = (u^2 - Dv^2)^2 = (-1)^2 = 1. \end{aligned}$$

It means that $\alpha^2 = \beta^l$ for some integer l . From the inequalities $1 < \alpha \leq \beta$ it follows that $l = 1$ or 2 . If $l = 2$ then $\alpha = \beta$ which is impossible because α and β generate fundamental solutions to different equations. Thus $l = 1$ and $\alpha^2 = \beta$. It means that equation $x^2 - Dy^2 = -1$ has a single class of solutions and α generates the fundamental solution to it. ■

Problem 2.2. Let (u, v) be the fundamental solution to Pell's equation $x^2 - Dy^2 = 1$. Prove that equation $x^2 - Dy^2 = -1$ has a solution if and only if $u \equiv -1 \pmod{2D}$.

Solution. By Problem 2.1, if $a + b\sqrt{D}$ is the fundamental solution to $x^2 - Dy^2 = -1$ then $u + v\sqrt{D} = (a + b\sqrt{D})^2$. Hence

$$u = a^2 + Db^2 = 2Db^2 - 1 \equiv -1 \pmod{2D}.$$

Conversely, if $u = 2Dk - 1$ then $u^2 = 4D^2k^2 - 4Dk + 1 = Dv^2 + 1$. Hence $4Dk^2 - 4k = v^2$. Therefore v is even, $v = 2z$, and $k(Dk - 1) = z^2$. Since k and $Dk - 1$ are relatively prime, both are perfect squares, $k = b^2$ and $Dk - 1 = a^2$ which gives $a^2 - Db^2 = -1$. ■

Problem 2.3. a) Consider coprime positive integers $m, n > 1$ such that mn is not a perfect square and equation $mx^2 - ny^2 = 1$ has a solution. Let (u, v) be the minimal positive solution to this equation. Prove that the fundamental solution to $x^2 - mny^2 = 1$ is given by $\gamma = \alpha^2$, where $\alpha = u\sqrt{m} + v\sqrt{n}$.

b) For any integer $a \geq 2$, describe all the integer solutions to $ax^2 - (a - 1)y^2 = 1$.

Solution. a) Notice that $\alpha^2 = (u\sqrt{m} + v\sqrt{n})^2 = u^2m + v^2n + 2uv\sqrt{mn}$ generates a solution $(u^2m + v^2n, 2uv)$ to Pell's equation $x^2 - mny^2 = 1$ because

$$\begin{aligned} (u^2m + v^2n)^2 - mn(2uv)^2 &= (u^2m + v^2n + 2uv\sqrt{mn})(u^2m + v^2n - 2uv\sqrt{mn}) = \\ &= (u\sqrt{m} + v\sqrt{n})^2(u\sqrt{m} - v\sqrt{n})^2 = (mu^2 - nv^2)^2 = 1. \end{aligned}$$

It means that $\alpha^2 = \gamma^l$ for some integer l .

If l is even then $\alpha = \gamma^{l/2} = p + q\sqrt{mn}$ for some integers p, q which is impossible because $m, n > 1$.

If l is odd and $l > 1$ then $\beta = \alpha(\gamma^{(1-l)/2})$ also generates a solution to equation $mx^2 - ny^2 = 1$ and $1 < \beta < \alpha$ which contradicts minimality of u, v . This means that $l = 1$ and $\gamma = \alpha^2$.

b) Equation $ax^2 - (a-1)y^2 = 1$ has the minimal solution $(1, 1)$ which is generated by $\alpha = \sqrt{a} + \sqrt{a-1}$. By a), $\gamma = \alpha^2$ generates the fundamental solution to Pell's equation $x^2 - a(a-1)y^2 = 1$. Let (u, v) be a solution to equation $ax^2 - (a-1)y^2 = 1$, and let $\beta = u\sqrt{a} + v\sqrt{a-1}$. Proceeding in the same way as in the proof of a), we see that

$$\beta^2 = (u\sqrt{a} + v\sqrt{a-1})^2 = u^2a + v^2(a-1) + 2uv\sqrt{a(a-1)}$$

generates a solution $(u^2a + v^2(a-1), 2uv)$ to Pell's equation $x^2 - a(a-1)y^2 = 1$. Therefore $\beta^2 = \gamma^l$ with an odd l . It follows that $\beta = \alpha^l$ and

$$u\sqrt{a} + v\sqrt{a-1} = (\sqrt{a} + \sqrt{a-1})^l$$

for an odd l . ■

Problem 2.4. Suppose that the fundamental solution to $x^2 - Dy^2 = -4$ is $2\alpha = a + b\sqrt{D}$, where a and b are odd integers. Find the fundamental solutions to equations

$$x^2 - Dy^2 = 4, \quad x^2 - Dy^2 = -1, \quad x^2 - Dy^2 = 1.$$

Solution (by V. Patrushev). Notice that

$$a^2 \equiv b^2 \equiv 1 \pmod{8}$$

and

$$D \equiv b^2D \equiv a^2 + 4 \equiv 5 \pmod{8}.$$

Since $2\alpha = a + b\sqrt{D} > 1$, we have $0 < b\sqrt{D} - a < 4$. Therefore $a \geq -1$ and $b \geq 1$. If $a = -1$ then $b = 1$, $D = 5$, and $2\alpha = \sqrt{5} - 1$. It is easy to check that the fundamental solutions to given equations are given by

$$3 + \sqrt{5} = 2\alpha^{-2}, \quad 2 + \sqrt{5} = \alpha^{-3}, \quad 9 + 4\sqrt{5} = \alpha^{-6}.$$

Suppose further $D > 5$, then $a, b \geq 1$ and $\alpha > 1$. One may check by direct computation that numbers $2\alpha^2, \alpha^3, \alpha^6$ are solutions to equations

$$x^2 - Dy^2 = 4, \quad x^2 - Dy^2 = -1, \quad x^2 - Dy^2 = 1$$

respectively. Suppose β generates the fundamental solution to equation $x^2 - Dy^2 = -1$, then $\alpha^3 = \beta^k$ for some odd positive k . Since $\alpha \neq \beta$, we have $k \neq 3$. Suppose $k \geq 5$. Then there is an odd l such that $k/3 < l < 2k/3$. It follows that

$$\alpha = \beta^{k/3} < \beta^l < \alpha^2 = \beta^{2k/3}.$$

Notice that

$$1 < \gamma = \frac{2\alpha^2}{\beta^l} < 2\alpha$$

and γ generates a solution to equation $x^2 - Dy^2 = -4$ which is impossible because 2α generates the fundamental solution to this equation.

Hence $k = 1$ and the number α^3 generates the fundamental solution to equation $x^2 - Dy^2 = -1$. Furthermore by Problem 2.1 the number α^6 generates the fundamental solution to Pell's equation $x^2 - Dy^2 = 1$.

Suppose now that $2\delta = p + q\sqrt{D}$ generates the fundamental solution to equation $x^2 - Dy^2 = 4$. Let us prove that $\delta = \alpha^2$. If it is false then $\delta < \alpha^2$.

If p is even then, as D is squarefree, q is even too. It means that δ generates a solution to Pell's equation $x^2 - Dy^2 = 1$ which is impossible because $\delta < \alpha^6$.

If p is odd then q is odd too. Hence $p^2 \equiv q^2 \equiv 1 \pmod{8}$. Notice that the number

$$\delta^3 = \frac{(p + q\sqrt{D})^3}{8} = \frac{p(p^2 + 3q^2D)}{8} + \frac{q(3p^2 + q^2D)}{8}$$

generates a solution to Pell's equation $x^2 - Dy^2 = 1$ as $p^2 + 3q^2D$ and $3p^2 + q^2D$ are divisible by 8. It follows that $\delta^3 \geq \alpha^6$ which contradicts to the inequality $\delta < \alpha^2$. Hence $\delta = \alpha^2$ and the number $2\alpha^2$ generates the fundamental solution to equation $x^2 - Dy^2 = 4$. ■

Problem 2.5. Prove that the following equations have no solutions in positive integers:

a) $x^4 - 8z^4 = 1$; b) $x^2 - 2y^4 = 1$.

Solution. a) Let us rewrite the equation as $(x-1)(x+1)(x^2+1) = 8z^4$. It is clear that $x > 1$ and x is odd, so $x = 2y + 1$ for some positive integer y . Then $8y(y+1)(2y^2+2y+1) = 8z^4$ or $y(y+1)(2y^2+2y+1) = z^4$. As $y, y+1, 2y^2+2y+1$ are pairwise coprime, numbers y and $y+1$ should be both perfect 4-th powers, but it is impossible for positive integer y .

b) Since $x^2 = 2y^4 + 1$, we have x is odd and $x = 2z + 1$ for some positive integer z . Then $2z(z+1) = y^4$, so $y = 2t$ for some positive integer t , and $z(z+1) = 8t^4$. The numbers z and $z+1$ are coprime and have different parity. If z is odd then $z = b^4, z+1 = 8c^4$, so $8c^4 = c^4 + 1$ but it is impossible modulo 4. If z is even then $z = 8b^4, z+1 = c^4$ and $c^4 - 8b^4 = 1$. It is impossible by a). ■

It is convenient for some problems provided below to use the method of *infinite descent*: Let P be a property such that integers may or may not possess. If an assumption that a positive integer n_0 has property P leads to the existence of a smaller positive integer $n_1 < n_0$ that also satisfies P then no positive integer has that property. This is so because the reasoning that led from n_0 to n_1 , if applied to the latter will produce $n_2 < n_1$ that has property P too. Since the process could be repeated thus leading to an infinitely decreasing sequence of positive integers - which is impossible - the assumption that P is satisfied by a positive integer implies a contradiction and, hence, is false.

Problem 2.6. Prove that the following equations have no solutions in positive integers:

- a) $x^4 + y^4 = z^2$; б) $x^4 - 2y^2 = 1$; в) $x^4 + y^2 = z^4$;
 г) $x^4 - 2y^2 = -1$, except $(x, y) = (1, 1)$.

Solution. a) If a prime p divides x and y then p^4 divides z^2 , so p^2 divides z . But then $(x', y', z') = (x/p, y/p, z/p^2)$ is a positive solution with $z' < z$, so we can make a step of descent.

Suppose x, y are coprime. So (x^2, y^2, z) is a fundamental Pythagorean triplet, and there exist coprime positive integers m, n , not both odd, with $\{x^2, y^2\} = \{m^2 - n^2, 2mn\}$ and $z = m^2 + n^2$. Without loss of generality $x^2 = m^2 - n^2$ and $y^2 = 2mn$. Note that x is odd and y is even.

Now $x^2 + n^2 = m^2$. A prime divisor of both x and n must divide m , but $\gcd(m, n) = 1$. So x, n are coprime and (x, n, m) is a fundamental Pythagorean triplet. This means that there are coprime positive integers a, b with $\{a^2 - b^2, 2ab\} = \{x, n\}$ and $a^2 + b^2 = m$. Since x is odd, we have $x = a^2 - b^2$ and $n = 2ab$.

Now $y^2 = 2mn = 2(a^2 + b^2)(2ab) = 4(a^2 + b^2)ab$. But $\gcd(a, b) = 1$, so the members of $\{a, b, a^2 + b^2\}$ are pairwise coprime and their product $(y/2)^2$ is a square. Therefore each of $a, b, a^2 + b^2$ is a square and there are positive integers d, e, f with $a = d^2, b = e^2, a^2 + b^2 = f^2$. Hence

$$f^2 = a^2 + b^2 = d^4 + e^4.$$

But

$$f^2 = a^2 + b^2 = m < m^2 + n^2 = z,$$

so $f \leq f^2 < z$. Again we are able to make a step of descent. It follows that equation $x^4 + y^4 = z^2$ has no solutions in positive integers.

b) This equation can be rewritten as $x^4 + y^4 = (y^2 + 1)^2$, so it has no positive integer solutions because equation $x^4 + y^4 = z^2$ has no positive integer solutions.

c) Similarly to a) we suppose that x, y are coprime. Thus, there exist two coprime positive integers a, b with different parity, such that

$$\begin{cases} z^2 = a^2 + b^2 \\ x^2 = a^2 - b^2 \\ y = 2ab \end{cases} \text{ or } \begin{cases} z^2 = a^2 + b^2 \\ x^2 = 2ab \\ y = a^2 - b^2. \end{cases}$$

The first case implies

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

which let us make a step of descent since $a = \sqrt{z^2 - b^2} < z$. In the second case there exist two coprime positive integers α, β such that $a = 2\alpha^2, b = \beta^2$ and $z^2 = 4\alpha^4 + \beta^4$. Clearly z must be odd and there exist two coprime positive integers m, n such that

$$\begin{cases} z = m^2 + n^2 \\ \beta^2 = m^2 - n^2 \\ 2\alpha^2 = 2mn. \end{cases}$$

Again, there exist positive integers γ, δ such that $m = \gamma^2, n = \delta^2$ which let us make a step of descent since

$$\beta^2 = m^2 - n^2 = \gamma^4 - \delta^4$$

and $\gamma < \alpha < 2\alpha^2 = a < z$.

d) Square the equation $2y^2 = x^4 + 1$:

$$4y^4 = (x^4 + 1)^2 = x^8 + 2x^4 + 1.$$

Rearranging and dividing by 2 gives

$$y^4 = \left(\frac{x^2 - 1}{2}\right)^2 + x^4.$$

By b), $x = 1$. Therefore $(x, y) = (1, 1)$ is the only possible solution to equation $x^4 - 2y^2 = -1$ in positive integers. ■

Problem 2.7. Find all the solutions to the following equations in positive integers:

a) $x^2 = 8t^4 - 8t^2 + 1$; b) $x^2 = 2t^4 + 4t^2 + 1$.

Solution. a) Rewrite this equation as $8t^4 = (4t^2 - 1)^2 - x^2 = (4t^2 - 1 - x)(4t^2 - 1 + x)$. As $8t^4, 4t^2 - 1$ are coprime, the greatest common divisor of $4t^2 - 1 - x$ and $4t^2 - 1 + x$ is equal to 2. Then there exist coprime positive a, b such that $t = ab$ and

$$\{4t^2 - 1 - n, 4t^2 - 1 + n\} = \{4a^4, 2b^4\}.$$

It means that

$$4(ab)^2 - 1 = 4t^2 - 1 = 2a^4 + b^4 \implies b^4 - 2(a^2 - b^2)^2 = 1.$$

By Problem 2.6.b this is possible only if $a = b = 1$, so $(x, t) = (1, 1)$ is the only positive integer solution to given equation.

b) Similarly,

$$2t^4 = (2t^2 + 1)^2 - x^2 = (2t^2 + 1 - x)(2t^2 + 1 + x)$$

and

$$\gcd(2t^2 + 1 - x, 2t^2 + 1 + x) = 2.$$

Then there exist positive integers a, b such that $t = 2ab$ and

$$\{2t^2 + 1 - n, 2t^2 + 1 + n\} = \{16a^4, 2b^4\}.$$

It means that

$$2(2ab)^2 + 1 = 2t^2 + 1 = 8a^4 + b^4 \implies b^4 - 2(2a^2 - b^2)^2 = -1.$$

By Problem 2.6.d it follows that $a = b = 1$, so $(x, t) = (7, 2)$ is the only positive integer solution to given equation. ■

Consider the equation $x^4 - 6y^2 = 1$. The minimal solution to Pell's equation $x^2 - 6y^2 = 1$ is $(5, 2)$, so all the solutions (u_k, v_k) are described by

$$u_k + v_k\sqrt{6} = (5 + 2\sqrt{6})^k.$$

Particularly,

$$u_k = \frac{1}{2} \left((5 + 2\sqrt{6})^k + (5 - 2\sqrt{6})^k \right).$$

Note that if equation $x^4 - 6y^2 = 1$ has a positive integer solution then $x^2 = u_k$ for some positive integer k .

Problem 2.8.

- Prove that k is even.
- Express u_{2l} as a polynomial in u_l .
- Prove that k is not divisible by 4.
- Prove that $u_{2l+1} - 1$ is a square of an integer.
- Find all the solutions to equation $x^4 - 6y^2 = 1$ in positive integers.

Solution. a) $u_k \equiv -1 \pmod{3}$ for odd k , so u_k never is a perfect square.

b) $u_{2l} = 2u_l^2 - 1$.

c) If $k = 4l$ for some positive integer l then by b)

$$u_{4l} = 2u_{2l}^2 - 1 = 2(2u_l^2 - 1)^2 - 1 = 8u_l^4 - 8u_l^2 + 1.$$

By Problem 2.7.a it follows that $u_l = 1$, this is impossible for positive l .

d) Note that $5 + 2\sqrt{6} = \frac{1}{2}(2 + \sqrt{6})^2$. Hence

$$\begin{aligned} u_{2l+1} &= \frac{1}{2} \left((5 + 2\sqrt{6})^{2l+1} + (5 - 2\sqrt{6})^{2l+1} \right) = \frac{1}{2^{2l+2}} \left((2 + \sqrt{6})^{2l+1} + (2 - \sqrt{6})^{2l+1} \right)^2 + 1 = \\ &= \left(\frac{(2 + \sqrt{6})^{2l+1} + (2 - \sqrt{6})^{2l+1}}{2^{l+1}} \right)^2 + 1. \end{aligned}$$

e) It remains to consider the case $k = 4l + 2$. By d) we know that $u_{2l+1} = c^2 + 1$ for some positive integer c . Furthermore $x^2 = u_{4l+2} = 2(c^2 + 1)^2 - 1 = 2c^4 + 4c^2 + 1$. It follows from Problem 2.7.b that $x = 7$. Hence $(x, y) = (7, 20)$ is the only positive integer solution to equation $x^4 - 6y^2 = 1$. ■

Problem 2.9. a) Prove that if equation $x^2 - Dy^2 = 2$ has a solution then it has a single class of solutions. Also, if $\alpha = u + v\sqrt{D}$ generates the fundamental solution to $x^2 - Dy^2 = 2$ then the fundamental solution to $x^2 - Dy^2 = 1$ is given by $\beta = \alpha^2/2$.

b) Prove that equation $x^2 + 1 = 2(t^2 - 1)^2$ has no solutions in positive integers.

c) Prove that if equation $x^2 - Dy^2 = 2$ has an integer solution then equation $x^4 - Dy^2 = 1$ has no solutions in positive integers.

Solution. a) Consider some class of solutions to equation $x^2 - Dy^2 = 2$ with minimal solution (u, v) . By definition,

$$1 < \alpha = u + v\sqrt{D} \leq \beta,$$

where β generates the fundamental solution to $x^2 - Dy^2 = 1$. Since

$$\alpha^2/2 = u^2 - 1 + uv\sqrt{D},$$

we have that $(u^2 - 1, uv)$ is another solution to Pell's equation $x^2 - Dy^2 = 1$. It means that $\alpha^2/2 = \beta^l$ for some integer l . From the inequalities $1 < \alpha^2/2 \leq \beta^2/2 < \beta^2$ it follows that $l = 1$.

b) Since the left side of equation is not divisible by 4, we obtain that t is even. Then

$$t^2 - 1 \equiv 3 \pmod{4}$$

and $x^2 + 1$ has a prime divisor $p \equiv 3 \pmod{4}$ which is impossible.

c) The equation $x^4 - 2y^2 = 1$ has no positive integer solutions by Problem 2.6.b, so we assume that $D > 2$.

If $\alpha = u + v\sqrt{D}$ generates the fundamental solution to $x^2 - Dy^2 = 2$ then the fundamental solution to the corresponding Pell's equation is given by $\beta = \alpha^2/2$ in view of a). Thus if $x^4 - Dy^2 = 1$ then

$$x^2 = \frac{\beta^n + \beta'^n}{2} = \frac{\alpha^{2n} + \alpha'^{2n}}{2^{n+1}},$$

i.e.,

$$x^2 + 1 = \frac{\alpha^{2n} + \alpha'^{2n} + 2(\alpha\alpha')^n}{2^{n+1}} = \frac{(\alpha^n + \alpha'^n)^2}{2^{n+1}}.$$

Now $\alpha^n + \alpha'^n$ is an integer, and so either n is odd yielding $x^2 + 1 = s^2$ whence $x = 0$ which is impossible or $n = 2m$ is even whence

$$x^2 + 1 = 2s^2,$$

where

$$s = \frac{\alpha^{2m} + \alpha'^{2m}}{2^{m+1}}.$$

Then

$$s + 1 = \frac{(\alpha^m + \alpha'^m)^2}{2^{m+1}} = t^2 \quad \text{or} \quad 2t^2.$$

If $s = t^2 - 1$ then

$$x^2 + 1 = 2(t^2 - 1)^2$$

which is impossible by b).

Finally, if $s = 2t^2 - 1$ then

$$x^2 = 8t^4 - 8t^2 + 1$$

and $x = 1$ by Problem 2.7.a. It follows that $y = 0$ which is a contradiction. ■

Problem 2.10. Prove that if equation $x^2 - Dy^2 = -2$ has a solution then equation $x^4 - Dy^2 = 1$ has no solutions in positive integers with the sole exception $D = 6$.

Solution. As in the previous problem, we may suppose that $D > 2$. In the same way as in Problem 2.9.a we obtain that equation $x^2 - Dy^2 = -2$ has a single class of solutions and if $\alpha = u + v\sqrt{D}$ is the fundamental solution then the fundamental solution to the corresponding Pell's equation is $\beta = \alpha^2/2$. In this case of course $\alpha\alpha' = -2$. If $x^4 - Dy^2 = 1$ then

$$x^2 = \frac{\beta^n + \beta'^n}{2} = \frac{\alpha^{2n} + \alpha'^{2n}}{2^{n+1}},$$

i.e.,

$$x^2 + (-1)^n = \frac{(\alpha^n + \alpha'^n)^2}{2^{n+1}}.$$

Thus if n is odd we obtain $x^2 - 1 = s^2$ whence $x = 1$, i.e. $y = 0$, while if $n = 2m$ is even then

$$x^2 + 1 = 2s^2,$$

where

$$s = \frac{\alpha^{2m} + \alpha'^{2m}}{2^{m+1}}.$$

Thus

$$s + (-1)^m = \frac{(\alpha^m + \alpha'^m)^2}{2^{m+1}}.$$

Now if m is even then $s + 1 = 2t^2$ and

$$x^2 = 8t^4 - 8t^2 + 1$$

which is impossible by Problem 2.7.a.

If m is odd then $s - 1 = t^2$ and so

$$x^2 = 2(t^2 + 1)^2 - 1 = 2t^4 + 4t^2 + 1.$$

By Problem 2.7.b this is possible only if $(x, t) = (7, 2)$. Hence

$$Dy^2 = x^4 - 1 = 2400 = 2^5 \cdot 3 \cdot 5^2.$$

Since equation $x^2 - Dy^2 = -2$ has a solution, we get D is not divisible by 4 and 5. Thus we must have $D = 6$ and there is the only solution $(x, y) = (7, 20)$ by Problem 2.8. ■

3 On the diophantine m -tuples and the equation $x^2 - (k^2 + 1)y^2 = k^2$

Definition. Let n be an integer. A set of m different positive integers is called a *Diophantine m -tuple with the property $D(n)$* or simply *$D(n)$ - m -tuple* if the product of any two of them increased by n is a perfect square.

Problem 3.1. Prove that there does not exist a $D(n)$ -quadruple for any $n \equiv 2 \pmod{4}$.

Solution. Suppose that $\{x_1, x_2, x_3, x_4\}$ is a $D(n)$ -quadruple with $n \equiv 2 \pmod{4}$. Then

$$x_i x_j + n \equiv 0 \text{ or } 1 \pmod{4}$$

so that

$$x_i x_j \equiv 2 \text{ or } 3 \pmod{4}.$$

Hence at most one of the x_i can be even; without loss of generality, we may assume that x_1, x_2 and x_3 are odd. This implies that

$$x_i x_j \equiv 3 \pmod{4} \quad \text{for } 1 \leq i \neq j \leq 3$$

Thus x_1, x_2, x_3 have different odd residues modulo 4 which is impossible. ■

For the case $n = 1$, the problem of existence of such m -tuples was first studied by Diophantus, and he found a set of four positive rationals with the above property: $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$. However the first $D(1)$ -quadruple, the set $\{1, 3, 8, 120\}$, was found by Fermat. The folklore conjecture is that there does not exist a $D(1)$ -quintuple. Recently, Dujella proved that there is no $D(1)$ -sextuple and there are only finitely many $D(1)$ -quintuples.

Problem 3.2. Prove that every $D(1)$ -couple can be extended to a $D(1)$ -triple.

Solution. Let $\{a, b\}$ be a $D(1)$ -couple. The number

$$c = a + b + 2\sqrt{ab + 1}$$

extends this $D(1)$ -couple to $D(1)$ -triple. ■

Problem 3.3. Show that every $D(1)$ -triple $\{a, b, c\}$ can be extended to a $D(1)$ -quadruple:

a) Prove that quadratic equation

$$t^2 + a^2 + b^2 + c^2 - 2(ta + tb + tc + ab + bc + ca) - 4abct - 4 = 0$$

has at least one positive integer solution t_0 .

b) Prove that $\{a, b, c, t_0\}$ is a $D(1)$ -quadruple.

Solution. a) Direct computation shows that

$$t_0 = a + b + c + 2abc + 2\sqrt{(ab + 1)(bc + 1)(ca + 1)}$$

is a positive integer solution to the given equation.

b) It remains to check that numbers $at_0 + 1, bt_0 + 1, ct_0 + 1$ are perfect squares. This is true because of the following identities:

$$(a + b - c - t_0)^2 = 4(ab + 1)(ct_0 + 1),$$

$$(c + a - b - t_0)^2 = 4(ca + 1)(bt_0 + 1),$$

$$(b + c - a - t_0)^2 = 4(bc + 1)(at_0 + 1).$$
■

In 1969, Baker and Davenport proved that the Fermat set cannot be extended to a $D(1)$ -quintuple.

By definition, if $\{a, b, c\}$ is a $D(1)$ -triple then there exist positive integers u, v, w such that

$$ab + 1 = w^2, \quad bc + 1 = u^2, \quad ca + 1 = v^2.$$

Since

$$bv^2 - au^2 = b(ac + 1) - a(bc + 1) = b - a,$$

the equation $bx^2 - ay^2 = b - a$ has a positive integer solution (v, u) . Notice that Pell's equation $x^2 - aby^2 = 1$ has a solution $(w, 1)$. Let $\alpha = v\sqrt{b} + u\sqrt{a}$ and $\beta = w + \sqrt{ab}$.

Problem 3.4. a) Prove that for any integer l the number $\alpha\beta^l$ is of the form

$$v_l\sqrt{b} + u_l\sqrt{a},$$

where (v_l, u_l) is a solution to equation

$$bx^2 - ay^2 = b - a.$$

b) Prove that if $c \geq |b - a|$ then $u_{-1}, v_{-1} > 0$.

c) Prove that there exists a nonnegative integer c' such that

$$bc' + 1 = u_{-1}^2, \quad ac' + 1 = v_{-1}^2.$$

d) Prove that every $D(1)$ -couple $\{a_1, a_2\}$ has exactly one extension to $D(1)$ -triple $\{a_1, a_2, a_3\}$ such that

$$\max\{a_1, a_2\} < a_3 < 4a_1a_2.$$

Solution. a) By direct computation we see that $\alpha\beta^l$ is of the form $v_l\sqrt{b} + u_l\sqrt{a}$ with integer u_l, v_l . It follows that

$$(v_l\sqrt{b} - u_l\sqrt{a})(w - \sqrt{ab}) = v_l\sqrt{b} - u_l\sqrt{a}.$$

Multiplying both identities, we get

$$bv_l^2 - au_l^2 = (bv^2 - au^2)(w^2 - ab)^l = b - a.$$

b) Notice that

$$v_{-1} = vw - au, \quad u_{-1} = uw - bv$$

so it is enough to prove the following inequalities:

$$vw > au, \quad uw > bv.$$

Squaring the first inequality we get

$$(ac + 1)(ac + 1) > a^2(bc + 1)$$

or

$$a^2bc + ac + ab + 1 > a^2bc + a^2$$

which is true when $c + b \geq a$. Similarly we get that the second inequality is true when $c + a \geq b$.

c) The number

$$c' = 2abc + a + b + c - 2wuv$$

satisfies the above conditions. Also

$$c' \geq \frac{u_{-1}^2 - 1}{b} \geq 0.$$

d) Let $a = \min\{a_1, a_2\}$, $b = \max\{a_1, a_2\}$, $c = a_3$ then $a < b < c$. By b) we see that u_{-1} and v_{-1} are positive and

$$v = wv_{-1} + au_{-1}, \quad u = wu_{-1} + bv_{-1}.$$

Hence

$$\begin{aligned} ac + 1 &= v^2 = (wv_{-1} + au_{-1})^2 = \\ &= (ab + 1)(ac' + 1) + a^2(bc' + 1) + 2awv_{-1}u_{-1} = \\ &= ((ab + 1)a + a^2b)c' + a^2 + ab + 1 + 2wav_{-1}u_{-1}. \end{aligned}$$

Subtracting 1 and dividing by a , we get

$$c = (2ab + 1)c' + a + b + 2wv_{-1}u_{-1}.$$

If $c' = 0$ then $v_{-1} = u_{-1} = 1$ and $b < c = a + b + 2w < 4ab$. If $c' \geq 1$ then

$$c > 2ab + 1 + a + b + 2\sqrt{ab}\sqrt{ac'}\sqrt{bc'} > 4ab.$$

■

Problem 3.5. a) Prove that there are infinitely many arithmetic progressions of length 3 that are also $D(1)$ -triples.

b) Prove that there are no arithmetic progressions of length 4 that are also $D(1)$ -quadruples.

Solution. a) Let (l, k) be a solution to Pell's equation $x^2 - 3y^2 = 1$. Let

$$a = 2k - l, b = 2k, c = 2k + l$$

(one can check that $a, b, c > 0$), then

$$ab + 1 = 4k^2 - 2kl + 1 = k^2 + l^2 - 1 - 2kl + 1 = (k - l)^2,$$

$$bc + 1 = 4k^2 + 2kl + 1 = k^2 + l^2 - 1 + 2kl + 1 = (k + l)^2,$$

$$ca + 1 = 4k^2 - l^2 + 1 = k^2.$$

Hence the set $\{a, b, c\}$ satisfies the conditions of the problem.

b) Let $\{a, b, c, d\}$ be such a $D(1)$ -quadruple with $a < b < c < d$.

Solution I: By Problem 3.3.d this is possible only if $d > 4ab$. But

$$d = a + 3(b - a) < 3b < 4ab,$$

that's a contradiction.

Solution II (by M. Demidkin, G. Kostitsyn): Numbers $(db + 1)(dc + 1)$ and $d^2(bc + 1)$ are perfect squares with the difference that is equal to $d(b + c - d) + 1 = ad + 1$. On the other hand, this difference should be at least $2d\sqrt{bc + 1} + 1$. But

$$2d\sqrt{bc + 1} + 1 > 2da + 1 > ad + 1$$

which is a contradiction. ■

Consider the case $n = -1$. It is easy to find some $D(-1)$ -triples, for example, $\{1, 2, 5\}$, $\{1, 5, 10\}$, $\{1, 26, 37\}$.

Problem 3.6. a) Prove that every $D(-1)$ -couple $\{a_1, a_2\}$ can be extended to a $D(-1)$ -triple $\{a_1, a_2, a_3\}$.

b) Prove that there exists exactly one extension such that

$$\max\{a_1, a_2\} < a_3 \leq 3a_1a_2.$$

Solution. Let $a = \min\{a_1, a_2\}$, $b = \max\{a_1, a_2\}$, $c = a_3$, then $a < b < c$ and

$$ab - 1 = w^2, \quad bc - 1 = u^2, \quad ca - 1 = v^2$$

for some positive integers u, v, w . Since

$$bv^2 - au^2 = b(ac + 1) - a(bc + 1) = a - b,$$

we obtain that equation $bx^2 - ay^2 = a - b$ has a positive integer solution (v, u) . Notice that equation $x^2 - aby^2 = -1$ has a solution $(w, 1)$. Let $\alpha = v\sqrt{b} + u\sqrt{a}$ and $\beta = w + \sqrt{ab}$.

In the same way as in Problem 3.4 one can show that for any integer l the number $\alpha\beta^l$ is of the form $v_l\sqrt{b} + u_l\sqrt{a}$, where (v_l, u_l) is a solution to equation

$$bx^2 - ay^2 = (-1)^l(a - b).$$

Similarly it is easy to check that $u_{-1}, v_{-1} > 0$ and

$$ac' + 1 = v_{-1}^2, \quad bc' + 1 = u_{-1}^2$$

for a nonnegative integer c' such that

$$c = 2abc' + a + b - c' + 2u_{-1}v_{-1}w.$$

If $c' = 0$ then $b < c = a + b + 2\sqrt{ab} - 1 \leq 3ab$ otherwise $c' \geq 1$ and $c > 3ab$. ■

It is known that some particular $D(-1)$ -triples, for example, $\{1, 2, 5\}$, cannot be extended to $D(-1)$ -quadruples. Moreover, Dujella and Brown proved that some infinite families of $D(-1)$ -triples cannot be extended to quadruples.

Problem 3.7. Prove that $D(-1)$ -triple $\{n^2 + 1, (n + 1)^2 + 1, (2n + 1)^2 + 4\}$ cannot be extended to a $D(-1)$ -quadruple if

- a) $n \equiv 1 \pmod{4}$;
- b) $n \equiv 2 \pmod{4}$;
- c) $n = 4$.

Solution. Suppose $\{n^2 + 1, (n + 1)^2 + 1, (2n + 1)^2 + 4, d\}$ is a $D(-1)$ -quadruple. Then

$$(n^2 + 1)d - 1 = x^2,$$

$$((n + 1)^2 + 1)d - 1 = y^2,$$

$$((2n + 1)^2 + 4)d - 1 = z^2.$$

After eliminating d we get the following system of equations:

$$(n^2 + 1)y^2 - ((n + 1)^2 + 1)x^2 = 2n + 1, \quad (1)$$

$$(n^2 + 1)z^2 - ((2n + 1)^2 + 4)x^2 = 3n^2 + 4n + 4, \quad (2)$$

$$((n + 1)^2 + 1)z^2 - ((2n + 1)^2 + 4)y^2 = 3n^2 + 2n + 3. \quad (3)$$

- a) If $n = 4k + 1$ then (1) becomes

$$2y^2 - x^2 \equiv -1 \pmod{4}$$

so that x is odd. Further,

$$n^2 + 1 \equiv 8k + 2 \pmod{16},$$

$$(n + 1)^2 + 1 \equiv 5 \pmod{16},$$

$$(2n + 1)^2 + 4 \equiv 13 \pmod{16}.$$

Hence (3) becomes

$$5z^2 - 13y^2 \equiv 8 \pmod{16}$$

so that y and z are both odd. Then (2) yields

$$(8k + 2)z^2 - 13x^2 \equiv 8k + 11 \pmod{16},$$

$$2 + 3x^2 \equiv 11 \pmod{16},$$

$$x^2 \equiv 3 \pmod{16}$$

which is a contradiction.

- b) Next, suppose that $n = 2k$ with odd k . Then (1) becomes

$$y^2 - 2x^2 \equiv 1 \pmod{4}$$

so that y is odd and x is even. Now (3) becomes

$$2z^2 - 5y^2 \equiv 3 \pmod{8}$$

so that z is even. Putting $z = 2u$ and $x = 2v$ in (2) leads to the equation

$$(4k^2 + 1)u^2 - (16k^2 + 8k + 5)v^2 = 3k^2 + 2k + 1.$$

As k is odd this leads to the congruence

$$u^2 - 5v^2 \equiv \pm 2 \pmod{8}$$

which is impossible.

c) If $n = 4$ then equations (1) and (2) become

$$17y^2 - 26x^2 = 9,$$

$$z^2 - 5x^2 = 4.$$

The first equation gives that

$$y^2 - 2x^2 \equiv 1 \pmod{8}$$

which implies that x is even. Hence z is also even; putting $z = 2u$ and $x = 2v$ yields

$$17y^2 - 104v^2 = 9,$$

$$u^2 - 5v^2 = 1.$$

All the solutions to Pell's equation $x^2 - 5y^2 = 1$ are given by

$$u_n + v_n\sqrt{5} = (9 + 4\sqrt{5})^n$$

with integer n . The following recurrence is true:

$$v_0 = 0, \quad v_1 = 4, \quad v_{n+1} = 18v_n - v_{n-1}$$

so it follows that $v \equiv 0, 4$ or $13 \pmod{17}$.

Now look at equation $17y^2 - 104v^2 = 9$ modulo 17:

$$-2v^2 \equiv 9 \pmod{17}$$

or

$$v^2 \equiv 4 \pmod{17}$$

which is impossible when $v \equiv 0, 4$ or $13 \pmod{17}$.

■

Let $\{a, b, c\}$ be a $D(-1)$ -triple and let r, s, t be nonnegative integers defined by

$$ab - 1 = r^2, \quad ac - 1 = s^2, \quad bc - 1 = t^2.$$

Assume that there exists a positive integer d that extends this $D(-1)$ -triple to a $D(-1)$ -quadruple. We have

$$ad - 1 = x'^2, \quad bd - 1 = y'^2, \quad cd - 1 = z'^2$$

with nonnegative integers x', y', z' .

Eliminating d from previous equalities, we obtain that x', y', z' form a solution to the following system of equations:

$$\begin{aligned} ay^2 - bx^2 &= b - a, \\ az^2 - cx^2 &= c - a, \\ bz^2 - cy^2 &= c - b. \end{aligned}$$

Problem 3.8. Suppose $2 \leq a < b < c < d$.

a) Prove that there exist integer solutions (z_0, x_0) and (z_1, y_1) to equations

$$az^2 - cx^2 = c - a \quad \text{and} \quad bz^2 - cy^2 = c - b$$

respectively such that

$$\begin{aligned} |x_0| &< s, \quad 0 < z_0 < c, \\ |y_1| &< t, \quad 0 < z_1 < c, \\ z'\sqrt{a} + x'\sqrt{c} &= (z_0\sqrt{a} + x_0\sqrt{c})(s + \sqrt{ac})^{2m}, \\ z'\sqrt{b} + y'\sqrt{c} &= (z_1\sqrt{b} + y_1\sqrt{c})(t + \sqrt{bc})^{2n} \end{aligned}$$

with nonnegative integers m, n .

b) Prove that $z_0 = z_1$.

c) Prove that there exists $d_0 < c$ such that $\{a, b, c, d_0\}$ is also a $D(-1)$ -quadruple.

Solution. a) It is enough to prove the statement only for equation $az^2 - cx^2 = c - a$. Notice that $\alpha = s + \sqrt{ac}$ generates the fundamental solution to equation $x^2 - acy^2 = -1$ and by Problem 2.1 α^2 generates the fundamental solution to Pell's equation $x^2 - acy^2 = 1$. Thus for any integer l numbers $(z'\sqrt{a} + x'\sqrt{c})\alpha^{2l}$ generate solutions to equation $az^2 - cx^2 = c - a$ and there is a solution (z_0, x_0) such that

$$\alpha^{-1}\sqrt{c-a} < \gamma = z_0\sqrt{a} + x_0\sqrt{c} \leq \alpha\sqrt{c-a}.$$

Since

$$\gamma' = z_0\sqrt{a} - x_0\sqrt{c} = \frac{c-a}{z_0\sqrt{a} + x_0\sqrt{c}},$$

we have

$$\alpha^{-1}\sqrt{c-a} < \gamma' = z_0\sqrt{a} - x_0\sqrt{c} \leq \alpha\sqrt{c-a}.$$

It follows that

$$2|x_0|\sqrt{c} = |\gamma - \gamma'| \leq |\alpha - \alpha^{-1}| = 2s\sqrt{c-a}.$$

Therefore $|x_0| \leq s\sqrt{c-a}/\sqrt{c} < s$. Also

$$2\alpha^{-1} < \gamma - \gamma' = 2z_0\sqrt{a},$$

it means that $z_0 > 0$. Suppose $z_0 \geq c$. Since $|x_0| < s$, we have

$$c - a = az_0^2 - cx_0^2 \geq ac^2 - cs^2 = c(ac - s^2) = c > c - a$$

which is a contradiction.

b) It is easy to see that

$$z' \equiv (-1)^m z_0 \equiv (-1)^n z_1 \pmod{2c}.$$

It follows from a) that $0 < z_0 + z_1 < 2c$ so $z_0 = z_1$ is the only possible option.

c) Since $z_0^2 \equiv z'^2 \equiv -1 \pmod{c}$, there is a positive integer

$$d_0 = \frac{z_0^2 + 1}{c} < c.$$

It is easy to check that $ad_0 - 1 = x_0^2$ and $bd_0 - 1 = y_1^2$ which shows that $ad_0 - 1, bd_0 - 1, cd_0 - 1$ are perfect squares. ■

Suppose there exists at least one $D(-1)$ -quadruple that does not contain number 1. It follows from the previous problem and from the method of infinite descent that there is another $D(-1)$ -quadruple that contains 1.

Existence of $D(-1)$ -quadruples is closely related to the number of classes of solutions to Diophantine equation $x^2 - (k^2 + 1)y^2 = k^2$.

Problem 3.9. a) Prove that for any integer $k > 1$ every class of solutions to the equation $x^2 - (k^2 + 1)y^2 = k^2$ contains exactly one solution x_0, y_0 with $|y_0| < k$.

b) Prove that this equation has at least three different classes of solutions.

Solution. a) Note that $\alpha = 2k^2 + 1 + 2k\sqrt{k^2 + 1}$ generates the fundamental solution to Pell's equation $x^2 - (k^2 + 1)y^2 = 1$ and $\beta = k + \sqrt{k^2 + 1}$ generates the fundamental solution to equation $x^2 - (k^2 + 1)y^2 = -1$. Take any class of solutions to equation $x^2 - (k^2 + 1)y^2 = k^2$ and consider solution (x_0, y_0) in this class such that

$$k\beta^{-1} < \gamma = x_0 + y_0\sqrt{k^2 + 1} < k\beta.$$

There is exactly one such solution because $k\beta/(k\beta^{-1}) = \beta^2 = \alpha$ by Problem 2.1. The inequalities are sharp because γ and $k\beta$ generate solutions to different equations.

Since

$$2|y_0|\sqrt{k^2 + 1} = |\gamma - \gamma'| = |\gamma - k^2\gamma^{-1}| < |k\beta - k\beta^{-1}| = 2k\sqrt{k^2 + 1},$$

we have $|y_0| < k$. Similarly we get that $y_0 > k$ for $\gamma > k\beta$ and $y_0 < -k$ for $\gamma < k\beta^{-1}$. This means that every class of solutions to the equation $x^2 - (k^2 + 1)y^2 = k^2$ contains exactly one solution (x_0, y_0) with $|y_0| < k$.

b) Solutions $(k, 0)$, $(k^2 - k + 1, k - 1)$ (belongs to the integer -1) and $(k^2 - k + 1, 1 - k)$ (belongs to the integer 1) represent different classes by a). ■

Definition. We call a solution (x_0, y_0) to $x^2 - (k^2 + 1)y^2 = k^2$ with $k > 1$ an *exceptional solution* if $x_0 > 0$ and $0 < y_0 < k - 1$.

Problem 3.10. Suppose $\{1, a, b, c\}$ is a $D(-1)$ -quadruple. Prove that there exists $k > 1$ such that equation $x^2 - (k^2 + 1)y^2 = k^2$ has at least two exceptional solutions (or, equivalently, more than 5 classes of solutions).

Solution. Without loss of generality, $a < b < c$ and

$$a = i^2 + 1, b = j^2 + 1, c = k^2 + 1$$

for some positive integers i, j, k .

From the solution to Problem 3.6 it follows that either $c = a + b + 2\sqrt{ab - 1}$ or $c > 3ab$. Hence $j < k - 1$.

Now consider the equation $(y^2 + 1)(k^2 + 1) = x^2 + 1$, i.e.,

$$x^2 - (k^2 + 1)y^2 = k^2.$$

This equation has at least two solutions with $0 < y < k - 1$, namely, $y = i$ and $y = j$. ■

Problem 3.11. Prove that equation

$$x^2 - (k^2 + 1)y^2 = k^2$$

- a) has no exceptional solutions if $k^2 + 1$ is a prime;
- b) has no exceptional solutions if $k = p^i$ for any odd prime p and positive integer i ;
- c) has at most one exceptional solution if $k = pq$ for any distinct odd primes p, q ;
- d) has at most one exceptional solution if $k = p^i q^j$ for any distinct odd primes p, q and positive integers i, j .

Solution.

a) Notice that $x^2 - k^2 = (x - k)(x + k)$ is divisible by prime $k^2 + 1$. This means that either $x - k$ or $x + k$ is divisible by $k^2 + 1$. Hence $x \geq (k^2 + 1) - k$ and

$$y^2 = \frac{x^2 - k^2}{k^2 + 1} \geq \frac{(k^2 + 1)(k^2 - 2k + 1)}{k^2 + 1} = (k - 1)^2.$$

By definition, it follows that this equation has no exceptional solutions.

b) Let (x_0, y_0) be a solution to equation $x^2 - (k^2 + 1)y^2 = k^2$. Denote $\gcd(x_0, y_0)$ by n , then $k = ln$ for some positive integer l . Then equation

$$x^2 - (l^2 n^2 + 1)y^2 = l^2$$

has a primitive solution $(x_0/n, y_0/n)$.

If $l \leq n$ then $l^2 < \sqrt{l^2 n^2 + 1}$ and by Problem 1.6 all the solutions to equation

$$x^2 - (l^2 n^2 + 1)y^2 = l^2$$

should be of the form (p_m, q_m) , where p_m/q_m is a convergent to $\sqrt{l^2 n^2 + 1}$.

Since $\sqrt{l^2 n^2 + 1} = [ln, \overline{2ln}]$, we get by Problem 1.10 that a sequence $p_m^2 - (l^2 n^2 + 1)q_m^2$ has a period 1 or 2. It is easy to check that $p_m - (l^2 n^2 + 1)q_m^2 = \pm 1$. Hence $l = 1$ and $n = k$. As y_0 is divisible by k , the solution (x_0, y_0) could not be exceptional.

If $l > n$ then $l = p^j$ for some $j > i/2$. A congruence $s^2 \equiv p^{2i} + 1 \pmod{p^{2j}}$ has the only solutions $s \equiv \pm 1 \pmod{p^{2j}}$. Hence all the solutions to equation

$$x^2 - (l^2 n^2 + 1)y^2 = l^2$$

belong to either -1 or 1 . By Problem 1.14 equation $t^2 - (l^2 n^2 + 1)u^2 = m$ with

$$m = \frac{s^2 - (l^2 n^2 + 1)}{l^2} = -n^2$$

has a solution (t_0, u_0) that belongs to ± 1 . As $|-n^2| < \sqrt{l^2 n^2 + 1}$, by Problem 1.6 all the solutions to equation

$$x^2 - (l^2 n^2 + 1)y^2 = -n^2$$

should be of the form (p_m, q_m) . Since $p_m - (l^2 n^2 + 1)q_m^2 = \pm 1$, we have $n = 1$. Hence for $l > n$ all the solutions to equation $x^2 - (k^2 + 1)y^2 = k^2$ are primitive and belong to ± 1 . The solution $(k^2 - k + 1, -k + 1)$ belongs to 1 and the solution $(k^2 - k + 1, k - 1)$ belongs to -1 . By Problem 1.13 any solution to equation $x^2 - (k^2 + 1)y^2 = k^2$ is in the same class with one of solutions $(k^2 - k + 1, \pm(k - 1))$. It follows from Problem 3.9 that this equation has no exceptional solutions.

c) **(by V. Patrushev):** Let (x_0, y_0) be an exceptional solution to equation

$$x^2 - (p^2 q^2 + 1)y^2 = p^2 q^2.$$

Denote

$$d_- = \gcd(x_0 - y_0, p^2 q^2), d_+ = \gcd(x_0 + y_0, p^2 q^2).$$

Since $(x_0 - y_0)(x_0 + y_0) = x_0^2 - y_0^2$ is divisible by $p^2 q^2$, we have $d_- d_+ = p^2 q^2$. Consider three cases:

1) $d_- = p^2, d_+ = q^2$. Then x_0, y_0 are coprime and solution (x_0, y_0) is primitive and it belongs to the integer k such that

$$k \equiv 1 \pmod{p^2}, \quad k \equiv -1 \pmod{q^2}.$$

By CRT there exists exactly one such integer k modulo $p^2 q^2$.

2) $d_- = q^2, d_+ = p^2$. Similarly (x_0, y_0) is a primitive solution and it belongs to the integer l such that

$$l \equiv -1 \pmod{q^2}, \quad l \equiv 1 \pmod{p^2}.$$

By CRT there exists exactly one such integer l modulo p^2q^2 , moreover, $l \equiv -k \pmod{p^2q^2}$.

3) Either d_- or d_+ is divisible by pq . Let $r = x_0 - pqy_0$, then $r \equiv \pm y_0 \pmod{pq}$. It is easy to see that $0 < r < pq$. Since $y_0 < pq$, we have either $r = y_0$ or $r = pr - y_0$.

If $r = y_0$ then $2pqy_0^2 = p^2q^2$ which is impossible modulo 2. If $r = pq - y_0$ then $y_0 = pq - 1$ which could not be a second coordinate of an exceptional solution.

It follows that there exist at most two exceptional solutions: (x_1, y_1) that belongs to the integer k and (x_2, y_2) that belongs to the integer $-k$. Since $(x_2, -y_2)$ belongs to the integer k and $|y_1|, |-y_2| < pq$, by Problem 3.9.a we have $y_1 = -y_2$ which contradicts inequalities $y_1, y_2 > 0$. Hence there exists at most one exceptional solution.

d) See [11].

■

Problem 3.12. Is it possible to find an integer $k > 1$ such that equation

$$x^2 - (k^2 + 1)y^2 = k^2$$

has at least two exceptional solutions?

Solution. It is an open question known as Dujella's unicity conjecture.

■

Acknowledgements.

Authors would like to thank B. Frenkin and M. Surkov for their helpful comments, which improved the exposition.

References.

1. J. E. Shockley, Introduction to Number Theory, Holt, Rinehart and Winston, Inc., New York-Toronto, Ont.-London (1967).
2. M. Waldschmidt, Continued fractions, Ecole de recherche CIMPA-Oujda, Théorie des Nombres et ses Applications, 18 - 29 mai 2015: Oujda (Maroc).
3. JHE Cohn, The Diophantine equation $x^4 - Dy^2 = 1$, Quart. J. Math. Oxford (2) 26 pp. 279-281 (1975).
4. JHE Cohn, Some quartic Diophantine equations, Pacific J. Math. 26(2): 233-243 (1968).
5. A. Dujella, On the size of Diophantine m-tuples. Mathematical Proceedings of the Cambridge Philosophical Society, 132, pp. 23-33 (2002).
6. E. Brown, Sets in which $xy + k$ is always a square. Math. Comp. 45, pp. 613-620 (1985).

7. B. W. Jones, A second variation on a problem of Diophantus and Davenport, *Fibonacci Quart.* 16 pp. 155-165(1978).
8. A. Dujella, C. Fuchs, Complete solution of a problem of Diophantus and Euler. *J. London Math. Soc.* 71, pp. 33–52 (2005).
9. K. Matthews, J. Robertson, J. White, On a diophantine equation of Andrej Dujella, *Math. Glasnik*, 48, number 2, pp. 265-289 (2013).
10. A. Srinivasan, $D(-1)$ quadruples and products of two primes, *Glas. Mat. Ser. III* 50, pp. 261–268 (2015).
11. M. Le, A. Srinivasan, Note on Dujella’s unicity conjecture, *Glas. Mat.* Vol. 58(78), pp. 59 – 65 (2023).
12. <https://artofproblemsolving.com/community/c6h1186131p5767378>
13. <https://artofproblemsolving.com/community/c6h577945p3408321>
14. <https://artofproblemsolving.com/community/c6h1849278p12466367>
15. <https://artofproblemsolving.com/community/c6h2183565p16353210>
16. <https://artofproblemsolving.com/community/c146h150369p849188>
17. <https://artofproblemsolving.com/community/c146t383f146h150370>
18. <https://artofproblemsolving.com/community/c6h553573p3216004>