Introductory problems

Problem 1. Prove that the equations a) $2x^2+2xy-y^2=1$, b) $x^2-xy+y^2=2$ have no integer solutions.

Proof. a) Analyzing residues modulo three, we see that the equation

$$2x^2+2xy-y^2=3x^2-(y-x)^2=1$$

has no integer solutions.

b) First solution. Notice that $x^2-xy+y^2=(x-y/2)^2+3/4y^2=2$, hence $y^2\leqslant 8/3$, $|y|\leqslant 1$, analogously for x. From the other hand, at least one of x and y must be even, so it must be zero; if we put $x=0$ then $y^2=2$, we get a contradiction.

Second solution. Clearly, if $|x|\geqslant 3$ or $|y|\geqslant 3$, the equation $x^2-xy+y^2=\frac{1}{2}(x^2+y^2+(x-y)^2)=2$ has no integer solutions. A case-by-case consideration of the remaining 25 possibilities shows that this equation has no integer solutions. □

Problem 2. Prove that each of the equations a) $x^2-2y^2=1$, b) $x^2-3y^2=1$, and c) $x^2-6y^2=1$ has infinitely many integer solutions.

Proof. a) For every integer n the pair

$$x=\frac{(3+2\sqrt{2})^n+(3-2\sqrt{2})^n}{2},\quad y=\frac{(3+2\sqrt{2})^n-(3-2\sqrt{2})^n}{2\sqrt{2}}$$

is a solution of the equation.

b) For every integer n the pair

$$x=\frac{(2+\sqrt{3})^n+(2-\sqrt{3})^n}{2},\quad y=\frac{(2+\sqrt{3})^n-(2-\sqrt{3})^n}{2\sqrt{3}}$$

is a solution of the equation.

c) For every integer n the pair

$$x=\frac{(5+2\sqrt{6})^n+(5-2\sqrt{6})^n}{2},\quad y=\frac{(5+2\sqrt{6})^n-(5-2\sqrt{6})^n}{2\sqrt{6}}$$

is a solution of the equation. □

Problem 3. Prove that the equation $x^2+1000xy+1000y^2=2001$ has infinitely many integer solutions.

Proof. The discriminant $1000^2-4\cdot 1000$ of the equation $x^2+1000xy+1000y^2=2001$ is greater than 0 and is not a perfect square. Hence, the quadratic form $x^2+1000xy+1000y^2=2001$ is indefinite, does not represent 0 and represents 2001 for $x=y=1$. From Problem 46 it follows that the equation

$$x^2+1000xy+1000y^2=2001$$

has infinitely many solutions. □

Problem 4. Fix an odd prime p. Prove that equation $x^2-py^2=-1$ has an integer solution if and only if $p\equiv 1 \pmod 4$.

Proof. Suppose that the equation $x^2-py^2=-1$ has an integer solution. Let us prove that p is equivalent to 1 modulo 4. Indeed, in this case -1 is a quadratic residue modulo p, i.e., $p\equiv 1 \pmod 4$.

Now let us prove the converse, let $p\equiv 1 \pmod 4$. By Problem 46, the equation $x^2-py^2=1$ has a nontrivial solution.

Define by S_+ the set of solutions (x_0,y_0) of the equation $x^2-py^2=1$ such that $x_0,y_0>0$. Let (x_0,y_0) be a solution from S_+ with minimal y_0. Then

$$(x_0-1)(x_0+1)=py_0^2. \tag{1}$$

It follows from (1) that either $2(x_0+1)$ or $2(x_0-1)$ is a perfect square. Consider two cases.

First, assume that $2(x_0+1) = d^2$ for a positive integer d. Then d is even ands $d \mid y_0$. Let $d = 2d_0$, and let

$$x_1 = (x_0+1)/d = d_0,\ y_1 = y_0/d.$$

Then

$$x_1^2 - py_1^2 = \frac{1}{d^2}((x_0+1)^2 - py_0^2) = \frac{2(x_0+1)}{d^2} = 1.$$

Hence, (x_1, y_1) also belongs to S_+. Clearly, $y_1 < y_0$, which contradicts the minimality of the pair (x_0, y_0).

Now consider the second case, let $2(x_0-1) = d^2$ for some positive integer d. Then d is even and $d \mid y_0$. Let $d = 2d_0$, and let

$$x_1 = (x_0-1)/d = d_0,\ y_1 = y_0/d.$$

Then

$$x_1^2 - py_1^2 = \frac{1}{d^2}((x_0-1)^2 - py_0^2) = \frac{2(1-x_0)}{d^2} = -1.$$

We see that (x_1, y_1) is a required solution of $x^2 - py^2 = -1$. □

Problem 5. Prove that for every integer m, the numbers of integer solutions of equations

$$x^2 - xy + y^2 = m \quad \text{and} \quad 3x^2 + 9xy + 7y^2 = m$$

are equal.

Proof. Let us show that there is a bijection between integer solutions of the equation $x^2 - xy + y^2 = m$ and integer solutions of $3x^2 + 9xy + 7y^2 = m$.

Let $v = x + y$, $u = -x - 2y$, clearly, they are integers. Substitute x by $u + 2v$, and y by $-u - v$ in $x^2 - xy + y^2$. We get $3u^2 + 9uv + 7v^2$. So for every solution of $3x^2 + 9xy + 7y^2 = m$ there is a corresponding solution of $x^2 - xy + y^2 = m$.

Conversely, u and v in $u^2 - uv + v^2$ can be replaced by an appropriate integer linear combination of x and y. Hence, for every solution of the equation $x^2 - xy + y^2 = m$ we can produce the solution of the equation $3x^2 + 9xy + 7y^2 = m$. □

Problem 6. Prove that for every integer n the equation $x^2 + y^2 = n$ has an integer solution if and only if it has a rational solution.

Proof. Let x, y be rational numbers such that $x^2 + y^2 = n$. Reduce x and y to a common denominator d and choose the pair (x, y) with the minimal possible d. We assume that $d > 1$ (this means that x, y are not integers and the equation $x^2 + y^2 = n$ has no integer solutions). Let r_x, r_y be the integers closest to x and y, respectively. Denote $s_x := x - r_x$, $s_y := y - r_y$. Then

$$|s_x|,\ |s_y| \leqslant \frac{1}{2}, \quad s_x^2 + s_y^2 = n - (r_x^2 + r_y^2) - 2(s_x r_x + s_y r_y). \tag{2}$$

Let

$$x' = r_x - \frac{s_x(n - r_x^2 - r_y^2)}{s_x^2 + s_y^2}, \qquad y' = r_y - \frac{s_y(n - r_x^2 - r_y^2)}{s_x^2 + s_y^2}.$$

It follows from (2) that $s_x^2 + s_y^2 = d'/d$, and $0 < d' < d$. Hence, if we write x', y' with common denominator d', then it divides d, in particular, it is less than d. Meanwhile $x'^2 + y'^2 = n$. It contradicts the minimality of (x, y). Hence, $d = 1$, i.e., the equation $x^2 + y^2 = n$ has integer solutions. □

Problem 7. Provide an example of a quadratic equation with integer coefficients which has a rational solution but has no integer solutions.

Proof. The equation $4x^2 = 1$ is the required example. It has a rational solution $x = \frac{1}{2}$. Clearly, it has no integer solutions. □

Problem 8. Prove that for every positive integers a and b there exist infinitely many positive integers m such that the equation $ax^2 + by^2 = m$ has no integer solutions.

Proof. Let N be an integer. If the equation $ax^2 + by^2 = n$ has integer solutions for some $n \leqslant N$, then

$$|x| \leqslant \sqrt{\frac{N}{a}}, \quad |y| \leqslant \sqrt{\frac{N}{b}}.$$

If the equation $ax^2 + by^2 = n$ has an integer solution for each $n \leqslant N$, then there exist N pairs (x, y) such that $0 \leqslant x \leqslant \sqrt{\frac{N}{a}}$, $0 \leqslant y \leqslant \sqrt{\frac{N}{b}}$. We obtain

$$N \leqslant \frac{N}{\sqrt{ab}}.$$

Clearly, if $ab > 1$, then this inequality is not held for N great enough. So it remains to consider the case $a = b = 1$. But if n is equivalent to 3 modulo 4, then it cannot be represented in form $x^2 + y^2$, which ends the proof. □

Problem 9. Prove that for every integer m the equation $x^2 + 2y^2 - 3z^2 = m$ has an integer solution.

Proof. It is enough to show that $x^2 + 2y^2 - 3z^2$ represents 0, every odd number and every number equivalent to 2 modulo 4.

If $x = y = z = 1$, then $x^2 + 2y^2 - 3z^2$ equals 0. Hence, $x^2 + 2y^2 - 3z^2$ represents 0.

If $x = u + 1$, $y = u$, $z = u$, then $x^2 + 2y^2 - 3z^2$ equals $2u + 1$. Hence, $x^2 + 2y^2 - 3z^2$ represents all the odd numbers.

If $x = u$, $y = u + 1$, $z = u$, then $x^2 + 2y^2 - 3z^2$ equals $4u + 2$. Hence, $x^2 + 2y^2 - 3z^2$ represents all the numbers equivalent to 2 modulo 4.

If m is divisible by 4, then we factor it out and reduce the problem to one of the already considered cases. □

Quadratic forms

Problem 10. Describe all integers which are represented by forms a) $x^2 + y^2$; b) $x^2 - y^2$; c)* $x^2 + xy + y^2$.

Proof. a) $n = x^2 + y^2$ if and only if in the factorization of n into primes, every prime divisor entering in n in odd power, is equivalent to 1 modulo 4.

b) $(u + 1)^2 - u^2 = 2u + 1$. Hence, $x^2 - y^2$ represents all the odd numbers. Also $(u + 1)^2 - (u - 1)^2 = 4u$.

We see that $x^2 - y^2$ represents all the integers equivalent to 0, 1, and 3 modulo 4. Analyzing this form modulo 4, we see that residue 2 cannot be represented .

c) Let us fix n. Analogously the proof of Problem 6, we can show that the equation $x^2 + xy + y^2 = n$ has integer solutions if and only if it has rational solutions. In rational numbers, $x^2 + xy + y^2$ is linearly equivalent to $x^2 + 3y^2$ ($x^2 + xy + y^2 = (x + \frac{y}{2})^2 + 3(\frac{y}{2})^2$). We show here (read the section about the Hilbert symbol!), that $x^2 + 3y^2$ represents n in rational numbers if and only if every prime entering in n in odd power is equivalent to 0 or 1 modulo 3.

Indeed, $x^2 + 3y^2 = n$ has solutions in $\mathbb{Q}$ if and only if $x_1^2 + 3y_1^2 - nz^2 = 0$ has solutions in $\mathbb{Z}$ with nonzero z. By the Minkowski-Hasse theorem, this equation has solutions if and only if the Hilbert symbol $(n, -3)_p$ equals 1 for every prime p. Let us find it.

Consider $p > 3$. Let $n = p^\alpha \cdot u$, $3 = p^0 \cdot (-3)$. Using the formula for the Hilbert symbol and the quadratic reciprocity law (Serre, Chapter 1, § 3, Theorem 6) we get that

$$(n, -3)_p = \left(\frac{-3}{p}\right)^\alpha = \left(\frac{-1}{p}\right)^\alpha \left(\frac{3}{p}\right)^\alpha = \left(\frac{-1}{p}\right)^\alpha \cdot \left((-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)\right)^\alpha,$$

so it always equals 1 for even α, and for odd α it equals $\left(\frac{p}{3}\right)$, i.e., equals 1 if and only if p has residue 1 modulo 3. So, if the equation

$$x_1^2 + 3y_1^2 - nz^2 = 0$$

has solutions modulo p, for p of the form $3k + 2$, then p enters in pair degree into the decomposition of n into primes.

The case $p = 2$ is let to the reader.

Consider $p = 3$. Let $n = 3^\alpha \cdot u$, here $\beta = 1$, $v = -1$. We have:

$$(n, -3)_3 = (-1)^\alpha \left(\frac{u}{3}\right) \left(\frac{-1}{3}\right)^\alpha = \left(\frac{u}{3}\right).$$

This expression equals 1 if and only if u has residue 1 modulo 3. But we have already checked that all the prime divisors of the form $3k + 2$ enter in even degree, so this condition gives nothing new. □

Definition 1. Two quadratic forms are called *equivalent* if they represent the same set of numbers.

Problem 11. Prove that the quadratic forms

$$f(x, y), \qquad f(x - y, y), \qquad f(x, y - x), \qquad f(-x, y), \qquad f(x, -y) \tag{3}$$

are equivalent.

Proof. If m is represented by the form $f(x, y)$ for $x = x_0$, $y = y_0$, then m can be represented by the form $f(x - y, y)$ for $x = x_0 + y_0$, $y = y_0$, by the form $f(x, y - x)$ for $x = x_0$, $y = y_0 + x_0$, by the form $f(-x, y)$ for $x = -x_0$, $y = y_0$, by the form $f(x, -y)$ for $x = x_0$, $y = -y_0$. Hence, every integer which can be represented by the form $f(x, y)$ can also be represented by any other form from the list (3). One can analogously prove that every integer represented by one of these forms can be represented also by any other form from the list (3). We obtain that all the forms (3) are equivalent. □

Problem 12. a) Prove that the forms $x^2 + y^2$ and $x^2 + xy + y^2$ are not equivalent.

b) Prove that the form $4x^2 - 6xy + 5y^2$ is not equivalent to any form $ax^2 + by^2$ with integer a and b.

Proof. a) The form $x^2 + y^2$ represents 2, while $x^2 + xy + y^2$ not. Hence, they are not equivalent.

b) The form $4x^2 - 6xy + 5y^2$ has a unique well, and the values around it equal 3, 4, and 5. Hence, 3, 4, and 5 are three minimal values of the form $4x^2 - 6xy + 5y^2$.

Let $a, b \geqslant 0$. Then three minimal values of the form $ax^2 + by^2$ can be the following sets of numbers:

$$\{a,\ b,\ a + b\}, \quad \{a,\ 2a,\ b\}, \quad \{a,\ b,\ 2b\}, \quad \{a,\ 2a,\ 4a\}, \quad \{b,\ 2b,\ 4b\}. \tag{4}$$

Clearly, we cannot find a and b to represent the set $\{3, 4, 5\}$ in any of forms (4).

We conclude that there do not exist nonnegative integers a and b such that the form $4x^2 - 6xy + 5y^2$ is equivalent to $ax^2 + by^2$. □

Problem 13. Provide an example of a non-negative definite form which is not positive definite.

Proof. Example: $f(x, y) = x^2$. □

Extended arithmetics: p-adic numbers

Problem 14. Let m and n be square-free integers. Assume that the equation

$$z^2 - mx^2 - ny^2 = 0 \tag{5}$$

has a nontrivial rational solution. Prove that

a) either m or n is positive,

b) m is a quadratic residue modulo n,

c) n is a quadratic residue modulo m.

Proof. We fix a nonzero rational solution (x_0, y_0, z_0) of equation (5). Let us assume that x_0, y_0, z_0 have no common divisor greater than 1.

a) If $m, n \leqslant 0$, then $x_0^2 - my_0^2 - nz_0^2 \geqslant 0$, and the equality can be obtained only for $x_0 = y_0 = z_0 = 0$. We get a contradiction.

b) It is enough to show that for every prime divisor p of m, the integer n is a quadratic residue modulo p.

Fix a prime divisor p of m. If $n \vdots p$, then there is nothing to prove. Now let $n \not\vdots p$. Consider two cases: $y_0 \vdots p$ and $y_0 \not\vdots p$.

First let $y_0 \vdots p$. Then x_0 and z_0 are also divisible by p, which contradicts our assumption that

$$\gcd(x_0, y_0, z_0) = 1.$$

Hence, $y_0 \not\vdots p$. Then the following equivalence is true modulo p:

$$n \equiv (z/y)^2 \pmod{p},$$

which ends the proof of b).

The proof of c) is analogous. □

Problem 15. Reduce Metatheorem for the equations in two variables to the case of equations of the form (5).

Proof. Every quadratic equation has form

$$f(X_1, X_2) = f_2(X_1, X_2) + f_1(X_1, X_2) + f_0 = 0,$$

where f_2 is a homogeneous polynomial of degree 2, f_1 of degree 1, f_0 is a constant.

First let us prove a general statement: either both

$$f(X_1, X_2) = 0 \text{ and } f(X_1 + cX_2 + t, X_2) = 0$$

have rational solutions, or have no rational solutions for all the pairs of rational numbers (c, t). We leave the proof of this fact as an exercise.

Clearly, the following changes of variables

$$f(X_1, X_2) \to f(X_1 + cX_2, X_2) \tag{6}$$

change f_1 and f_2 independently and preserve f_0.

Let us present f_2 in the form

$$c_1X_1^2 + c_{12}X_1X_2 + c_2X_2^2,$$

where c_1, c_2, and c_{12} are parameters.

If $f_2 \neq 0$, then we can perform several changes of the form (6) and assume that $c_1 \neq 0$.

Consider the function

$$f(X_1 - \frac{c_{12}}{2c_1}X_2, X_2). \tag{7}$$

It is easy to see that (7) has form

$$c_1X_1^2 + c_2'X_2^2$$

for some rational number c_2'. Hence, we may assume that

$$f_2(X_1, X_2) = c_1X_1^2 + c_2X_2^2$$

for some rational numbers c_1, c_2. If $c_2 = 0$, but $c_1 \neq 0$, then the equation $f = 0$ can be written as

$$c_1X_1^2 = -rX_2 - f_0$$

which can be easily solved. So from now on we assume that $c_1 \neq 0$. Analogously, we may assume that $c_2 \neq 0$.

The linear part $f_1(X_1, X_2)$ has the form $r_1X_1 + r_2X_2$. Consider the following change of variables:

$$f(X_1, X_2) \to f\left(X_1 - \frac{r_1}{2c_1}, X_2 - \frac{r_2}{2c_2}\right).$$

If now we expand the function $f(X_1 - \frac{r_1}{2c_1}, X_2 - \frac{r_2}{2c_2})$, we obtain that its linear part f_1 equals 0. Now the equation $f = 0$ takes the form

$$c_1X_1^2 + c_2X_2^2 + f_0 = 0.$$

This equation is equivalent to a homogeneous equation

$$z^2 + \frac{c_2}{c_1}y^2 + \frac{f_0}{c_1}z^2 = 0.$$

This ends the proof. □

Problem 16. Let f be a polynomial with integer coefficients. Prove that the equation $f = 0$ has a solution in $\mathbb{Z}_p$ if and only if it has a solution modulo p^n for every positive integer n.

Proof. Let $x_1, \ldots, x_n, \ldots$ be the solution of the equation $f = 0$ in $\mathbb{Z}_p$. Then for every n the residue of x_n modulo p^n is a solution of the equivalence modulo p^n. In particular, $f \equiv 0$ has a solution modulo p^n for every positive integer n.

Now prove the other implication. Suppose that the equation $f \equiv 0$ has a solution modulo p^m for every positive integer m. For every m, we denote by S_m the set of solutions of the equation $f \equiv 0$ modulo p^m. By our assumption, S_m is non-empty for every $m \geqslant 0$.

Since every residue modulo p^{m+1} can be treated as a residue modulo p^m, we have a projection $S_{m+1} \to S_m$. Let us denote by S_m^∞ the intersection of images of S_{m+k} for all $k \geqslant 0$. Since $S_{m+k} \neq 0$, the set $S_m^\infty \neq 0$. For every $s_m \in S_m^\infty$ there exists a $s_{m+1} \in S_{m+1}^\infty$ such that s_m is the image of s_{m+1} with respect to the projection defined above. Proceeding in such a way, we can construct an infinite chain

$$s_1, \ldots, s_m, \ldots, \tag{8}$$

where s_m is a set containing n residues modulo p^m and s_m is the projection of s_{m+1} to the residues modulo p^m. The sequence (8) defines the unique set of n p-adic integers $x_1, \ldots, x_n$, having the prescribed sets of residues $s_1, \ldots, s_m, \ldots$ modulo $p, \ldots, p^m, \ldots$.

The numbers $x_1, \ldots, x_n$ are the solutions of the equation $f = 0$. □

Problem 17. When is a p-adic number in the form (2) equal to 0?

Proof. The answer follows from the definition: If $a_{-k} + \ldots + a_{-k+i}p^i \equiv 0 \,(\mathrm{mod}\ p^{i+1})\ \ \forall i$. □

Problem 18. Prove that the product of two nonzero p-adic numbers is also nonzero.

Proof. Consider two non-zero p-adic numbers a, b. We assume without loss of generality that $a, b \in \mathbb{Z}_p$ and $a, b \not\equiv 0 (\mathrm{mod}\ p)$. But it means that $ab \not\equiv 0 (\mathrm{mod}\ p)$, hence, $ab \neq 0$. □

Problem 19. Prove that $\mathbb{Q} \subset \mathbb{Q}_p$ for any prime p (i.e., prove that for every pair of nonzero integers m and n there exists a p-adic number x such that $nx = m$).

Proof. Without loss of generality we may assume that m, n are coprime with p. But now the statement of Problem 16 follows from Problem 20. □

Problem 20. Prove that -1 is a square in $\mathbb{Q}_p$ if and only if $p \equiv 1 \pmod 4$.

Proof. It follows from Problem 21. □

Problem 21. Find a description of all perfect squares in $\mathbb{Q}_p$.

Proof. We consider two cases $p = 2$ and $p \neq 2$ separately.

First consider $p = 2$. Every 2-adic number x can be represented as $2^n(2m + 1)$, where n is an integer, and m is an integer 2-adic number. We have $x^2 = 2^{2n}(1 + 8\frac{m(m+1)}{2})$. Let $m' = \frac{m(m+1)}{2}$. Then

$$x^2 = 2^{2n}(1 + 8m'), \tag{9}$$

where m' is a 2-adic integer.

Let us prove that every 2-adic integer of the form (9) is a perfect square in 2-adic numbers. It is sufficient to show that every 2-adic integer m' can be represented in the form $\frac{m(m+1)}{2}$.

By Problem 16, is is enough to show that the equivalence $x(x + 1) \equiv 2m'$ has solutions in $\mathbb{Z}$ for every $i \in \mathbb{Z}_{\geqslant 0}$. We will prove this by induction.

Base $i = 1$ is true.

The step of the induction: $i \to i + 1$. Let $m_i \in \mathbb{Z}$ be a solution of the equation $x(x + 1) \equiv 2m' (\mathrm{mod}\ 2^i)$. There are two possibilities:

1) $m_i(m_i + 1) \equiv 2m' \pmod{2^{i+1}}$,

2) $m_i(m_i + 1) \equiv 2m' + 2^i \pmod{2^{i+1}}$.

In Case 1), m_i is also the solution of the equation $x(x + 1) \equiv 2m' \pmod{2^{i+1}}$. In Case 2), $m_i + 2^i$ is the solution of the equation $x(x + 1) \equiv 2m' \pmod{2^{i+1}}$.

Now let $p \neq 2$, i.e., p is an odd prime. Every p-adic number x can be represented in the form $p^n m$, where n is an integer and m is a p-adic integer which is not divisible by p. We have $x^2 = p^{2n} m^2$. Let $m' = m^2$. Then

$$x^2 = p^{2n} m', \tag{10}$$

where m' is a p-adic integer such that its residue modulo p is a nonzero quadratic residue.

Let us prove that every p-adic number of the form (9) is a perfect square in p-adic numbers. It is enough to show that every p-adic integer m' such that

3) m' is not divisible by p,

4) the residue of m' modulo p is a nonzero quadratic residue,

can be represented in the form m^2.

Using Problem 16, it is enough to prove that the equation $x^2 \equiv m' \pmod{p^i}$ has solutions in $\mathbb{Z}$ for every $i \in \mathbb{Z}_{\geqslant 0}$. We prove this statement by induction.

Base $i = 1$ is fulfilled since the residue of m' modulo p is a quadratic residue.

Step: $i \to i + 1$. Let $m_i \in \mathbb{Z}$ be the solution of the equation $x^2 \equiv m' \pmod{p^i}$. Then

$$m_{i+1}^2 \equiv m' + rp^i \pmod{p^{i+1}},$$

for some $r \in \mathbb{Z}$. Since m' is not divisible by p and $p \neq 2$, there exists a $r' \in \mathbb{Z}$ such that $2m_i r' \equiv r \pmod{p^{i+1}}$. Let $m_{i+1} := m_i - r'p^i$. Then $m_{i+1}^2 \equiv m' \pmod{p^{i+1}}$, which ends the proof of the induction step. □

Problem 22. Prove that for any nonzero 3-adic number m there exists a 3-adic number x such that m is equal to one of the numbers x^2, $2x^2$, $3x^2$, or $6x^2$.

Proof. Note that for every p, any p-adic number can be represented in the form $p^i \cdot a \cdot y$, where a is an integer from 1 to $p-1$, p^i is a power of p, and y is a p-adic integer, equivalent to 1 modulo p (by Problem 21, it is a perfect square). In our case $p = 3$, and we obtain that, depending on parity of i, p^i is either a perfect square or 3 times a perfect square, $a \in \{1,\ 2\}$, and y is a perfect square. Clearly, their product has the required form. □

Problem 23. Let p be an odd prime, and let $x_1, \ldots, x_5$ be nonzero p-adic numbers. Prove that there exist indices i and j with $1 \leqslant i < j \leqslant 5$ such that x_i/x_j is a perfect square in $\mathbb{Q}_p$.

Proof. As in the proof of the previous problem, every p-adic number has the form $p^i \cdot a \cdot y$. Divide the given numbers into 2 groups: in the first group i is even and in the second odd. Now divide each group into two smaller groups depending on whether a is a quadratic residue or not. By pigeonhole principle, since we have 5 numbers and 4 groups, there are two numbers in the same group. Their ratio has the form

$$p^j \cdot a_{new} \cdot \frac{y_1}{y_2},$$

where j is even, a_{new} is a quadratic residue (since it is the ratio of either two quadratic residues or two quadratic non-residues), and $\frac{y_1}{y_2}$ is a p-adic number starting with 1. So this ratio is a perfect square as a product of three perfect squares. □

Problem 24. Prove that for every odd prime p there exist p-adic numbers $x_1, \ldots, x_{p-1}$ such that $x_1^2 + \ldots + x_{p-1}^2 + 1 = 0$.

Proof. By Problem 21, $1-p$ is a perfect square in p-adic numbers. Hence, $-1 = 1+1\ldots+1$ ($p-2$ ones)$+1-p$ is a sum of $(p-1)$ perfect squares in p-adic numbers. □

Problem 25. Prove that the equation $x^2 + x + 1 = 0$ has exactly two solutions in $\mathbb{Z}_7$.

Proof. The solutions of the $x^2+x+1 = 0$ can be found with the help of the standard formula $x_{1,2} = \frac{-1 \pm \sqrt{-3}}{2}$. Since $\sqrt{-3} \in \mathbb{Z}_7$ (see Problem 21), the equation $x^2 + x + 1 = 0$ has two distinct solutions in $\mathbb{Z}_7$. □

Problem 26. Prove that the equation $x^2 + y^2 = -1$ has a p-adic solution for every odd prime p.

Proof. First solution. It is enough to show that this equation can be solved modulo p. Indeed, x^2 can take $(p+1)/2$ different values: zero and all the quadratic residues. Now write down the list of all the values of $-x^2-1$. If any of them has the form y^2, we are done. But if no one of them has the form y^2, then there are at most $(p-1)/2$ possible values for y^2, a contradiction.

Second solution. It is enough to show that this equation can be solved modulo p. Every quadratic residue can be represented as x^2+y^2. If only quadratic residues can be represented in the form x^2+y^2, then for every i we show by induction that only quadratic residues can be represented in the form $x_1^2+\ldots+x_i^2$. But by Problem 24 every residue modulo p can be represented in the form $x_1^2+\ldots+x_{p-1}^2$. Hence, x^2+y^2 represents also quadratic non-residues. It means that x^2+y^2 represents all the elements of $\mathbb{Z}/p$, in particular, -1. □

Problem 27. Prove the Hasse–Minkowski principle for equations in one and two variables.

Proof. A) Equations in one variable. Any such equation has the form $ax^2=b$. It is enough to show that if it has no solutions in $\mathbb{Q}$, then either it has no solutions in $\mathbb{R}$, or it has no solutions in $\mathbb{Q}_p$ for some p. If $ax^2=b$ has no solutions in $\mathbb{Q}$, then b/a is not a perfect square in $\mathbb{Q}$, i.e., either $b/a<0$, or there exists a prime number p which enters in b/a in odd power. In the first case $ax^2=b$ has no solutions in $\mathbb{R}$, in the second in $\mathbb{Q}_p$.

B) Equations in two variables. By Problem 15, every equation (of degree two!) in two variables in rational numbers is equivalent to the equation $ax^2+by^2=1$. We may assume that:

1) the coefficients a, b are square-free integers,

2) $|a|\leqslant|b|$.

It is enough to show that if the equation $ax^2+by^2=1$ has a solution in $\mathbb{Q}_p$ for every p and in $\mathbb{R}$, then it has solutions in $\mathbb{Q}$. Let $m(a,b):=|a|+|b|$. We prove this statement by induction on $m(a,b)$.

Base $m(a,b)=2$ can be verified directly.

Step: $m\to m+1$. Let a, b be some integers verifying the conditions 1), 2) and such that

• $m(a,b)=m+1$

• the equation $ax^2+by^2=1$ has solutions in p-adic numbers for every p and has a solution in $\mathbb{R}$.

Consider two cases: $|a|=|b|$ and $|a|<|b|$. If $|a|=|b|$, then the equation $ax^2+by^2=1$ is equivalent to the equation

$$-(b/a)y^2+az^2=1. \tag{11}$$

Moreover, the equation (11) has solutions in $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{Q}_p$, if and only if the equation $ax^2+by^2=1$ has solutions in the same set. Since $m(-\frac{b}{a},a)<m(a,b)=m+1$, the equation $-(b/a)y^2+az^2=1$ has solutions in $\mathbb{Q}$ by the induction assumption. Hence, the initial equation has solutions in $\mathbb{Q}$.

Now let $|a|<|b|$. It follows from the condition • that a is a perfect square modulo b, i.e.,

$$a+bb'=t^2,$$

where b', t are some integers and $b'\geqslant 0$. We assume without loss of generality that

$$|t|\leqslant\frac{|b|}{2}.$$

The equation $ax^2+by^2=1$ has solutions in $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{Q}_p$ if and only if the equation

$$ax^2+b'y^2=1, \qquad b'=\frac{t^2-a}{b}$$

has solutions in the same set. We have $|b'|\leqslant\frac{|b|}{4}$ and $m(a,b')<m(a,b)=m+1$. Since $m(a,b')\leqslant m$, the equation $ax^2+b'y^2=1$ has solutions in $\mathbb{Q}$ by the induction hypothesis. Hence, the initial equation also has solutions in $\mathbb{Q}$. □

Problem 28. Prove the following properties of the Hilbert symbol:

1) $(a,b)_p=(b,a)_p$,

2) $(a,c^2)_p=1$,

3) $(a,-a)_p=1$, $\quad(a,1-a)_p=1$,

4) $(a,b)_p=(a,-ab)_p=(a,(1-a)b)_p$.

Proof. 1) Obvious from the definition.
2) The equation $z^2 - ax^2 - c^2y^2 = 0$ has a nonzero solution $z = c, x = 0, y = 1$.
3) The equation $z^2 - ax^2 + ay^2 = 0$ has a nonzero solution $z = 0, x = y = 1$.
The equation $z^2 - ax^2 - (1-a)y^2 = 0$ has a nonzero solution $x = y = z = 1$.
4) Using Problem 29, one can deduce it from 3). □

Problem 29. Let $(a, b)_p = 1$. Show that $(a', b)_p = (aa', b)_p$ for any a'.

Proof. Let b be a perfect square. Then $(a, b)_p = (aa', b)_p = 1$.
Now suppose that b is not a perfect square. We need the following lemma.

Lemma 1. If
- b is not a perfect square,
- $(a, b)_p = 1$ and $(a', b)_p = 1$,

then $(aa', b) = 1$.

Finish the proof of Problem 29 using Lemma 1. If $(a', b)_p = 1$, then by Lemma 1 we have $(aa', b)_p = 1$. If $(aa', b)_p = 1$, then by Lemma 1 $(a', b)_p = (a^2a', b)_p = 1$. Hence, if one of the numbers $(aa', b)_p$ and $(a', b)_p$ equals 1, then the second one either equals 1. Hence, they are equal.

Proof of Lemma 1. Let (x_0, y_0, z_0) be a nonzero solution of the equation $z_0^2 - ax_0^2 - by_0^2 = 0$. Since b is not a perfect square in $\mathbb{Q}_p$, $x_0 \neq 0$. So we may assume that $x_0 = 1$ and $a = z_0^2 - by_0^2$. By the similar reasoning, there exist z_1, y_1 such that $a' = z_1^2 - by_1^2$. Then

$$aa' = (z_0z_1 - by_0y_1)^2 - b(z_0y_1 + z_1y_0)^2.$$

Hence, $(aa', b) = 1$. □

□

To write down an expression for the Hilbert symbol in a compact form, we will use the *Legendre symbol* $\left(\frac{x}{p}\right)$ defined for any integer x and prime p. It equals to 1, -1, or 0 depending on whether x is a nonzero quadratic residue, a quadratic non-residue, or zero.

Problem 30. Let p be an odd prime; let $a = p^\alpha u$, $b = p^\beta v$, where α, β, u, v are integers such that u and v are not divisible by p. Prove that

$$(a, b)_p = (-1)^{\alpha\beta\cdot\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha,$$

where $\varepsilon(p) = \frac{p-1}{2}$.

Proof. The proof of this fact can be found in the book "A course in arithmetic" by J.-P. Serre, Chapter 3, § 1, Theorem 1. □

Problem 31. Find an explicit formula for $(a, b)_2$ for every nonzero integers a and b.

Proof. Let $a = 2^\alpha u$, $b = 2^\beta v$, where α, β, u, v are integers such that u and v are odd. The Hilbert symbol $(a, b)_2$ is given by the formula

$$(-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)},$$

where $\varepsilon(u) = \frac{u-1}{2}$, and $\omega(u) = \frac{u^2-1}{8}$. The proof of this fact can be found in the book "A course in arithmetic" by J.-P. Serre, Chapter 3, § 1, Theorem 1. □

Problem 32. Prove that $(a, b)_p(a, b')_p = (a, bb')_p$ for every nonzero integers a, b, b'.

Proof. The proof of this fact can be found in the book "A course in arithmetic" by J.-P. Serre, Chapter 3, § 1, Theorem 2. □

Problem 33. Prove that the equation $ax^2 + by^2 = c$ in variables x and y (with parameters a, b, and c) has a solution in p-adic numbers if and only if $(c, -ab)_p = (a, b)_p$.

Proof. If the equation $ax^2 + by^2 = c$ has a solution, then the equation

$$z^2 - \frac{a}{c}x^2 - \frac{b}{c}y^2 = 0$$

also has a solution. By definition, this means that $(a/c, b/c)_p = 1$. We can re-write it as follows.

$$1 = (a/c, b/c)_p = (a, b)_p(a, c)_p(b, c)_p(c, c)_p = (a, b)_p(ab, c)_p(c, -1)_p. \tag{12}$$

So $(a, b)_p = (c, -ab)_p$.

Now let $(a, b)_p = (c, -ab)_p$ and show that the equation $ax^2 + by^2 = c$ has a non-zero solution. It follows from (12) that $(a/c, b/c)_p = 1$. Hence, the equation $z^2 - \frac{a}{c}x^2 - \frac{a}{b}y^2 = 0$ has a solution. Let us denote by (x_0, y_0, z_0) one of its solutions. If $z_0 \neq 0$, then $(\frac{x_0}{z_0}, \frac{y_0}{z_0})$ is a solution of the equation $ax^2 + by^2 = c$.

We have solved the problem if $z_0 \neq 0$. Now we assume that $z_0 = 0$. For any r_x, r_y consider the equation

$$a(tx_0 + r_x)^2 + b(ty_0 + r_y)^2 = c.$$

It is equivalent to the equation

$$(ar_x^2 + br_y^2) + 2t(ax_0r_y + by_0r_x) = c. \tag{13}$$

For a generic pair of rational numbers (r_x, r_y), we see that $(ax_0r_y + by_0r_x) \neq 0$ and $t_0 = \frac{c-(ar_x^2+br_y^2)}{2(ax_0r_y+by_0r_x)}$ is a solution of the equation (13). Hence, the equation $ax^2 + by^2 = c$ has infinitely many rational solutions. □

Using the properties of the Hilbert symbol, solve the following problem.

Problem 34*. Let us fix a homogeneous polynomial $f = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$ with $n \geqslant 2$, where $a_1, \ldots, a_n \neq 0$. Set

$$d = a_1a_2 \ldots a_n \quad \text{and} \quad \varepsilon = \prod_{i<j}(a_i, a_j)_p. \tag{14}$$

Prove that the equation $f = 0$ has a nonzero p-adic solution if and only if one of the following conditions is satisfied:

1) $n = 2$ and $-d$ is a square in $\mathbb{Q}_p$;
2) $n = 3$ and $(-1, d)_p = \varepsilon$;
3) $n = 4$ and $d \neq \alpha^2$, or $d = \alpha^2$ and $\varepsilon = (-1, -1)_p$;
4) $n \geqslant 5$. (i.e., if f depends on 5 or more variables, then $f = 0$ has a nonzero solution in $\mathbb{Q}_p$ for any p.)

Proof. The proof of this fact can be found in the book "A course in arithmetic" by J.-P. Serre, Chapter 4, § 2, Theorem 6. □

Deduce the following problem from problem 34.

Problem 35. Fix a homogeneous polynomial $f = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$, where $a_1, \ldots, a_n \neq 0$, and an integer $a \neq 0$. Define d, ε by formula (14). Then the equation $f = a$ has a p-adic solution if and only if one of the following conditions is satisfied:

1) $n = 1$ and a/d is a square in $\mathbb{Q}_p$;
2) $n = 2$ and $(a, -d)_p = \varepsilon$;
3) $n = 3$ and ad is not a perfect square in $\mathbb{Q}_p$, or ad is a perfect square and $\varepsilon = (-1, -d)_p$;
4) $n \geqslant 4$. (i.e., if f depends on 4 or more variables, then the equation $f = a$ has a nonzero solution in $\mathbb{Q}_p$ for any p.)

Proof. 1) $a_1x_1^2 = a \Leftrightarrow x_1^2 = \frac{a}{a_1}$. Obviously, it has solutions in p-adic numbers if and only if $\frac{a}{a_1}$ is a perfect square in $\mathbb{Q}_p$.

2) $a_1x_1^2 + a_2x_2^2 = a$. The condition $(a, -d)_p = \varepsilon$ is equivalent to $(a, -a_1a_2)_p = (a_1, a_2)$ which is just Problem 33 for $a = a_1$, $b = a_2$, $c = a$.

3) We are solving the equation $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 - a = 0$. Obviously, it is equivalent to the equation $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 - ax_4^2 = 0$ because of transformation

$$(x_1, x_2, x_3, x_4) \leftrightsquigarrow (\frac{x_1}{x_4}\frac{x_2}{x_4}\frac{x_3}{x_4}, 1),$$

which is solvable in p-adic numbers.

Now we prove that if there is a nontrivial solution with $x_4 = 0$, then there exists a nontrivial solution with $x_4 \neq 0$. Without loss of generality $x_1 \neq 0$. Let (C, D) be a solution of the equation $C^2 - D^2 = -\frac{a}{a_1}$ (for example, $C = \frac{1-a/a_1}{2}$, $D = \frac{-1-a/a_1}{2}$)).

Obviously, we can multiply our solution to $\frac{C}{x1}$, and we get $(C,\ x_2,\ x_3,\ 0)$. It is easy to check that

$$f(C, x_2, x_3, 0) = f(D, x_2, x_3, 1),$$

so we reduced this problem to Problem 34c.

First case: $ad \neq -m^2$ in $\mathbb{Q}_p$. It is equivalent to $d \neq m^2$.

Second case: $ad = -m^2$.

We need: $(a_1, a_2)_p(a_1, a_3)_p(a_2, a_3)_p = (-1, -a_1a_2a_3)_p \Leftrightarrow (a_1, a_2)_p(a_1, a_3)_p(a_2, a_3)_p(-a, d) = (-1, -1)_p$.

Obviously, if we have a problem like $a = b \Leftrightarrow c = d$ where (a, b, c, d) from $\{1, -1\}$, then we need to prove $ac = bd$, so we need

$$(-a, d)_p = (-1, -d)_p(-1, -1)_p \quad \Leftrightarrow \quad (-a, d)_p = (-1, -1)_p(-1, -1)_p(-1, d)_p \quad \Leftrightarrow$$
$$\Leftrightarrow \quad (-a, d)_p = (-1, d)_p \quad \Leftrightarrow \quad (-1, d)_p(-a, d)_p = 1 \quad \Leftrightarrow \quad (a, d)_p = 1 \quad \Leftrightarrow$$
$$\Leftrightarrow \quad (a, a)_p(a, \frac{d}{a})_p = 1 \quad \Leftrightarrow \quad 1 \cdot 1 = 1,$$

because $\frac{d}{a}$ is a perfect square in $\mathbb{Q}_p$.

4) As in 3), we only need to solve the equation

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 - ax_5^2 = 0.$$

But by Problem 34d this equation is always solvable.

Also, the proof of this fact can be found in the book "A course in arithmetic" by J.-P. Serre, Chapter 4, § 2, Corollary of Theorem 6. □

Problem 36. Prove the Hasse–Minkowski principle.

Proof. The proof of this fact can be found in the book "A course in arithmetic" by J.-P. Serre, Chapter 4, § 3, Theorem 8. □

Problem 37. Using problem 35 and the Hasse–Minkowski principle, show that an integer d is a sum of 3 squares in rational numbers if and only if the number d cannot be represented in the form $4^a(8b - 1)$, i.e. if $-d$ is not a perfect square in $\mathbb{Q}_2$.

Proof. By the Hasse-Minkowski principle, we only need to consider whether the equation $x^2 + y^2 + z^2 = n$ has a p-adic solution or not. We work in terms of Problem 35. $a_1 = a_2 = a_3 = 1$, $d = 1$, $\varepsilon = (1, 1)_p^3 = (1, 1)_p$, $a = n$. First, we prove that if $p > 2$, then it is solvable in p-adic numbers.

If n is not a $-m^2$ then we are done. If $n = -m^2$ then $\varepsilon = (1, 1)_p = [Problem30] = 1 = [Problem30] = (-1, -1)_p$, so a solution exists.

It remains to consider the case $p = 2$. If $n \neq -m^2$ then we are done. Now let $n = -m^2$. If a solution exists, then

$$\varepsilon = (1, 1)_2 = (-1, -1)_2,$$

which leads to a contradiction by Problem 31. □

Problem 38. Fix an integer n. Prove that if there exist rational numbers x, y, and z such that $x^2+y^2+z^2 = n$, then there also exist integers x', y', and z' such that $(x')^2 + (y')^2 + (z')^2 = n$. Deduce the Gauss theorem from this statement.

Proof. Let rational numbers x, y, z be such that $x^2 + y^2 + z^2 = n$. Denote by d the common denominator of x, y, z. Choose a triple (x, y, z) with the minimal value of d. Let us assume that $d > 1$ (i.e., that one of x, y, and z is not integer and that the equation $x^2 + y^2 + z^2 = n$ has no integer solutions). Let r_x, r_y, r_z be the integers closest to x, y, z, and let $s_x := x - r_x$, $s_y := y - r_y$, $s_z := z - r_z$. Then

$$|s_x|, |s_y|, |s_z| \leqslant \frac{1}{2}, \qquad s_x^2 + s_y^2 + s_z^2 = n - (r_x^2 + r_y^2 + r_z^2) - 2(s_xr_x + s_yr_y + s_zr_z). \tag{15}$$

Let

$$x' = r_x - \frac{s_x(n - r_x^2 - r_y^2 - r_z^2)}{s_x^2 + s_y^2 + s_z^2}, \qquad y' = r_y - \frac{s_y(n - r_x^2 - r_y^2 - r_z^2)}{s_x^2 + s_y^2 + s_z^2}, \qquad z' = r_z - \frac{s_z(n - r_x^2 - r_y^2 - r_z^2)}{s_x^2 + s_y^2 + s_z^2}.$$

It follows from (15) that $s_x^2 + s_y^2 + s_z^2 = d'/d$, and moreover $0 < d' < d$. It means that the least common denominator of x', y', z' divides d', i.e., is less than d. Notice that $x'^2 + y'^2 + z'^2 = n$. We get a contradiction. Hence, $d = 1$, and the equation $x^2 + y^2 + z^2 = n$ has integer solutions.

By Problem 37, every positive integer N which does not have the form $4^n(8m - 1)$ is a sum of three squares of rational numbers. But we proved above that in this case N is also a sum of three squares of integers. □

Problem 39. Deduce the Legendre theorem from the Gauss theorem.

Proof. It follows from the Gauss theorem that every positive integer, equivalent to 1, 2, 3, 5, or 6 modulo 8, can be represented as a sum of three (and, consequently, of four) perfect squares. It remains to show that every integer which is equivalent to 0, 4, or 7 modulo 8, can be represented as a sum of 4 perfect squares.

If n can be represented as a sum of four squares, then $4n$ either. So it is enough to consider the case $n \equiv 7 \mod 8$.

Fix n, $n \equiv 7 \mod 8$. Since $n - 1$ is equivalent to 6 modulo 8, by Gauss theorem $n - 1$ can be represented as a sum of three squares. Hence, n can be represented as a sum of four squares. □

Some properties of the Hilbert symbol (DE-2)

The goal of this section is to show that, for a pair of nonzero integers (a, b), the Hilbert symbol $(a, b)_p$ equals 1 for almost all (=all except finite number) primes p. We deduce this statement from a more general statement presented below.

Problem 40. a) Let f be a homogeneous polynomial of degree n, depending on k variables, where $k > n$. Then the number of solutions of the equivalence $f \equiv 0$ (including 0-solution!) modulo p is divisible by p (Hint: apply the little Fermat theorem and consider case $p = 2$).

b) Let f be a polynomial of degree n depending on k variables, where $k > n$. Then the number of solutions of the equivalence $f \equiv 0$ modulo p is divisible by p.

Proof. Obviously, case b) is a generalization of case a). We prove here b). Consider a polynomial $f(x_1, \ldots, x_k)$ of degree n. Consider the following sum:

$$\sum_{x_1, \ldots, x_n} f(x_1, \ldots, x_n)^{p-1}, \tag{16}$$

where $x_1, \ldots, x_n$ run all the residues modulo p. Note that every element of the sum (16) equals 0 or 1 modulo p. The key idea is that the residue modulo p of the number of solutions of the equation $f(x_1, \ldots, x_k) \equiv 0$ equals (16) modulo p. But the degree of the polynomial $f(x_1, \ldots, x_k)^{p-1}$ is $(p - 1)n$. Since we have $k > n$ variables, for every monomial of $f(x_1, \ldots, x_k)^{p-1}$ there exists a variable entering in this monomial in degree less than $p - 1$. But for such a monomial, the summation in (16) gives 0, because

$$\sum_{x_i} x_i^l \equiv 0 \pmod{p}$$

for all $l < p - 1$. Hence, the sum in (16) is equivalent to 0 (mod p), and the number of solutions of the equation $f(x_1, \ldots, x_n) = 0$ has residue 0 modulo p. □

Problem 41. Deduce from the previous problem that for any integers a, b, c the equivalence $ax^2 + by^2 + cz^2 \equiv 0$ in variables x, y, z has a nonzero solution modulo p .

Proof. The polynomial $ax^2 + by^2 + cz^2$ has degree 2 and depends on three variables. Hence, the number of solutions of the equation $ax^2 + by^2 + cz^2 \equiv 0$ has residue 0 modulo p. In particular, this means that the equation $ax^2 + by^2 + cz^2 \equiv 0$ has a nonzero solution. □

Problem 42. Deduce from the previous problem that, for a pair of nonzero integers (a, b) and an odd prime p, $(a, b)_p = 1$ if $a, b \not\vdots p$. Explain why $(a, b)_p = 1$ for all primes p except a finite number.

Proof. Let us fix $p \neq 2$ and relatively prime with a and b. We prove that $(a, b)_p = 1$.

Let (x_0, y_0, z_0) be a solution of the equation $z^2 - ax^2 - by^2 \equiv 0 \pmod p$ such that

$$(x_0, y_0, z_0) \not\equiv (0, 0, 0) \pmod p$$

(by Problem 41, such a solution exist). We assume without loss of generality that $z_0 \not\equiv 0 (\mathrm{mod}\ p)$. Then by Problem 21 the value $ax_0^2 + by_0^2$ is a perfect square in p-adic numbers, hence, the equation $z^2 - ax^2 - by^2 = 0$ has a nonzero solution in p-adic numbers, i.e., $(a, b)_p = 1$. □

Problem 43. Deduce from Problem 41 that the equation $ax^2 + by^2 + cz^2 + dv^2 + ew^2 = 0$ in variables x, y, z, v, w (a, b, c, d, e are parameters) has a nonzero solution in $\mathbb{Q}_p$ for any odd prime p.

Proof. We may assume without loss of generality that a, b, c, d, e are integer and square-free (i.e., every prime divisor enters in the 1st power). First we show that we may assume that no three of a, b, c, d, e have a nontrivial common divisor. Indeed, let p be a prime divisor of three or more parameters.Then we multiply the equation $ax^2 + by^2 + cz^2 + dv^2 + ew^2 = 0$ by p and factor out perfect squares, thus obtaining an equation in which p divides at most 2 of the parameters a, b, c, d, e. Clearly, we may apply this procedure for all the prime divisors of a, b, c, d, e. Finally we may assume that for each prime p, at least three numbers among a, b, c, d, e are not divisible by p.

Fix a prime p. Without loss of generality a, b, c are not divisible by p.

If p is odd, then we use Problem 42: the equation

$$ax^2 + by^2 + cz^2 = 0$$

(and, consequently, the equation $ax^2 + by^2 + cz^2 + dv^2 + ew^2 = 0$) has a non-zero solution in $\mathbb{Q}_p$.

If $p = 2$, then one has to consider case-by-case all the residues of a, b, c, d, e modulo 8. □

Problem 44. Prove that, for any pair of nonzero integers (a, b), we have

$$\prod_p (a, b)_p = (a, b)_{-1},$$

where the product is taken over all primes p and

$$(a, b)_{-1} = \begin{cases} 1, & \text{if the equation } z^2 - ax^2 - by^2 = 0 \text{ has a real solution,} \\ -1 & \text{otherwise.} \end{cases} . \tag{17}$$

Proof. Since the Hilbert symbol is multiplicative (Problem 32), is is enough to check (17) in the case when a, b are prime numbers or -1.

Consider the case $a = b = -1$. Then $(a, b)_p = (-1, -1)_p$ is not 1 only if $p = 2$. But in this case one can directly verify that $(-1, -1)_2 = (-1, -1)_{-1} = -1$.

The next case: $a = -1$, b is a prime number. Then $(a, b)_p = (-1, b)_p$ is not 1 only if $p = b$ or $p = 2$. The direct check shows that $(-1, p)_p = (-1, p)_2$ for $p \neq 2$ and $(-1, 2)_2 = 1$. It means that the left-hand side of (17) equals the right-hand side of (17) and equals 1. □

As a last problem of this list, we mention an "analogue" of the Chinese Remainder Theorem: it turns out that one can construct a rational number with the prescribed values of the Hilbert symbol.

Problem 45. Fix a finite set of nonzero integers a_i and for every prime p define the values $\varepsilon_{i,p} = \pm 1$. Show that the system of equations

$$(a_i, x)_p = \varepsilon_{i,p}, \quad \forall i,\ \forall p,$$

has a solution if and only if

a) almost all (=all except finite number) $\varepsilon_{i,p} = 1$,

b) for any prime p, there exists a nonzero p-adic number x_p such that

$$(a_i, x_p) = \varepsilon_{i,p}.$$

Proof. The proof of this fact can be found in the book "A course in arithmetic" by J.-P. Serre, Chapter 3, § 2, Theorem 4. □

Two variables: maps of quadratic forms (DE-4)

In this section we study the equation

$$E_m: \quad ax^2 + bxy + cy^2 = m \tag{18}$$

depending on integer variables x, y, where a, b, c, m are integer parameters.

Problem 46 (Superproblem)**.** Prove that if the equation E_m has a solution for some positive m, has a solution for some negative m, has no non-trivial solutions for $m = 0$, then for every m either E_m has no solutions, or E_m has infinitely many solutions.

Proof. It follows from the problem statement that $f(x, y) = ax^2 + bxy + cy^2$ is an indefinite quadratic form which does not represent 0. Hence, the map of f splits into a positive domain and a negative domain by a periodic river. Consequently, the map of f is periodic; it means that every value written on the map appears infinitely many times. □

Problem 47 (Superproblem)**.** Is it true that if the equation E_m has solutions for

$$m = \pm 1,\ \pm 2,\ \pm 3,$$

then in this case E_m has solutions for any integer m?

Proof. We give a counterexample $f(x, y) = x^2 + xy - 18y^2$. □

Problem 48 (Superproblem)**.** Prove that if the equations E_1, E_2, E_3, E_5 have integer solutions, then the equation E_m has an integer solution for some $m < 0$.

Proof. Suppose the contrary. Then there are two cases: either f is positive definite or f is non-negative definite. We consider these cases independently.

Let f be non-negative definite. Then $f(x, y) = r(px + qy)^2$ for some integers r, p, q. Since f represents 1, we have $r = 1$. But then f does not represent 5.

Now let f be positive definite. Without loss of generality we assume that

$$f = px^2 + qy^2 + r(x - y)^2$$

for some non-negative integers p, q, r (see Problem 60). The values p, q, r are either all integers or all semi-integers. Without loss of generality we assume that $p \geqslant q \geqslant r$.

The minimal nonzero value of f is $q + r$. Since f represents 1, $q + r = 1$. Hence, either $q = 1$, $r = 0$, or $q = r = \frac{1}{2}$. We consider both these cases.

In the first case $q = 1$, $r = 0$. Since f represents 2, either $p = 1$, or $p = 2$. In the first case f does not represent 3, in the second case f does not represent 5.

In the second case $q = r = \frac{1}{2}$. Then for all positive p we have

$$f(x, y) \geqslant x^2 - xy + y^2.$$

Since f represents 2, $f(x, y) = 2$ for some integers x, y. In particular, $x^2 - xy + y^2 \leqslant 2$. This inequality is held for the following pairs (x, y):

$$(0, 1), \qquad (1, 0), \qquad (1, 1).$$

Since $f(0, 1) = 1$, there are only two cases: $f(1, 0) = 2$, $f(1, 1) = 2$. Let us consider both these cases.

Let $f(1, 0) = 2$. Then $p = \frac{3}{2}$, $f = y^2 - xy + 2y^2$. In this case f does not represent 3.

Let $f(1, 1) = 2$. Then $p = \frac{3}{2}$, $f = y^2 - xy + 2y^2$. In this case f does not represent 3 neither. □

Drawing a map

Problem 49. Prove that, if $\{w_1, w_2\}$ is a basis of $\mathbb{Z}^2$, then pairs

$$\{w_2, w_1\}, \{w_1 - w_2, w_2\}, \{w_1 + w_2, w_2\}, \{-w_1, w_2\} \tag{19}$$

are also bases of $\mathbb{Z}^2$.

Proof. Analogous to the proof of Problem 11. □

Problem 50. Show that, using transformations (19), it is possible to transform any basis to any other one.

Proof. Let $\{u, v\} := \{(a, b), (c, d)\}$ be a basis of $\mathbb{Z}^2$. We show that by transformations (19) we may send every basis $\{u, v\}$ to the basis $\{(1, 0), (0, 1)\}$. Consider the quadratic form $f(x, y) := x^2 - xy + y^2$. By Problem 60, in some basis $\{u', v'\}$ which can be obtained from $\{u, v\}$ via a series of transformations (19), the quadratic form f will be equivalent to a quadratic form of the form

$$\begin{gathered} px^2 + qy^2 + r(x + y)^2, \\ 2p = f(v') + f(u' + v') - f(u') \geqslant 0, \\ 2q = f(u') + f(u' + v') - f(v') \geqslant 0, \\ 2r = f(u' + v') - f(u') - f(v') \geqslant 0. \end{gathered} \tag{20}$$

The least values of the quadratic form (20) are attained for (x, y) equal to

$$(0, 1), \quad (1, 0), \quad (1, 1), \tag{21}$$

and the value on any other pair (x, y) is greater than at least one of these values. Since $x^2 - xy + y^2$ is positive definite, the value (20) is greater than 1 on all the pairs besides the pairs of the list (21). Hence, the value (20) on the pairs (21) is equal to 1. This implies one of the three statements below:

$$\{u', v'\} = \{(0, 1), (1, 0)\}, \qquad \{u', v'\} = \{(0, 1), (1, 1)\}, \qquad \{u', v'\} = \{(1, 0), (1, 1)\}. \tag{22}$$

Hence, the basis $\{u, v\}$ is equivalent to one of the bases (22). □

Problem 51. Show that a quadratic form can have the same representations in several different bases.

Proof. The quadratic form $x^2 - 2y^2$ is the same in bases $\{(3, 2), (4, 3)\}$ and $\{(1, 0), (0, 1)\}$. □

Problem 52. Find a quadratic form which has different representations in any two different bases of $\mathbb{Z}^2$.

Proof. Let $f(x, y) := 2x^2 - xy + 3y^2$, and let us show that for different bases, this form is written differently. Suppose the converse: assume that there exist two different bases such that this quadratic form has the same form in these bases. Let us reconstruct the map of this form step by step, starting from these bases, synchronously. Consider the first moment when the reconstructed domains intersect. Their intersection is either an edge or a vertex. Consider these cases independently.

If this intersection is a vertex, then the map of f is symmetric with respect to one of the edges incident to this vertex. Hence, the only well of the form $2x^2 - xy + 3y^2$ is also symmetric with respect to one of the edges incident to it. But this is not true since the values around the well are 2, 3, and 4.

If this intersection is an edge, then the map of f does not change, if we interchange the vertices of the edge. Hence, the vertices of this edge are wells, in particular, the form $2x^2 - xy + 3y^2$ has two wells. We get a contradiction.

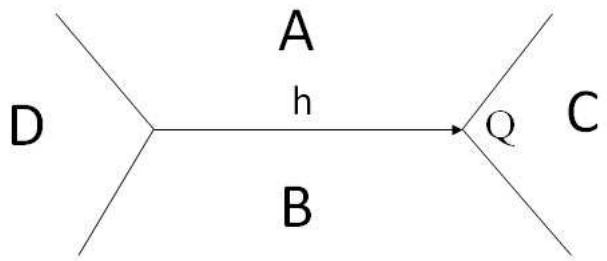
We proved that the quadratic form $2x^2 - xy + 3y^2$ is different in different bases. □

Exercise 1. Write down all the extensions of a basis $\{w_1, w_2\}$. Write down all the specializations of a superbasis $\{\pm w_1,\ \pm w_2,\ \pm(w_1 + w_2)\}$.

Exercise 2. Draw (oriented) maps of the following quadratic forms:

$$f_1 = 3x^2 + 9xy + 7y^2, \quad f_2 = x^2 - 2y^2, \quad f_3 = x^2 - 3y^2.$$

In two problems below, the values A, B, C, D, and h are related to the following picture.



Problem 53. Show that A, B, C, D, and h satisfy

$$C = A + B + h, \qquad D = A + B - h.$$

Proof. The problem statement is equivalent to the following identity for quadratic forms:

$$f(x + y) + f(x - y) = 2(f(x) + f(y)).$$

□

Problem 54. Assume that A, B, C are positive and the edge h goes from C to D. Show that in this case D is also positive and that the arrows on two other edges which are incident to Q go out of Q.

Proof. Since $D, h > 0$, $C = D + 2h > 0$. The values in the regions incident to the edges incident to D equal

$$4A + 2h + B, 4B + 2h + A \ (> A, B). \tag{23}$$

Hence, two remaining arrows go out of D. □

Problem 55. Show that the graph determined by the points-superbases and edges-bases is a tree, i.e., it has no cycles.

Proof. Consider the quadratic form $f(x, y) = x^2 + xy + y^2$. Its map has a unique well Q, and by Problem 54 all the arrows of this map go out of Q. If there were a cycle on this map, then it would be impossible that all the arrows go out of Q. Hence, the map of the quadratic form f does not contain cycles. But the underlying graph does not depend on the quadratic form, so for every f its map is a tree. □

Problem 56. Let Q be a unique well of a positive definite quadratic form f, and p, q, r be integers written in the regions adjacent to Q. Show that the number in any other region of a map related to f is strictly greater than $\max(p, q, r)$.

Proof. We fix a region A such that
a) A is not adjacent to a well,
b) the value of f on A is minimal among all the regions satisfying a).
We are going to prove that $f(A) > p, q, r$. It will end the proof. Let us find the path of the smallest length W from A to the well Q. Since W is the shortest, its last arrow bottoms at A. By the definition of the well all the arrows incident to it go out of it. This together with Problem 54 implies that all the arrows of W are oriented from Q. Hence, the last edge of W is oriented to A. So it follows from the conditions a) and b) that W contains only one edge. The statement of the problem for the regions connected with a well by an edge can be verified directly (see formula (23)). □

Problem 57. Prove that every positive definite form has a well.

Proof. Choose a vertex Q of the map, for which the sum of values of the neighbor regions is minimal. This vertex will be a well (cf. also Problem 53). □

Problem 58. a) Prove that a positive definite form has not more than two wells.
b) Find a positive definite form with two wells.

Proof. b) The form $x^2 + y^2$ is positive definite and has two wells.

a) Let Q be a well, and $p \geqslant q \geqslant r$ be the values written in the regions around it. There are two cases: $q + r > p$ or $q + r = p$. Consider these cases independently.

Let $q + r > p$. Then all the three arrows incident to Q go out of Q. Fix a vertex Q' and assume that it is a well. Let W be the shortest path joining Q and Q'. It follows from the proof of Problem 54 that all the edges of W are directed from Q to Q'. Hence, Q' is not a well.

Now let $q + r = p$. Then the second vertex of the edge E, separating the value q from the value r, is also a well. We denote it by Q'. The collections of values around Q and around Q' coincide. Assume that there exists one more well Q'', and let W be the shortest path, joining Q'' either with Q or with Q'. Then W does not pass through the second one. Without loss of generality we assume that W joins Q with Q''. Then all the edges of W are directed from Q, hence, Q'' is not a well. □

Problem 59. Provide an algorithm which solves the equation $ax^2+bxy+cy^2 = m$ (a, b, c, m are parameters, x, y, z are variables), under the assumption that $ax^2 + bxy + cz^2$ is positive definite.

Proof. After an appropriate change of variables we may assume that $f = px^2 + q(x - y)^2 + ry^2$ for some positive values p, q, r (see Problem 60). If $f(x, y) = n$ has integer solutions, then

$$px^2 \leqslant n, ry^2 \leqslant n. \tag{24}$$

The number of pairs of integers (x, y) for which x, y satisfy (24) is finite. If we check them all, we will detect whether the equation $f(x, y) = n$ has solutions or not. □

Problem 60 (Classification of positive definite quadratic forms)**.**

a) Show that any positive definite quadratic form is equivalent to the form

$$(p + q)x^2 + 2qxy + (q + r)y^2 \tag{25}$$

for some non-negative numbers p, q, r.

b) Show that the quadratic forms corresponding to

$$(p_1, q_1, r_1) \text{ and } (p_2, q_2, r_2)$$

are equivalent if and only if these triples coincide as multisets.

c) Find out which triples (p, q, r) determine an integer quadratic form.

d) Find out which triples (p, q, r) determine a positive definite quadratic form.

Proof. Let Q be a well of f, and m, n, k be the values around this well. Let

$$p = \frac{m + n - k}{2}, q = \frac{m + k - n}{2}, r = \frac{k + n - m}{2}.$$

Then f is equivalent to the form

$$px^2 + qy^2 + r(x - y)^2 = (25).$$

In the case b) there is a counterexample in our notation $x^2 + 3y^2$ и $x^2 + xy + y^2$. In the statement of the problem, "equivalent" must be replaced by "linearly equivalent".

The answer of c): when either p, q, r are integers, or $p - \frac{1}{2}$, $q - \frac{1}{2}$, $r - \frac{1}{2}$ are integers.

The answer of d): the form f is positive definite, if $p, q, r \geqslant 0$ and at least two of numbers p, q, r are nonzero. □