V.V. Ostrik, M.A. Tsfasman

ALGEBRAIC GEOMETRY AND NUMBER THEORY:

RATIONAL AND ELLIPTIC CURVES

MCCME Publishers
Moscow • 2022

Ostrik V.V., Tsfasman M.A.

Algebraic geometry and number theory: rational and elliptic curves. — Moscow: MCCME: IUM, 2022. — 54 p.

ISBN 978-5-4439-4630-6

Translated into English on the initiative and with financial support of Alexander Gerko

Translated from the Russian language edition
Острик В. В., Цфасман М. А. Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые. — 3-е изд., стер. — М.: МЦНМО, 2011.

ISBN 978-5-4439-4630-6

PYTHAGOREAN TRIPLES

For a right triangle with legs X and Y and hypotenuse Z, the Pythagorean theorem states that the sum of the squared lengths of the legs is equal to the squared length of the hypotenuse, i.e.,

$$X^2 + Y^2 = Z^2. \tag{1}$$

Even in ancient times, people had an example of positive integers X, Y, and Z, satisfying this equation: $X = 3$, $Y = 4$, $Z = 5$. The triangle with these side lengths is known as the Egyptian triangle. It can be constructed by stretching a circular rope with knots dividing it into 12 equal parts over three pegs stuck in the ground so that they form a triangle with sides lengths 3, 4, and 5 (Fig. 1). This is how one can construct a right angle on a flat terrain.

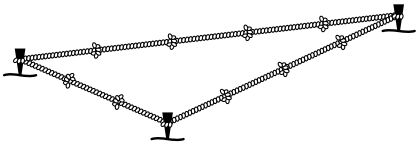


Fig. 1

Let us describe all *Pythagorean triples*, i.e., triples (X, Y, Z) of non-negative integers satisfying the relation $X^2 + Y^2 = Z^2$. First, note that if we have such a triple, then, multiplying all three integers of this triple by the same positive integer, we again obtain a Pythagorean triple. Therefore, it is sufficient to find only triples of coprime integers. Moreover, it suffices to find triples of pairwise coprime integers: if two of the numbers X, Y, and Z are divisible by a prime p, then so is the third number.

Note that the only solution with $Z = 0$ is $X = Y = Z = 0$, and we shall not consider it in what follows. For all other solutions of the equation $X^2+Y^2 = Z^2$, the number Z is nonzero. Dividing the equation by the square of Z, we obtain the following new equation

$$x^2 + y^2 = 1, \tag{2}$$

where $x = \dfrac{X}{Z}$ and $y = \dfrac{Y}{Z}$ are rational numbers.

Equation (2) determines a circle S of radius 1 centered at the origin (Fig. 2). We have reduced the initial problem to that of listing all rational points[1]) of this circle. It turns out that there are, in a certain sense, as many such points as there are rational points on the real line. Some of these rational points are easy to find: $(\pm 1, 0)$, $(0, \pm 1)$. Let us choose one of them, say $A = (0, 1)$, and draw all straight lines (except for the horizontal one) passing through point A. Every such line l intersects the circle in yet another point $B = (x, y)$ and the x-axis in some point $C = (c, 0)$.

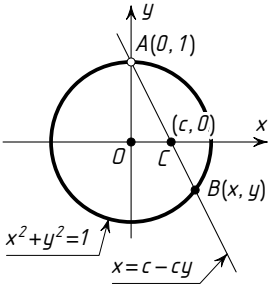


Fig. 2

1. Check that, assigning the point C to each point B, we obtain a one-to-one correspondence between the points of the circle S (except A) and the points of the straight line $y = 0$.[2])

Such is the geometry. What about the arithmetic? It turns out that the correspondence indicated above preserves the rationality of points.

Let us prove that a point B has rational coordinates if and only if the number c is rational. The line passing through A and C is determined by the equation $x = c - cy$. Let us substitute it into the equation of the circle. We obtain

$$(c - cy)^2 + y^2 = 1, \quad \text{i.e.,} \quad (c^2 + 1)y^2 - 2c^2 y + c^2 - 1 = 0,$$

whence $y = 1$ (which corresponds to the point A) or $y = \dfrac{c^2 - 1}{c^2 + 1}$, so that $x = c - cy = \dfrac{2c}{c^2 + 1}$. If the number c is rational, then so are x and y.

The converse is an immediate consequence of the following two assertions (which we constantly use in what follows).

---

[1]) A rational point is a point with rational coordinates.

[2]) The vertical double bar indicates text problems for unassisted solution. Challenging problems are marked by a star *.

2. If the coordinates of two points are rational, then the equation of the straight line passing through them can be written so that it has rational coefficients.

If two straight lines are determined by equations with rational coefficients, then their intersection point has rational coordinates (if it exists).

Thus, every rational solution of equation (2), except $x = 0$, $y = 1$, can be obtained by substituting some rational number for c into the formula

$$x = \frac{2c}{c^2+1}, \qquad y = \frac{c^2-1}{c^2+1}.$$

Let us represent c as an irreducible fraction m/n (m and n are integers). We have

$$x = \frac{2c}{c^2+1} = \frac{2mn}{m^2+n^2}, \qquad y = \frac{c^2-1}{c^2+1} = \frac{m^2-n^2}{m^2+n^2}$$

(note that, for $n = 0$ and $m \neq 0$, we obtain the solution $x = 0$, $y = 1$, which we had intentionally "lost").

Recall that our goal is to find all positive integer solutions of equation (1). We have

$$\frac{X}{Z} = \frac{2mn}{m^2+n^2}, \qquad \frac{Y}{Z} = \frac{m^2-n^2}{m^2+n^2}$$

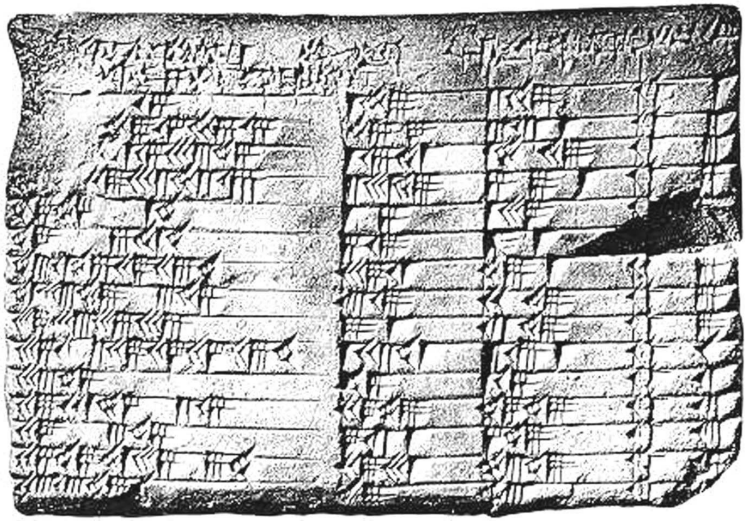
(where $m^2 + n^2 \neq 0$). The fractions on the left-hand sides of these equations are irreducible, because X, Y, and Z are pairwise coprime. If the fractions on the right-hand sides were irreducible as well, then we could set $X = 2mn$, $Y = m^2 - n^2$, and $Z = m^2 + n^2$, but this is not always the case; e.g., both fractions are reducible for $m = 5$ and $n = 3$. However, these fractions can be reduced only by 2. Indeed, consider the first fraction. Suppose that the prime p ($p \neq 2$) divides $2mn$; if p divides m, then it cannot divide n, because the fraction m/n is irreducible. Therefore, $m^2 + n^2$ is not divisible by p, and if m and n are odd, then the fraction $\dfrac{2mn}{m^2+n^2}$ can be reduced only by 2. Consider the second fraction: if the prime p divides both $m^2 - n^2$ and $m^2 + n^2$, then p divides $2m^2$ and $2n^2$. The numbers m and n have no common divisors; hence $p = 2$, and both m and n are odd.

Thus, the coprime positive integer solutions of (1) are

$$X = mn, \quad Y = \frac{m^2-n^2}{2}, \quad Z = \frac{m^2+n^2}{2} \tag{3}$$

for mutually coprime odd m and n, $m > n > 0$, whence we obtain

$$X = 2mn, \quad Y = m^2 - n^2, \quad Z = m^2 + n^2 \tag{4}$$



The figure above shows the Plimpton 322 clay tablet in the Plimpton collection at Columbia University, New York, with a Babylonian cuneiform inscription (19th to 17th century B.C.) discovered by G. Plimpton in the 1920s.

The tablet contains a list of several right triangles with integer side lengths X, Y, and Z. Several columns to the left of the tablet have been broken off. The first unbroken column, I, contains quotients $\frac{Z^2}{X^2}$, which smoothly decrease from 2 to a value slightly greater than 4/3. The next two columns, II and III, contain the corresponding "widths" Y and "diagonals" Z. The last column, IV, contains only the sequence of consecutive numbers from 1 to 15.

The widths Y and diagonals Z satisfy the equation

$$X^2 + Y^2 = Z^2,$$

in which the "height" X is an integer and the only prime divisors of X are 2, 3, and 5. In the 11th and 15th rows, the numbers X, Y, and Z have a common divisor greater than 1. In all other cases, these numbers are coprime.

The Plimpton 322 table is deciphered on p. 7 (the numbers are first presented in Babylonian sexagesimal notation, so that, say, the expression 1,22;5,14 denotes the number

$$1 \cdot 60^1 + 22 \cdot 60^0 + 5 \cdot 60^{-1} + 14 \cdot 60^{-2},$$

and then appear in decimal notation).

It should be mentioned that the Babylonian notation for integers is ambiguous. For example, the notations for 1,22;5,14, 1,22,5;14, and 1,22,5,14 (which correspond to different integers) were identical, and one could understand which one of these integers is meant only from the context. The notations for 5,14;1 and 5,0,14;1 were identical as well, because there was no symbol for zero. The deciphered version presented below was made under the assumption that all numbers in columns II and III are integer (to be more precise, they have the least positive integer values among all possible ones).

Z^2/X^2	X	Y	Z	No.
1;59,0,15	2,0	1,59	2,49	1
1;56,56,58,14,50,6,15	57,36	56,7	1,20,25[1])	2
1;55,7,41,15,33,45	1,20,0	1,16,41	1,50,49	3
1;53,10,29,32,52,16	3,45,0	3,31,49	5,9,1	4
1;48,54,1,40	1,12	1,5	1,37	5
1;47,6,41,40	6,0	5,19	8,1	6
1;43,11,56,28,26,40	45,0	38,11	59,1	7
1;41,33,45,14,3,45	16,0	13,19	20,49	8
1;38,33,36,36	10,0	8,1[2])	12,49	9
1;35,10,2,28,27,24,26	1,48,0	1,22,41	2,16,1	10
1;33,45	1,0	45	1,15	11
1;29,21,54,2,15	40,0	27,59	48,49	12
1;27,0,3,45	4,0	2,41[3])	4,49	13
1;25,48,51,35,6,40	45,0	29,31	53,49	14
1;23,13,46,40	1,30	56	1,46[4])	15
I		II	III	IV
approximately 1,98340	120	119	169	1
" 1,94916	3456	3367	4825	2
" 1,91880	4800	4601	6649	3
" 1,88625	13500	12709	18541	4
" 1,81501	72	65	97	5
" 1,78519	360	319	481	6
" 1,71998	2700	2291	3541	7
" 1,69271	960	799	1249	8
" 1,64267	600	481	769	9
" 1,58612	6480	4961	8161	10
1,5625	60	45	75	11
approximately 1,48942	2400	1679	2929	12
" 1,45002	240	161	289	13
" 1,43024	2700	1771	3229	14
" 1,38716	90	56	106	15

In deciphering this table, the following four corrections were made:

[1]) the number 3,12,1 (written in the Plimpton 322 table) was replaced by 1,20,25;
[2]) 9,1 was replaced by 8,1;
[3]) 7,12,1 was replaced by 2,41;
[4]) 53 was replaced by 1,46.

for the coprime integers m and n, $m > n > 0$, one of which is even. (It is easy to check that any such triple (X, Y, Z) is indeed a solution.) All positive integer solutions are obtained by multiplying (3) or (4) by a positive integer.

Note that, in fact, formulae (3) and (4) coincide. If $X = pq$, $Y = \dfrac{p^2 - q^2}{2}$, $Z = \dfrac{p^2 + q^2}{2}$ is the solution calculated by (3) (here p and q are odd and coprime), then the same solution is obtained by (4) with $m = \dfrac{p+q}{2}$ and $n = \dfrac{p-q}{2}$ (check that m and n are coprime and precisely one of them is even), although X and Y exchange places. Similarly, any solution from (4) can be written in the form (3). One may say that all positive integer solutions of (1) are described by (4) up to interchanging X and Y and multiplying X, Y, and Z by a positive integer.

All solutions of equation (1) can also be written as

$$\left.\begin{aligned} X = 2mnr, \quad Y = (m^2 - n^2)r, \\ Z = (m^2 + n^2)r, \end{aligned}\right\} \quad (3'\text{–}4')$$

where m and n are any integers and r is a suitable rational, i.e., a rational such that X, Y, and Z are integers.

Check that the known solutions $(3, 4, 5)$ and $(4, 3, 5)$ are given by formulae (3) with $m = 3$ and $n = 1$ and by formulae (4) with $m = 2$ and $n = 1$. These solutions are also given by $(3'\text{–}4')$ with $m = 3$, $n = 1$, $r = \dfrac{1}{2}$ and with $m = 2$, $n = 1$, and $r = 1$.

3. Write out all Pythagorean triples (a, b, c), $0 < a < b < c < 100$.

4. What do we obtain when we take $(1, 0)$ for the point A and consider the intersection point of lines through A with the line $y = -1$ rather than with the x-axis (see Fig. 3)?

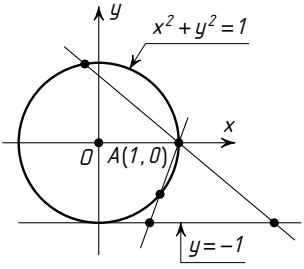


Fig. 3

A bit of history

The ancient Greeks learned about the triangle with sides 3, 4, 5 from the Egyptians and called it the Egyptian triangle. We refer to a right triangle with integer sides as a Pythagorean triangle. Actually, neither Pythagoras nor the Egyptians were the first to use them. On ancient Mesopotamian headstones (over 5 000 years old), an isosceles triangle constructed from two right triangles with sides 9, 12, and 15 ells already appears. Constructing the pyramid of Pharaoh Sneferu (17th century BC), Egyptian architects used a right triangle with sides of ten times 20, 21, and 29 ells, and another right triangle with sides of ten times 18, 24, and 30 ells. In the Plimpton clay tablet no. 322 (19th–17th centuries BC), there are 15 rows containing the values Y, Z, and Z^2/X^2 (see pages 6–7 above). Note that the triples of numbers mentioned by us are fairly large. It is natural to assume that the ancient Babylonians also knew a general method for finding these solutions.

The Greek mathematician Diophantus (3rd century AD) knew how to find integer solutions not only of equation (1), but also of certain other quadratic equations, some systems of two quadratic equations in three unknowns, as well as some cubic equations in two unknowns (see Supplement 4). Probably Diophantus knew and used the work of several of his precursors. Number theory of present times begins with Fermat's notes on the margins of Diophantus' book. The foundations of the new geometrical approach to integer solutions were laid by Newton, who understood that the complicated changes of variable used by Diophantus often reduce to drawing secants and tangents.

RATIONAL CURVES

The example involving the construction of secants considered above is actually quite general. Let us use it to solve the following problem: describe all the integer triples such that the square of the first plus twice the square of the second one equals three times the square of the third, i.e., let us find the integer solutions of the equation

$$X^2 + 2Y^2 = 3Z^2. \tag{5}$$

As noted above, the unique solution with $Z = 0$ is $X = Y = Z = 0$, which we have agreed to ignore. Dividing both sides of the equation (5) by Z^2, we obtain the following new equation:

$$x^2 + 2y^2 = 3, \tag{6}$$

where $x = X/Z$ and $y = Y/Z$ are rational numbers.

Equation (6) describes the ellipse with horizontal semi-axis $\sqrt{3}$ and vertical semi axis $\sqrt{6}/2$ centered at the origin (Fig. 4).

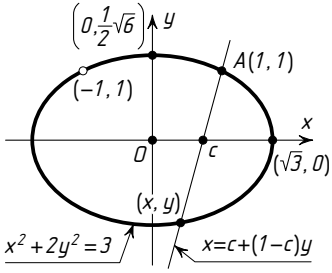


Fig. 4

It is not difficult to find a rational point on this ellipse: such is, for instance, the point $(1, 1)$. Just as in the problem of Pythagorean triples, let us construct a bijection between all the points of the ellipse (except for $(-1, 1)$) and the points of the line $y = 0$. Here again there are as many rational points on the ellipse (with $(1, 1)$ removed) as on the line. The equation of the line passing through the points $A(1, 1)$ and $(c, 0)$ can be written as $x = c + (1 - c)y$. The y coordinate of the second intersection point of the line with the ellipse satisfies the condition

$$(c + (1 - c)y)^2 + 2y^2 = 3.$$

We know one root of this quadratic equation, it equals 1. Now, using Vieta's theorem, it is not difficult to find the other root:

$$y = \frac{c^2 - 3}{c^2 - 2c + 3}$$

Then

$$x = c + (1 - c)y = \frac{-c^2 + 6c - 3}{c^2 - 2c + 3}.$$

(Note that for $c = 3$ we get $x = 1$, $y = 1$, i.e., this is not the second intersection point but a tangent point. The point $(-1; 1)$ does not lie on such a line.)

Using the assertion of Problem 2, we conclude that all the rational solutions of equation (6) (except for the solution $x = -1$, $y = 1$, which corresponds to the horizontal line), are given by the formulae

$$x = \frac{-c^2 + 6c - 3}{c^2 - 2c + 3}, \qquad y = \frac{c^2 - 3}{c^2 - 2c + 3},$$

where c is a rational number, while the integer solutions of equation (5) are given by the formulae

$$X = (-m^2+6mn-3n^2)r, \quad Y = (m^2-3n^2)r, \quad Z = (m^2-2mn+3n^2)r,$$

where m and n are integers and r is an appropriate rational number[1]).

5. Describe all the integer solutions of the equations
a) $X^2 - 15Y^2 = Z^2$, b) $X^2 - YZ = 9Z^2$, c) $X^2 + 3Y^2 = 5Z^2$.

* * *

Now let the curve be given by the equation $f(x, y) = 0$, where $f(x, y)$ is a polynomial that cannot be decomposed into the product of polynomials of degree higher than zero, even if complex coefficients are allowed (such curves are called *absolutely irreducible*[2]). If, as in the above examples, there exist polynomials with rational coefficients $F(c)$, $G(c)$, and $H(c)$, such that at least one of the functions $\frac{F(c)}{H(c)}$ and $\frac{G(c)}{H(c)}$ is non-constant, and substituting $x = \frac{F(c)}{H(c)}$ and $y = \frac{G(c)}{H(c)}$ into $f(x, y)$ we get identical zero, then we say that our curve is *rational* (since the ratio of two polynomials is called a rational function).

6. Let $f(x, y)$ be a polynomial of degree 2 with rational coefficients and assume that the curve $f(x, y) = 0$ is absolutely irreducible. Prove that if this curve contains at least one rational point, then it is a rational curve.

Legendre's Theorem

Consider the following problem. Let a, b, c be positive integers. How can one find the rational solutions of the equation

$$ax^2 + by^2 = c?$$

You have probably guessed: we work as above, and begin by finding at least one rational point on the curve determined by the equation $ax^2 + by^2 = c$.

Thus the following question arises: When does the equation $ax^2 + by^2 = c$ have a rational solution? The answer is not as easy as one may think. For example, for $a = b = 1$, the following problem arises:

7*. When is a positive integer c equal to the sum of squares of two rational numbers?

This is a very difficult problem. We recommend not to hurry with its solution, and first get acquainted with the notion of *quadratic residue.*

---

[1]) Note that for a different choice of the point A on the ellipse the final formulae may differ from those presented above, however, they will obviously describe the same set of solutions (*cf. Problem 4*).

[2]) Attention: the curve $x^2 + y^2 = 0$ is not absolutely irreducible, since $x^2 + y^2 = (x + \sqrt{-1}y)(x - \sqrt{-1}y))$

Now let us consider the general situation. We can assume that the integers a, b, c are coprime (if they aren't, divide them by their greatest common divisor) and *square-free*, i.e., are not divisible by squares of integers (if, say, a is divisible by m^2, make the change of variables $x' = mx$).

8*. Let a, b, c be pairwise coprime square-free integers. If the equation $ax^2 + by^2 = c$ has a rational solution, then there exist integers m, n, k such that $m^2 + ab$ is divisible by c, $n^2 - ac$ is divisible by b, and $k^2 - bc$ is divisible by a.

Thus, the remainders in the division of $(-ab)$ by c, of ac by b, and of bc by a cannot be arbitrary.

* * *

Quadratic residues. The remainders obtained in the division of squares of integers by a number M are called *quadratic residues modulo* M, while all the other remainders are *quadratic nonresidues modulo* M. For example, 2 is a quadratic residue modulo 7, while 3 is a quadratic nonresidue modulo 7 (prove this!). We also say that an integer N is a quadratic residue (nonresidue) modulo M if the remainder in the division of N by M is a quadratic residue (respectively, nonresidue) modulo M. For example, 8 is quadratic residue modulo 7, while 10 is a quadratic nonresidue modulo 7.

9. Find all the quadratic residues and nonresidues modulo 7, modulo 17, modulo 24, and modulo 30.

10. Let p be an odd prime number. Prove that among the p possible remainders in division by p exactly $(p+1)/2$ are quadratic residues and exactly $(p-1)/2$ are quadratic nonresidues.

11*. Let $M = p_1 \cdot \ldots p_n$ be the product of distinct primes. Find the number of quadratic residues and nonresidues modulo M.

12*. Let p be an odd prime. Prove that the remainder $p-1$ is a quadratic residue modulo p if and only if the remainder in the division of p by 4 is 1.

* * *

Thus, the equation $ax^2 + by^2 = c$, where a, b, c are square-free coprime positive integers, will have a rational solution, it is *necessary* that the integer $(-ab)$ be a quadratic residue modulo c, the integer ac be a quadratic residue modulo b, and (bc) be a quadratic residue modulo a. It turns out that these conditions are also *sufficient*:

Legendre's Theorem. *The equation $ax^2 + by^2 = c$, where a, b, c are coprime positive integers, will have a rational solution if and only if the integer $(-ab)$ is a quadratic residue modulo c, the integer ac is a quadratic residue modulo b, and bc is a quadratic residue modulo a.*

13. Do the equations

$$\text{a) } 3x^2 + 5y^2 = 7; \qquad \text{b) } 5x^2 + 7y^2 = 3$$

have rational solutions?

14. Let us prove the Legendre Theorem. Let a, b, c satisfy the conditions of the theorem.

a) Show that in the statement of the Legendre Theorem it suffices to assume that the integers are pairwise coprime.

b) Let p be a prime that divides abc. Show that there exist linear functions with integer coefficients

$$L_p = \lambda_1(p)x + \lambda_2(p)y + \lambda_3(p)z,$$
$$M_p = \mu_1(p)x + \mu_2(p)y + \mu_3(p)z$$

such that $ax^2 + by^2 - cz^2 \equiv L_p M_p \pmod{p}$.

c) Show that there exist linear functions with integer coefficients

$$L = \lambda_1 x + \lambda_2 y + \lambda_3 z,$$
$$M = \mu_1 x + \mu_2 y + \mu_3 z$$

such that $ax^2 + by^2 - cz^2 \equiv LM \pmod{abc}$.

d) Prove that there exists a nonzero solution of the equation $ax^2 + by^2 + cz^2 \equiv 0 \pmod{abc}$ such that

$$-\sqrt{bc} < x < \sqrt{bc}, \quad -\sqrt{ac} < y < \sqrt{ac}, \quad -\sqrt{ab} < z < \sqrt{ab}.$$

e) Let (x_0, y_0, z_0) be a solution of of the equation from item d). Prove that either $ax_0^2 + by_0^2 - cz_0^2 = 0$ or $ax_0^2 + by_0^2 - cz_0^2 = abc$.

f) Let $ax_0^2 + by_0^2 - cz_0^2 = abc$. Prove that in that case

$$a(x_0 z_0 + by_0)^2 + b(y_0 z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0.$$

g) Prove Legendre's Theorem.

ELLIPTIC CURVES

Consider the following problems:

A. Find all the pairs of natural numbers m and n such that the sum of the first m positive integers is equal to the sum of squares of the first n positive integers:

$$1 + 2 + 3 + \ldots + m = 1^2 + 2^2 + 3^2 + \ldots + n^2.$$

B. For what values of n, the sum of squares of the first n positive integers is itself the square of an integer?

C. What positive integers are simultaneously the product of two successive positive integers and the product of three successive positive integers?

D. (Fermat's last theorem for $n = 3$). Prove that the equation $X^3 + Y^3 = Z^3$ has no positive integer solutions.

E. When does the sum of the square of a rational number and the cube of the same number equal the cube of a rational number?

F. When does the sum of the square of a rational number and the cube of the same number equal the square of a rational number?

All these problems are united by the fact that they can be reduced to the study of integer or rational solutions of *cubic* equations in two variables.

15. Prove that

$$1+2+\ldots+m=\frac{m(m+1)}{2} \quad \text{and} \quad 1^2+2^2+\ldots+n^2=\frac{n(n+1)(2n+1)}{6}.$$

A. This problem is equivalent to finding the integer solutions of the equation

$$\frac{m(m+1)}{2}=\frac{n(n+1)(2n+1)}{6}.$$

B. While this problem is equivalent to finding the integer solutions of the equation

$$\frac{n(n+1)(2n+1)}{6}=m^2.$$

C. Here we must find the integer solutions of the equation

$$m(m+1)=(n-1)n(n+1).$$

D. By the change of variables $x=X/Z$, $y=Y/Z$ the problem reduces to finding the positive *rational* solutions of the equation $x^3+y^3=1$.

E. In this problem, one must find the rational solutions of the equation $x^2+x^3=y^3$.

F. And here $x^2+x^3=y^2$.

Equations in two variables determine a curve on the plane. Since our curves are given by third degree polynomial equations, they are examples of *curves of third degree* or *cubic curves* (Fig. 5).

Notice that among the curves in Fig. 5, the two curves from problems **E** and **F** differ from the other ones (**A**–**D**): the first one has a *cusp point* while the second one has a *self-intersection point*. These points are examples of *singular points*[1]); the curves possessing at least one singular point are called *singular*. Curves having no singular points are called *non-singular* or *smooth* — such are the curves from problems **A**–**D**.

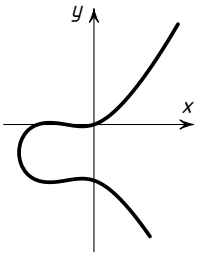
16. What is the maximal number of singular points of a second degree curve? a third degree curve? a fourth degree curve?

---

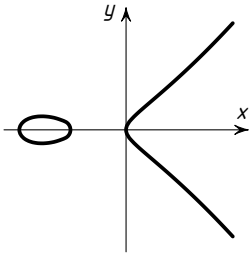
[1]) Let us give a precise definition: a point (x_0, y_0) on the curve $F(x,y)=0$ is called *nonsingular* if there exists at least one line passing through it

$$x=x_0+at, \qquad y=y_0+bt$$

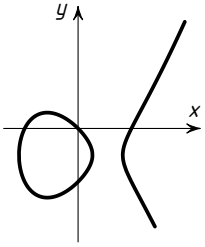
such that $t=0$ is a root of the equation $F(x_0+at,\ y_0+bt)=0$ of multiplicity 1. In the converse case, the point is called *singular*.



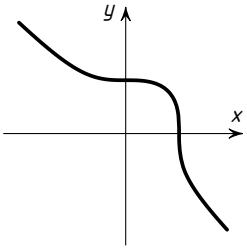
A. $\dfrac{y(y+1)}{2} = \dfrac{x(x+1)(2x+1)}{6}$



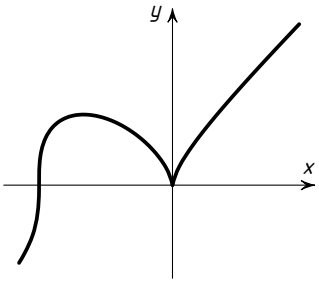
B. $y^2 = \dfrac{x(x+1)(2x+1)}{6}$



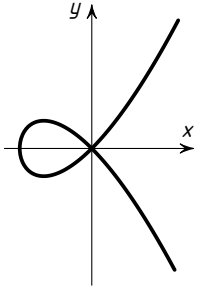
C. $y(y+1) = (x-1)x(x+1)$



D. $x^3 + y^3 = 1$



E. $x^2 + x^3 = y^3$



F. $x^2 + x^3 = y^2$

Fig. 5

17. Can a curve of degree four have exactly five singular points?

Let us try to apply the method of secants from the previous sections to our curves. On each of the curves it is easy to find points with integer coordinates. However, the construction of secants in this situation gets us nowhere: a typical curve will intersect our curve in three points (and not in two, as before) and the argument used for second degree curves no longer works. Nevertheless, we can save the day in the case of singular curves.

18. Prove that any line passing through a singular point of a third degree curve can intersect the curve in no more than one other point:
a) for the curves in problems E and F;
b) for any absolutely irreducible singular cubic curve.

Thus, drawing secants through the singular point and applying the same arguments as for second degree curves, we can find the rational solutions of cubic equations (with rational coefficients) that determine singular curves. Note that there is a delicate condition here: in applying the method of secants, it is necessary for the initial point (in our case, the singular point) to have rational coordinates.

19. Suppose that on an absolutely irreducible singular cubic curve given by an equation with rational coefficients there is at least one rational point. Prove that in that case the coordinates of the singular point are also rational.

20*. Give an example of a cubic equation with rational coefficients that determines a singular curve all of whose singular points have irrational coordinates.

21. Give a solution of problems E and F. Prove that the corresponding curves are rational.

Unfortunately, nonsingular cubic curves are never rational. What must we do with these curves? The first thing that can be done is to bring them to a simpler form. To do this, we will use *projective changes of coordinates*, i.e., changes of the following form:

$$x' = \frac{\alpha_1 x + \alpha_2 y + \alpha_3}{\gamma_1 x + \gamma_2 y + \gamma_3}, \quad y' = \frac{\beta_1 x + \beta_2 y + \beta_3}{\gamma_1 x + \gamma_2 y + \gamma_3}, \quad \gamma_1^2 + \gamma_2^2 + \gamma_3^2 \neq 0.$$

Such changes of variables are very convenient, but they have a defect: they are not everywhere defined (what do x' and y' equal on the line $\gamma_1 x + \gamma_2 y + \gamma_3 = 0$?). Note, however, that the line $\gamma_1 x + \gamma_2 y + \gamma_3 = 0$ intersects our cubic curve in no more than three points; if we intend to find the rational (or integer, or positive integer) roots of the given cubic equation, we can first consider all the intersection points of the line with the curve and then perform an appropriate projective change.

22. a) Under what conditions on the coefficients $\alpha_i, \beta_i, \gamma_i$, $i = 1, 2, 3$, is the projective change invertible, i.e., takes distinct points (x, y) to distinct points (x', y')?

b) Assume that we consider an invertible projective change. The inverse change (i.e., the change expressing x and y in terms of x' and y') is also a projective change of coordinates.

c) The successive application of two invertible projective changes is equivalent to a certain single such change.

In what follows, we will consider only invertible projective changes of coordinates.

A cubic curve in the (x, y)-plane is said to be a *curve in Weierstrass form* if it is given by an equation of the following form:

$$y^2 = x^3 + ax + b.$$

23. A curve in Weierstrass form is singular if and only if $4a^3+27b^2 = 0$.

The number $\Delta = 4a^3 + 27b^2$ is called the *discriminant* of a given cubic curve, as well as the *discriminant* of the corresponding polynomial $x^3 + ax + b$. (The discriminant is zero if and only if the polynomial has a multiple root.)

24. When is the curve given by $y^2 = x^3 + ax^2 + bx + c$ singular?

Newton's Theorem. *For any nonsingular cubic curve there exists a projective change of coordinates that brings it to Weierstrass form. Moreover, if the coefficients of the equation determining the given curve are rational and the curve has at least one rational inflexion point*[1]*), there is a projective change with rational $\alpha_i, \beta_i, \gamma_i$, $i = 1, 2, 3$, that takes the given curve to a curve in Weierstrass form with rational a and b.*

25. Prove this theorem.

Let us illustrate Newton's theorem by problems A–D.

A. After the change $m = (y - 9)/18$, $n = (x - 3)/6$, we obtain the equation

$$y^2 = x^3 - 9x + 81.$$

B. The change $m = y/72$, $n = (x - 6)/12$ brings the equation to the form

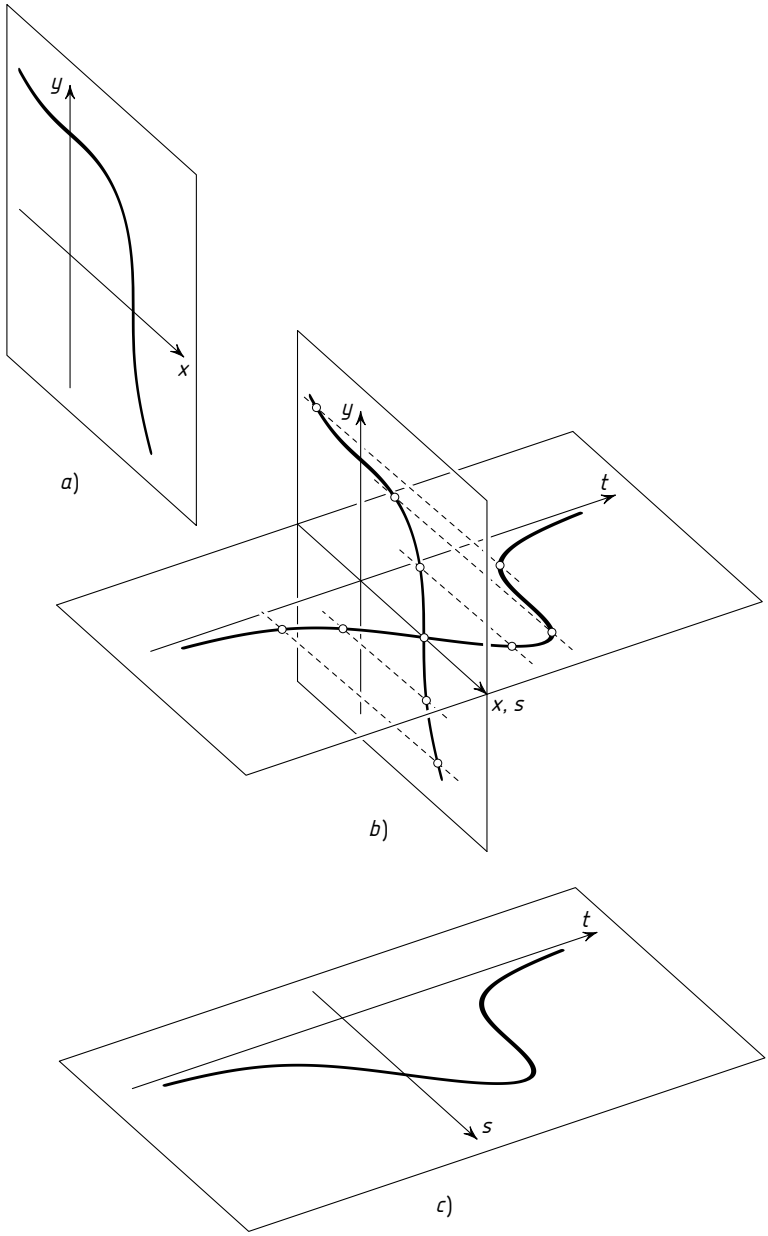
$$y^2 = x^3 - 36x.$$

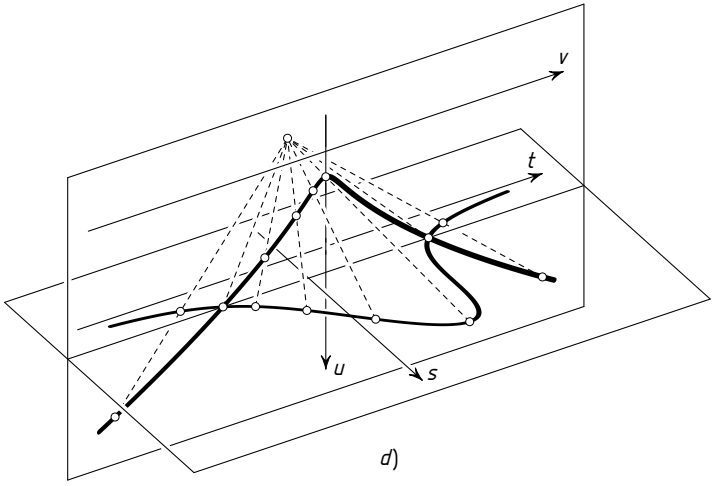
C. The change $m = y - \frac{1}{2}$, $n = x$ brings the equation to the form

$$y^2 = x^3 - x + \frac{1}{4}.$$

---

[1]) Recall that the tangent to a nonsingular curve $F(x, y) = 0$ at a point (x_0, y_0) is the line $x = x_0 + at$, $y = y_0 + bt$ such that $t = 0$ is a root of multiplicity no less than 2 of the equation $F(x_0 + at, y_0 + bt) = 0$. The tangent at a nonsingular point exists and is unique. In the case when the root $t = 0$ is of multiplicity 3 or more, then the point (x_0, y_0) is said to be a *inflexion point.*


y
x
a)
y
t
x, s
b)
t
s
c)



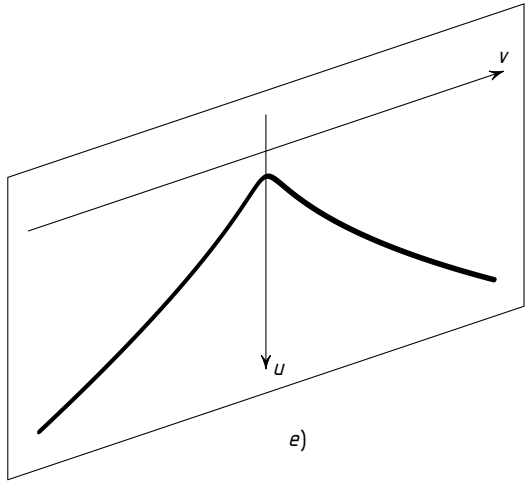


Fig. 6. Projective changes of variable that bring the curve $x^3 + y^3 = 1$ to Weierstrass form.

a) The curve $x^3+y^3=1$. *b*) The change $x=s-t$, $y=t$ is a parallel projection of the (x, y)-plane onto the (s, t)-plane. *c*) The curve $s^3-3s^2t+3st^2=1$. *d*) The change $s=\frac{1}{3u}$, $t=\frac{6v+1}{6u}$ is a central projection of the (s, t)-plane onto the (u, v)-plane. *e*) The curve $v^2=u^3-\frac{1}{108}$ (in Weierstrass form).

D. The case of the Fermat curve $x^3 + y^3 = 1$ is the most interesting one (Fig. 6). First let us perform the change $x = s - t$, $y = t$, obtaining the equation $s^3 - 3st(s - t) = 1$. Now the change $s = \frac{1}{3u}$, $t = \frac{6v + 1}{6u}$ brings the equation to the form

$$v^2 = u^3 - \frac{1}{108}.$$

Unfortunately, not all cubic curves determined by equations with rational coefficients have a rational inflexion point.

26. Check that there are no rational points at all on the curves

$$x^3 + 2y^3 = 4 \quad \text{and} \quad x^3 + 2y^3 = 7.$$

But even if there is a rational point on the curve, all the inflexion points can turn out to be non rational.

27. Check that all the inflexion points of the curve $x^3 + 2y^3 = 3$ are non rational (note that this curve contains the rational point $(1, 1)$).

Thus, Newton's theorem is not sufficient for bringing a curve to Weierstrass from. For that we have the following

Nagell's Theorem. *If a nonsingular cubic curve C_1 contains a rational point, then all the other rational points on this curve are in bijective correspondence with the rational points of a certain curve C_2 in Weierstrass form with the exception of no more than three rational points on C_2.*

Let us illustrate this theorem in the case of the curve

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

1) Construct the tangent at the rational point $(1, 1)$. It has the equation $x + 2y = 3$ and intersects the curve in one more point, namely $(-5, 4)$.

2) Introduce new coordinates $X = x + 2y - 3$, $Y = y - 4$ (the point $(-5, 4)$ is now the origin of the new coordinates, and the tangent is the new Y-axis). Now introduce the variable $u = Y/X$. In the new coordinates, the curve is determined by the equation

$$x^3(1 - 6u + 12u^2 - 6u^3) + x^2(-15 + 60u - 36u^2) + x(75 - 54u) = 0.$$

Let f_1, f_2, f_3 denote the coefficients at x, x^2, x^3, respectively (thus f_1, f_2, f_3 are polynomials in u of degrees 1, 2, 3, resp.).

3) After cancelling out x and multiplying by $4f_3$, we arrive at the equation

$$4x^2 f_3^2 + 4x f_3 f_2 + 4 f_3 f_1 = 0,$$

or bringing out an exact square,

$$(2xf_3 + f_2)^2 = f_2^2 - 4f_1f_3.$$

A simple calculation shows that

$$f_2^2 - 4f_1f_3 = -75 + 216u - 216u^2 + 72u^3$$

(note that a magic cancellation of all the terms containing u^4 has occurred!). Introduce the variable $s_1 = 2xf_3 + f_2$. Our equation is then close to Weierstrass form:

$$s_1^2 = -75 + 216u - 216u^2 + 72u^3.$$

After the change $u = u_1 + 1$, we obtain $s_1^2 = -3 + 72u_1^3$. And, finally, the change $9s_1 = s$, $18u_1 = t$ gives us the following equation in Weierstrass form:

$$s^2 = t^3 - 243.$$

28. Verify that the rational points on the curve $x^3 + 2y^3 = 3$, except the point $(1, 1)$ correspond to the rational points of the new curve $s^2 = t^3 - 243$. Note that the point $(1, 1)$ "moves away to infinity" on the new curve; since the equation $f_3 = 0$ has no rational roots, it follows that the set of exceptional points from Nagell's Theorem is empty. What point corresponds to the point $(-5, 4)$?

29*. Prove that the method described above allows to bring to Weierstrass form any nonsingular curve containing at least one rational point which is not necessarily an inflection point. (We recommend returning to this problem after reading the next section.)

A third order nonsingular curve is called an *elliptic curve*. In number theory problems, it is natural to consider elliptic curves given by equations with rational coefficients and containing a rational point, and this is what we will do in what follows (such curves are usually called elliptic curves over the field of rational numbers).

As we have just explained, such a curve can be transformed to Weierstrass form by a coordinate change with rational coordinates.

30. If the discriminant $\Delta = 4a^3 + 27b^2$ of the curve

$$y^2 = x^3 + ax + b$$

equals zero, the curve is rational.

The converse is also true: if $\Delta \neq 0$, then the curve

$$y^2 = x^3 + ax + b$$

is not rational, but this is already a rather difficult theorem.

31*. Under what conditions can the curve given by the equation $y^2 = x^3 + a_1x + b_1$ be transformed into the curve given by $y^2 = x^3 + a_2x + b_2$ by a projective change of coordinates?

Addition of points on an elliptic curve

Thus, problems **A**–**C** are equivalent to finding all the points with integer coordinates on elliptic curves, whereas problem **D** requires finding all the points with *rational* coordinates on an elliptic curve.

It turns out that for an arbitrary elliptic curve, the problem of finding rational points in some sense is easier, than finding integer points on the same curve! This is because the method of secants allows us to introduce a certain structure on the set of rational points of an elliptic curve. Namely, rational points of an elliptic curve can be "added".

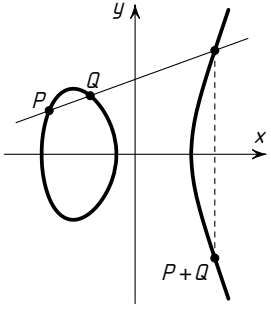


Fig. 7

Suppose that we have found two rational points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ on the elliptic curve $y^2 = x^3 + ax + b$ (Fig. 7). Let us construct the line PQ and find the coordinates of the third intersection point of the line with our curve[1]). These coordinates satisfy the system of equations

$$\begin{cases} y^2 = x^3 + ax + b, \\ (y - y_P)(x_Q - x_P) = (x - x_P)(y_Q - y_P). \end{cases}$$

If $x_P \neq x_Q$ and $y_P \neq y_Q$, then, expressing x in terms of y from the second equation, let us substitute the obtained expression into the first equation. As the result, we arrive at a cubic equation in y with rational

[1]) Generally speaking, not all lines intersect our curve in exactly three points. In some cases (Fig. 12, *a*–*d*), the line intersects the curve in less than three points. There are different ways of overcoming this difficulty, but we will come to that later.

coefficients. Since two roots of this equation are rational (they are y_P and y_Q), while the sum of all three roots is rational (by Vieta's Theorem), it follows that the third root is also rational[1]). Thus, from two rational points on an elliptic curve, we have constructed a third rational point on it. One more rational point is obtained from the constructed one by symmetry in the x-axis. This symmetric point is called the *sum* of the points P and Q and is denoted by $P + Q$ (see Fig. 7).

It is remarkable that the addition of points of an elliptic curve satisfies the properties of the addition of numbers, namely:

a) commutativity (for any points P and Q, we have the identity $P + Q = Q + P$);

b) existence of zero (a point $\mathbf{0}$ such that $P + \mathbf{0} = P = \mathbf{0} + P$);

c) existence for any point P of the elliptic curve of an opposite point (a point $-P$ such that $P + (-P) = \mathbf{0} = (-P) + P$;

d) associativity (for any points P, Q, and R of the elliptic curve, we have the identity $(P + Q) + R = P + (Q + R)$).

Let us check these properties.

Commutativity. To calculate $Q + P$, we use the same line as for the calculation of $P + Q$.

Existence of zero and of the opposite point. Suppose that the curve contains a point P (Fig. 8). We intend to find a point such that the line passing through it and the point P intersects the curve at a point whose reflection in the X-axis turns out to be the starting point P. Let us denote by Q the point symmetric to P with respect to the x-axis. It follows from the above that the line must pass through the points P and Q, i.e., the line must be vertical. Therefore, the point $\mathbf{0}$ must lie on both on the curve and on any vertical line intersecting the curve.

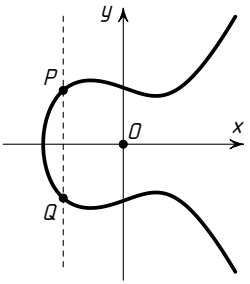


Fig. 8

[1]) If $x_P \neq x_Q$ and $y_P = y_Q$, then the equation of the line PQ is $y = y_P$ and, substituting $y = y_P$ into the first equation, we obtain a cubic equation in x with rational coefficients. Thus everything is all right in this case as well.

There is no such point on the plane. We need it very badly, so we will add it to the plane, call it the *point at infinity*, and denote it by ∞. We will assume that ∞ is the intersection point of *all* vertical lines. Thus, although we added the point $\mathbf{0} = \infty$ formally, we know that any line passing through ∞ and Q is the vertical line passing through Q[1]).

It is reasonable to consider the point $\mathbf{0}$ as being rational.

The vertical line passing through the point P goes through the point $\mathbf{0} = \infty$. Therefore Q, the intersection point of that line with the curve satisfies the relation $P + Q = \mathbf{0}$, i.e., is the point opposite to P. Therefore, any point P has the opposite point $Q = -P$ symmetric to P with respect to the x-axis. Note that for points P lying on the x-axis, we have $-P = P$.

Associativity. Let us choose points P, Q, R on our elliptic curve (Fig. 9). Construct the intersection points $-P - Q$ and $-R - Q$ of the lines PQ and RQ with the curve, as well as the points $P + Q$ and $R + Q$. To prove the equality $(P + Q) + R = P + (Q + R)$, it suffices to show that the intersection point of the line passing through the points $P + Q$ and R with the line passing through the points P and $Q + R$ lie on our curve.

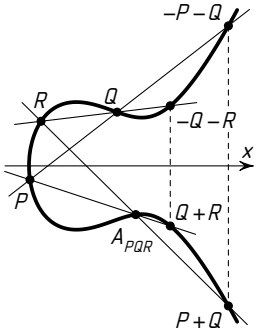


Fig. 9

We obtain a configuration of six lines $l_1, l_2, l_3, m_1, m_2, m_3$ that pass through the points Q and R, $-P - Q$ and $P + Q$, P and $Q + R$, P and Q, $-R - Q$ and $R + Q$, R and $P + Q$, respectively. This configuration is schematically represented in Fig. 10. Each of these six lines passes through three points (the line passing through $-R - Q$ and $R + Q$ and the line passing through $-P - Q$ and $P + Q$ both pass through the point $\mathbf{0} = \infty$), so there are nine intersection points in the configuration. We know that eight of these points lie on the the elliptic curve E given by the

[1]) Now we already know what to do in the situation shown in Fig. 12a below. The vertical line has three common points with the curve P, Q, ∞.

equation $F(x, y) = 0$. We shall prove that the nineth point A_{PQR} also lies on this curve. Suppose the equations of the lines $l_1, l_2, l_3, m_1, m_2, m_3$ are

$$L_1(x, y) = 0 \quad L_2(x, y) = 0 \quad L_3(x, y) = 0$$
$$M_1(x, y) = 0 \quad M_2(x, y) = 0 \quad M_3(x, y) = 0.$$

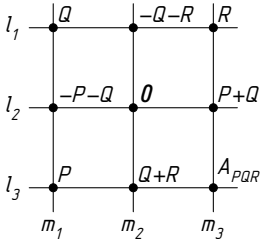


Fig. 10

Let us show that

$$F(x, y) = \alpha L_1(x, y)L_2(x, y)L_3(x, y) + \beta M_1(x, y)M_2(x, y)M_3(x, y),$$

where α and β are some numbers. Consider the difference

$$F - (\alpha L_1 L_2 L_3 + \beta M_1 M_2 M_3). \tag{7}$$

The above difference is a polynomial in x and y of degree no greater than three. This polynomial vanishes at the points P, $-P - Q$, and Q. On the line m_1, let us choose one more point $S = (s_1, s_2)$ that differs from P, $-P - Q$, and Q. The point S does not lie on any of the lines l_1, l_2, l_3 and, therefore,

$$L_1(s_1, s_2) \neq 0, \ L_2(s_1, s_2) \neq 0, \ L_3(s_1, s_2) \neq 0, \text{ but } M(s_1, s_2) = 0.$$

Let us substitute the coordinates of the point S into the difference (7) and find α from the equation

$$F(s_1, s_2) - \alpha L_1(s_1, s_2)L_2(s_1, s_2)L_3(s_1, s_2) = 0.$$

For this choice of α, the difference (7) will vanish at four points P, Q, $-P - Q$, and S of the line m_1.

32. Suppose that a polynomial $F_1(x, y)$ of degree no greater than three vanishes at four points of some line $M(x, y) = 0$. Then the polynomial F_1 is divisible by the polynomial M.

Thus we have chosen the parameter α so that the difference (7) is divisible by M_1. Considering the points Q, $-Q - R$, and R of the line l_1, let us choose as above the parameter β so that the difference (7) will be divisible by L_1. We see that expression (7) can be represented in the form $L_1(x, y)M_1(x, y)N(x, y)$, where $N(x, y)$ is a polynomial of

degree no greater than one. If this degree equals one, then the equation $N(x, y) = 0$ determines a certain line n.

Thus we have $F - (\alpha L_1 L_2 L_3 + \beta M_1 M_2 M_3) = L_1 M_1 N$. Let us substitute the coordinates of the point $P + Q$ into this equality. On the left-hand side, we get zero. If neither L_1 nor M_1 vanish, then $N = 0$, and this means that the point $P + Q$ lies on the line n. Similarly, we conclude that the point $Q + R$ lies on n. If ∞ were an ordinary point, we could prove in the same way that it also lies on n.

33. Suppose the lines l_1 and m_1 are not vertical. Prove that in that case the line n is vertical.

Obviously, in the general case the fact that the lines l_1 and m_1 are not vertical does not imply that the line passing through the points $P+Q$ and $Q+R$ is vertical. Therefore the polynomial N is of degree zero, i.e., is a constant. But N vanishes at the point $P + Q$, hence it is identically zero. Thus,

$$F(x, y) = \alpha L_1(x, y) L_2(x, y) L_3(x, y) + \beta M_1(x, y) M_2(x, y) M_3(x, y),$$

And the point A_{PQR} whose coordinates are determined from the system of equations

$$\begin{cases} L_3(x, y) = 0, \\ M_3(x, y) = 0. \end{cases}$$

lies on the line $F(x, y) = 0$.

Thus we have proved the associativity of the sum operation for points of an elliptic curve under certain additional assumptions, namely: none of the points in Fig. 10 coincide; the lines l_1 and m_1 do not pass through the points $P + Q$ and $Q + R$; the line passing through the points $P + Q$ and $Q + R$, as well as the lines l_1 and m_1, are not vertical. Each of these cases may be considered separately, but we can argue differently: note that the coordinates of the points $(P + Q) + R$ and $P + (Q + R)$ depend *continuously* on the coordinates of the points P, Q, R. We have established the equality $(P + Q) + R = P + (Q + R)$ for all sufficiently general collections P, Q, R. By continuity, this implies that the equality always holds (of course, to make this argument rigorous, we must define the notions used in it: "continuity" and "sufficiently general collections", but here we only give an idea of the proof).

* * *

How can we calculate the point $P + P = 2P$? When the two points were distinct, we constructed the line passing through them, and so on. Since the points have merged, we should construct the tangent (Fig. 11). And what must we do to calculate $3P$? That's very easy, we simply take the sum of $2P$ and P. Similarly, we can calculate $4P = 3P + P$, $5P = 4P + P$, etc.

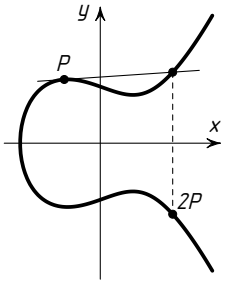


Fig. 11

34. Let $P = (x_0, y_0)$ be a point of the curve $y^2 = x^3 + ax + b$. Compute the coordinates of the point $2P$.

The time has come to explain what to do in the situations arising in Fig. 12, *b*–*d* (see the footnotes in pages 22 and 24). In the situation d), when the tangency occurs at an inflection point, we assume that the line l also has three intersection points with the curve, but these three points have merged together. In the situation with "simple" tangency (*b* and *c*), the point P is counted twice, and, in particular, in case *c*, the line l passes through ∞.

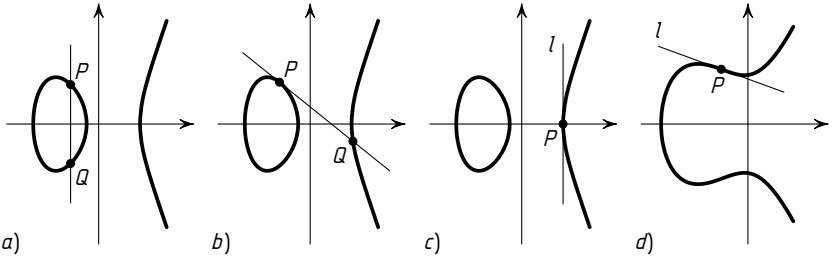


Fig. 12

Thus any line passing through at least one point of an elliptic curve other than ∞, intersects the curve in three points. The sum of these three points is always equal to 0 (check this!).

In view of these remarks, we see that the sum of *any* two points of an elliptic curve is defined. It remains to show that now the sum operation still possesses the properties a)–d) of addition, see p. 23.

Torsion and rank

Let P be a point on an elliptic curve. Starting from it, we can construct the points $\ldots$, $-3P$, $-2P$, $-P$, $\mathbf{0}$, P, $2P$, $3P$, $\ldots$ If the point P was rational, then all these points will be rational. There are two "models of behaviour" of the point P: either all those points are

distinct, or among them there are coinciding ones. In the latter case, suppose that $mP = nP$, $m > n$. According to the rules of addition, we immediately see that $(m-n)P = \mathbf{0}$, i.e., there exists a positive integer k_1 such that $k_1 P = \mathbf{0}$. Let k be the smallest such positive number. The number k is called the *order* of the point P, and the point P itself is said to be a *torsion point* (or a *point of finite order*). Note that according to this definition, the point $\mathbf{0}$ is a torsion point of order 1. In case of the first "model of behaviour", we say that P is a point of infinite order.

35. Let P be a point of order k. Prove that among all the points ..., $-3P$, $-2P$, $-P$, $\mathbf{0}$, P, $2P$, $3P$, ... there are exactly k different points.

36. Prove that the sum of two torsion points is also a point of finite order.

37. Let P be a point of order k. What is the order of nP, where n is an integer?

38. Find all the points of order 2 on the elliptic curve $y^2 = x^3 + ax + b$. When are these points rational? Find the points of order 2 on the elliptic curves in problems **A**–**D**.

39. Find all the points of order 3 on the elliptic curves in problems **A**–**D**.

40*. What geometric property do the points of order 3 of an elliptic curve possess? How many points of order 3 (not necessarily rational) on an elliptic curve may there be?

It is remarkable that any elliptic curve has only a finite number of rational torsion points (try to prove this — the authors know no simple solution!). Moreover, as was established by Barry Mazur, for the number t of rational points of finite order, only the following values are possible: $0 \le t \le 10$, $t = 12$, and $t = 16$.

Now let us see how two points P and Q of infinite order can behave. Here there are also two possible "models of behaviour": either all the points $mP + nQ$, $m, n \in \mathbb{Z}$, or there are coinciding ones. In the first case we say that the points P and Q are *linearly independent*, in the latter case, *linearly dependent*. This definition can be generalised: we say that points $P_1, P_2, \ldots, P_n$ are linearly independent if all the points

$$m_1 P_1 + m_2 P_2 + \ldots + m_n P_n, \quad m_1, m_2, \ldots, m_n \in \mathbb{Z},$$

are distinct. The remarkable Mordell Theorem asserts that for any elliptic curve there exists a nonnegative integer n such that any $n+1$ points rational points of the curve are linearly dependent. The smallest such number is called the *rank* of the elliptic curve.

41. An elliptic curve has infinitely many rational points if and only if its rank is positive.

Mordell's Theorem. *Let E be an elliptic curve. Then there exists a collection of rational points $P_1, P_2, \ldots, P_n$ on the curve such that any of its rational points can be expressed in the form*

$$P = a_1P_1 + a_2P_2, \ldots a_nP_n + Q,$$

where $a_1, a_2, \ldots, a_n$ are integers uniquely determined by the point P, while Q is a certain rational torsion point.

In other words, all rational points on an elliptic curve can be obtained from a finite number of such points by constructing secant and tangent lines.

The rank of the curve E is equal to the smallest possible value of n from Mordell's Theorem.

Let us look at our examples from the point of view of torsion and rank[1]).

A. The curve $y^2 = x^3 - 9x + 81$ has no torsion (i.e., the point **0** is the unique rational torsion point on that curve). The rank of the curve is 2. In the role of the points P_1 and P_2 from Mordell's theorem, we can take the points $(-3, 9)$ and $(0, 9)$.

B. The curve $y^2 = x^3 - 36x$ has exactly four rational torsion points: the point **0** and three other points of order two. Its rank is 1, and for P_1 we can take the point $(-2, 8)$.

C. The curve $y^2 = x^3 - x + 1/4$ has no torsion. Its rank is 1 and for P_1 we can take the point $(0, 1/2)$.

D. Fermat's curve $y^2 = x^3 - 1/108$ has exactly three rational torsion points: the point **0** and two other points of order three. Its rank is 0. Obviously, this statement is equivalent to Fermat's Last Theorem with exponent 3.

E. The curve $s^2 = t^3 - 243$ has no torsion. Its rank is 1; for P_1 we can take the point $(10, 7)$.

To show the reader how deeply we have penetrated in the jungle of contemporary number theory, note that the answer to the following question is presently unknown to humanity.

The Rank Problem. Can the rank of an elliptic curve be as large as we wish?

At present there are examples of curves of rank up to 24. The answer to the above problem is expected to be positive.

Integer points on elliptic curves

Even if we suppose that the results of the previous section are known, we cannot say that we have solved our original problems **A**–**C**. In all of

[1]) We must admit that finding torsion points and calculating the rank of our curves are difficult and non elementary problems.

them we have found infinitely many rational solutions, but in the original formulations *integer* solutions were required. How can one distinguish them among the infinite set of rational points? In the same article which contained the theorem from the previous section, Louis Joel Mordell proved that any elliptic curve contains only a finite number of integer points. However that assertion does not help us in actually *finding* these points.

The curve $y^2 + y = x^3 - x$ from problem C consists of two pieces: an oval and an infinite arc (Fig. 13). The point $P_1 = (0, 0)$ lies on the oval. All the integer solutions may be found by solving problem 42.

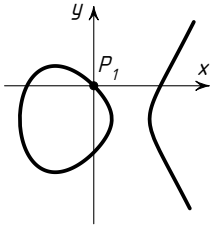


Fig. 13

42. a) Find all the integer points on the oval.

b) Prove that points nP_1 with odd n lie on the oval, those with even n, on the arc.

c) Check that if a prime number p divides the denominators of both coordinates of the point nP_1, then p divides the coordinates of the point $2nP_1$ (it is assumed that all coordinates are represented by non cancellable fractions).

d) Find all the integer points on the curve $y^2 + y = x^3 - x$.

43. Find all the integer points on the curve $y^2 = x^3 - 36x$ and solve problem **B**.

As we have seen, we were helped by the fact that the curve under consideration consists of two pieces. This is not the case in problem **A**. Nevertheless, in that case it is possible to show that all integer points of the curve are of the form $aP_1 + bP_2$, where $|a|, |b| \leq 13$, and then solve the problem by means of a finite exhaustive search (accessible to our computer, but not to the authors). The integer points have the following abscissas $-5, -3, 0, 3, 7, 9, 24, 33, 39, 513, 1099, 5112$. Using this, one can find all the pairs (m, n): (1,1), (10,5), (13,6), (645,85). The first three of these can be found by brute force; but to get to the fourth pair without the help of a computer is outside the possibility of humans.

An even more remarkable example of this kind is that of the curve $y^2 = x^3 + 24$. After a bit of thinking, we can come up with the following

"small" solutions:

$$P_1 = (-2, 4), \qquad 4^2 = (-2)^3 + 24$$
$$P_2 = (1, 5), \qquad 5^2 = 1^3 + 24$$
$$P_3 = (10, 32) \qquad 32^2 = 10^3 + 24$$

At first glance, it seems that there are no other solutions (with $y > 0$). But no, there is a fourth one:

$$P_4 = P_1 + 2P_2 = (8158, 736\,844).$$

Note that $P_3 = P_1 - P_2$ and that the rank of this curve is 2; moreover, any rational point P of the curve $y^2 = x^3 + 24$ may be represented in the form $P = aP_1 + bP_2$, where a and b are integers.

CONGRUENT NUMBERS

Let us return to the very first problem in this book. Suppose that three rational numbers X, Y, Z are the lengths of the sides of a right triangle. Although we derived formulae (3'–4') only for integer solutions of the equation $X^2 + Y^2 = Z^2$, they are actually valid for all rational solutions — one must only allow r to run over all rational values.

A rational number s is called *congruent* if there exists a right triangle of area s with rational side lengths.

The following natural question arises: how can one find out whether a given number is congruent? The problem of describing all congruent numbers leads to deep and meaningful algebraic geometry theorems and conjectures. We know the answer in a way, but at present are unable to justify it fully. However, for some rational numbers, it is known (and has been proved) that they are congruent and for some that they are not.

For example, the area of the Egyptian triangle (with sides 3,4,5) is $(3 \cdot 4)/2 = 6$, so 6 is a congruent number. It is slightly more difficult to prove that 5 is congruent: check that the area of a triangle with sides $3/2$, $20/3$, $41/6$ is equal to 5.

|| **44*.** (Euler). *Prove that* 7 *is a congruent number.*

Now note that if a number s is congruent, then so is the number sl^2 for any rational l, because the triangle of area sl^2 is obtained from a triangle of area s by increasing all its sides l times. Since $m/n = mn(1/n^2)$, in what follows we can restrict our considerations to integers. For the same reason we will consider only square free integers.

Fermat's Theorem. *The integer* 1 *is not a congruent number.*

Proof. Assume the converse — let 1 be a congruent number. This means that there is a right triangle with integer sides a, b, x (x is the

length of the hypothenuse) whose area is $ab/2 = y^2$, y being an integer (clearly, one can choose a and b so that only one of them is even). Let us transform the expression $x^4 - 16y^4$ as follows

$$x^4 - 16y^4 = (x^2 - 4y^2)(x^2 + 4y^2) = (x^2 - 2ab)(x^2 + 2ab)$$
$$= (a^2 + b^2 - 2ab)(a^2 + b^2 + 2ab) = (a - b)^2(a + b)^2.$$

Thus, if 1 is a congruent number, then the equation $x^4 - (2y)^4 = u^2$ has a positive integer solution (the number u being odd). Among all the nonzero solutions with odd u, let us choose the solution (x_0, y_0, u_0) for which $|u|$ is minimal.

The numbers x_0, y_0, and u_0 are pairwise coprime: if two of them had a common prime divisor p, then the third one would be divisible by p (actually the number u_0 would even be divisible by p^2), and then for the solution $(x_0/p,\ y_0/p,\ u_0/p^2)$ the value of $|u|$ would be less.

Applying formula (4) to the equality $x_0^4 = (2y_0)^4 + u_0^2$, we obtain

$$x_0^2 = m^2 + n^2, \quad (2y_0)^2 = 2mn$$

(in our case, the numbers x_0^2, $(2y_0)^2$, and u_0 are pairwise coprime and $(2y_0)^2$ is even); here m and n are pairwise coprime and we may assume that one of them (say n) is even. It follows from the equality $(2y_0)^2 = 2mn$ that $m = m_1^2$ and $n = 2n_1^2$. Further, the equality $x_0^2 = m^2 + n^2$ implies

$$x_0 = m_2^2 + n_2^2, \quad n = 2m_2n_2 = 2n_1^2, \quad m = m_2^2 - n_2^2 = m_1^2,$$

where m_2 and n_2 are also pairwise coprime and we may assume that one of them is even; it follows from the last equality that n_2 is even. We obtain:

$$m_2 = m_3^2, \quad n_2 = n_3^2, \quad m_3^4 - n_3^4 = m_1^2.$$

But since n_3 is even, it follows that $(m_3, n_3/2, m_1)$ is an integer solution of the equation $x^4 - (2y)^2 = u^2$ with a value of $|u|$ smaller than $|u_0|$:

$$|u_0| = |m^2 - n^2| \geq 2m - 1 = 2m_1^2 - 1$$

and

$$|m_1| \leq \sqrt{\frac{|u_0| + 1}{2}} < |u_0| \quad \text{for} \quad |u_0| > 1.$$

The case $|u_0| = 1$ is trivial.

The theorem is proved.

The argument used above is known as the *method of infinite descent* and helps solving many number theory problems.

45. (Fermat's Last Theorem with exponent equal to 4). The equation $x^4 + y^4 = z^4$ has no positive integer solutions.

Congruent numbers and elliptic curves

It is remarkable that the problem of establishing the congruence numbers is equivalent to the problem of finding the rank of certain elliptic curves. Let s be a congruent number, i.e., let s be the area of a right triangle with sides a, b and hypotenuse c, $c^2 = a^2 + b^2$, $s = ab/2$ (we assume that s is a square-free integer). To the number s, let us assign the elliptic curve E_s given by the equation

$$y^2 = x^3 - s^2 x = (x - s)x(x + s).$$

Let us substitute $x = (c/2)^2$ into that equation:

$$\begin{aligned} y^2 &= \big((c/2)^2 - ab/2\big)(c/2)^2\big((c/2)^2 + ab/2\big) \\ &= \big((c^2 - 2ab)/4\big)(c/2)^2\big((c^2 + 2ab)/4\big) \\ &= \big((a - b)/2\big)^2(c/2)^2\big((a + b)/2\big)^2 \end{aligned}$$

Thus

$$P = (x, y) = \Big(\frac{c^2}{4}\,,\ \frac{a-b}{2} \cdot \frac{c}{2} \cdot \frac{a+b}{2}\Big)$$

is a rational point.

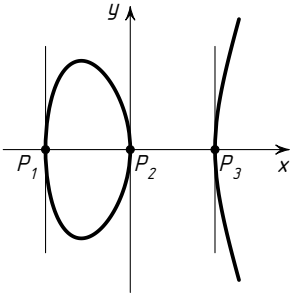


Fig. 14

The rational points $P_1 = (-s, 0)$, $P_2 = (0, 0)$, and $P_3 = (s, 0)$ also lie on the curve E_s. These three points are all of order 2, because the tangents at these points are vertical (Fig. 14). It turns out that the following theorem holds:

Theorem I. *There are exactly four rational points of finite order on the curve E_s: the point* **0** *and three points of order* 2.

This is a very difficult theorem. In its proof, which we present in Supplement 1, we use the arithmetic of residues modulo p and an important theorem due to Dirichlet about prime numbers in arithmetical progressions, which we do not prove.

Note that the curve E_6 coincides with the curve in problem **B**. Thus, we have calculated the torsion on that curve as well.

Theorem I implies that the point P that we have found is of infinite order. Moreover, we have the following

Theorem II. *A number s is congruent if and only if the curve E_s contains a rational point of infinite order.*

Proof. We already know that if s is congruent, then the curve E_s contains a point P of infinite order. However, that point is very special: its coordinate x is the square of a rational number. Thus, in order to prove Theorem II, we must learn to construct, starting from an *arbitrary* point Q of infinite order on E_s, a right triangle of area s.

At first we will work "backwards": given a right triangle of area s, sides a, b, and hypotenuse c, we will construct one more point on the curve E_s. As we have shown previously, there exists a rational number t such that

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

Since $s = ab/2$, it follows that

$$\frac{s}{c^2} = \frac{ab}{2c^2} = \frac{t(1-t^2)}{(1+t^2)^2}$$

Therefore,

$$\left(\frac{s^2(1+t^2)}{c}\right)^2 = s^3t(1-t^2) = st(s-st)(s+st)$$

so that the rational point $Q = (-st, s^2(1+t^2)/c)$ lies on the curve E_s. According to Theorem I, this point is of infinite order (since its y-coordinate is nonzero).

Conversely, let $Q = (x, y)$ be a rational point of infinite order on our curve. Then $y \neq 0$ (otherwise it would be one of the points of order 2), hence $x \neq 0$ and $x \neq -s$. Let us put:

$$t = -\frac{x}{s}, \; c = \left|\frac{s^2(1+t^2)}{y}\right|, \; a = \left|\frac{2t}{1+t^2}c\right|, \; b = \left|\frac{1-t^2}{1+t^2}c\right|.$$

46. Show that the numbers a, b, c are positive, rational, and satisfy the equations $a^2 + b^2 = c^2$ and $ab/2 = s$.

Theorem II is proved.

* * *

It is interesting to find out how the points P and Q are related. The next problem gives the answer.

47. Prove that $2Q = -P$.

Note that Theorem II, together with the Fermat theorem proved in the previous section, implies that the rank of the curve E_1 given by the equation $y^2 = x^3 - x$ is zero.

Congruent numbers: the answer

The problem of describing congruent numbers was known to the ancient Greeks, but the answer to this problem was stated only in the 20th century. Indeed, only in 1980s a surprising criterion for finding out if a given arbitrary integer is congruent or not was discovered.

Tunnell's Criterion. *An odd positive square-free integer n is congruent if and only if the number of integer solutions of the equation*

$$n = 2x^2 + y^2 + 32z^2$$

is equal to half of the number of integer solutions of the equation

$$n = 2x^2 + y^2 + 8z^2.$$

An even positive square-free integer n is congruent if and only if the number of integer solutions of the equation

$$\frac{n}{2} = 4x^2 + y^2 + 32z^2$$

is equal to half of the number of integer solutions of the equation

$$\frac{n}{2} = 4x^2 + y^2 + 8z^2.$$

Note that for a given n, the number of solutions of each of these equations is easy to find, e.g. by exhaustive search.

Let us consider some examples. For $n = 1$, both of the corresponding equations have two solutions $(0, \pm 1, 0)$. Therefore, the number 1 is not congruent. For $n = 2$, both of the corresponding equations also have two solutions each, so the number 2 is not congruent either. The number $n = 34$ behaves differently. The equation $17 = 4x^2 + y^2 + 32z^2$ has four solutions $(\pm 2, \pm 1, 0)$, while the equation $17 = 4x^2 + y^2 + 8z^2$ has eight $(0, \pm 3, \pm 1)$, $(\pm 2, \pm 1, 0)$. In that case, Tunnell's Criterion asserts that there exists a right triangle of area 34 with rational sides. This is indeed true: the lengths of the sides of one such triangle are $136/15$, $15/2$, and $353/30$.

Unfortunately, Tunnell's Criterion has not been completely proved. At present, we only know that if a number n is congruent, then the corresponding conditions about the number of solutions hold. The converse statement follows from a general conjecture concerning elliptic curves due to Birch and Swinnerton-Dyer. This conjecture relates the rank of an elliptic curve with the number modulo p of its rational points for all

prime p. (Computations have shown that if $n \leq 10\,000$ and n satisfies Tunnell's conditions, then it is indeed congruent.) In order to appreciate the Birch and Swinnerton-Dyer conjecture (and the non proved part of Tunnell's Criterion that follows from it), consider an example.

48. Verify that the number 157 satisfies Tunnell's conditions.

Thus we can assume that the number 157 is congruent. This is indeed the case, however the hypothenuse of the simplest right triangle of the area with rational sides is expressed by a fraction with a numerator that has 48 digits! (Fig. 15)!

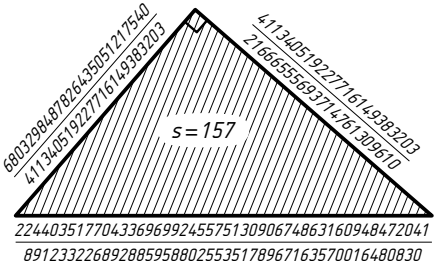


Fig. 15

49. Prove that all square-free integers that have remainders 5, 6, or 7 when they are divided by 8 satisfy Tunnell's conditions.

On the contrary, it has been proved that prime numbers that have the remainder 3 when divided by 8 do not satisfy Tunnell's conditions and therefore cannot be congruent.

50*. Split the numbers from 1 to 100 into those that do not satisfy Tunnell's conditions (and so are not congruent) and those that do (and so are conjecturally congruent). For the latter, try to find the corresponding right triangles.

ADDENDUM 1
PROOF OF THEOREM I

Assume that the curve E_s possesses, besides the points $\mathbf{0}$, P_1, P_2, P_3, some other rational points.

51. Prove that in this case the curve E_s has either a rational point of odd prime order r or a rational point of order 4.

52. Points of order 3 and 4 on the curves E_s have irrational coordinates.

Thus we can assume that the curve E_s has a point of odd prime order $r \neq 3$.

Now let us choose a prime number p such that the denominators of the coordinates of the point P and of the number s are not divisible by p. Consider the set $\widetilde{E}_s(p)$ of pairs (x, y) of remainders under division by p such that $y^2 - x^3 + s^2x$ is divisible by p. Add the point $\mathbf{0}$ to the set $\widetilde{E}_s(p)$ and denote

$$E_s(p) = \widetilde{E}_s(p) \cup \{\mathbf{0}\}.$$

The key observation is that the set $E_s(p)$ also possesses a sum operation. This is because the sum operation for rational points on the curve E_s is given my means of certain algebraic formulae that express the coordinates of the sum in terms of the coordinates of the summands. We did not write out these formulae, they are fairly complicated; what is important at this stage is that such formulae exist. These same formulae are valid for the arithmetic of remainders modulo p: in that arithmetic, we also know how to add, subtract, multiply and divide! The properties of addition — commutativity, associativity — reduce to certain algebraic identities and so remain valid for the addition of points "modulo p". Thus there is a sum operation on $E_s(p)$ possessing all the properties of ordinary addition. With respect to that operation, all the elements of $E_s(p)$ are torsion points because the set $E_s(p)$ itself is finite. Note that this construction does not work in the case when s is divisible by p, for the same reason as that there is no addition on singular third order curves: the singular point $(0, 0)$ interferes.

Consider the point P "modulo p": let us replace the numerators and denominators of its coordinates by their remainders modulo p and carry out the division in the arithmetic modulo p. We obtain an element $\overline{P}$ of the set $E_s(p)$.

Note that $r\overline{P} = \mathbf{0}$. Indeed, the fact that $rP = \mathbf{0}$ on the curve E_s is expressed by certain algebraic identities relating the coordinates of the point P. Obviously, the same algebraic identities are valid modulo p for the coordinates of the point $\overline{P}$. But according to our definition of addition on the set $E_s(p)$ this means precisely that $r\overline{P} = \mathbf{0}$.

53. Prove that the order of the point $\overline{P}$ is r.

Thus we have constructed the set $E_s(p)$ supplied with a sum operation[1]) and a point $\overline{P}$ of order r lying on it. The next important observation is that the number of elements of $E_s(p)$ is divisible by r.

[1]) The set $E_s(p)$ with the addition operation defined above is an example of a *finite Abelian group*. An *Abelian group* is a set with an addition operation possessing properties a)—d), see p. 23.

Indeed, let us split the set $E_s(p)$ into equivalence classes in the following way: we will say that two points $Q_1, Q_2 \in E_s(p)$ are equivalent if $Q_1 - Q_2 = m\overline{P}$ for some integer m.

54. Check that if Q_1 is equivalent to Q_2 and Q_2 is equivalent to Q_3, then Q_1 is equivalent to Q_3 and Q_2 is equivalent to Q_1.

55. Prove that each equivalence class contains exactly r elements of $E_s(p)$.

If q is the number of equivalence classes, then the number of elements in $E_s(p)$ is qr and, in particular, is divisible by r. In order to come to a contradiction, it is expedient to learn how to calculate the number of elements of $E_s(p)$. It turns out that this is easy to do for "about one half" of all prime numbers.

56*. Let the remainder of the division of p by 4 be 3. Show that the number of elements in $E_s(p)$ is $p + 1$.

Thus we have shown that r divides any number $p + 1$, where p is a prime of the form $4k + 3$ that does not divide s or any denominator of the coordinates of P. This already seems highly unlikely, since there are infinitely many prime numbers of the form $4k + 3$ and it would be surprising if all of them, except a finite number, would become divisible by a fixed prime after the addition of 1. However, in order to give a rigorous proof of the impossibility of such a phenomenon, we will have to use the following remarkable theorem due to Dirichlet.

Dirichlet's Theorem. *Every arithmetical progression whose initial term and difference are coprime integers contains infinitely many prime numbers.*

57. Prove that there exist infinitely many primes of the form a) $4k+3$, b) $6k + 5$, c)* $4k + 1$, d)* $6k + 1$.

In particular, since $r \neq 3$, there are infinitely many primes of the form $p = 4kr + 3$, where k is an integer. But $p + 1 = 4rk + 4$, which is obviously not divisible by r. This contradiction proves Theorem I.

ADDENDUM 2
FERMAT'S LAST THEOREM AND EULER'S PROBLEM

At the beginning of this book, we described all the positive integer solutions of the equation $X^2 + Y^2 = Z^2$. That problem was studied by mathematicians since antiquity. In the 17th century, Pierre Fermat claimed that the equation

$$X^n + Y^n = Z^n$$

has no solution for $n \neq 3$[1]). What is more, Fermat believed that he could prove this. For more than three centuries, many scientists tried to prove that claim, which became known as Fermat's Last Theorem. These attempts turned out to be extremely beneficial, thanks to them a large part of contemporary number theory came into being. But Fermat's theorem continued to resist. The bastion fell under the united efforts of numerous outstanding mathematicians from the whole world. Recently, the problem obtained its final solution in the work of Andrew Wiles. The proof uses some very very deep results – from the same theory of elliptic curves.

The proof begins something like this: let $A^n + B^n = C^n$; construct the elliptic curve

$$y^2 = x^3 + (A^n B^n - A^n C^n - B^n C^n)x + A^n B^n C^n.$$

Further, the properties of this curve is studied, and they turn out to be so amazing that no such curves exist.

The great 18th century mathematician Leonard Euler was the first to prove that no positive integer solutions of the equation $X^3 + Y^3 = Z^3$ exist (the three cubes problem) and conjectured that the equations

$$X^4 + Y^4 + Z^4 = T^4, \quad X^5 + Y^5 + Z^3 + U^5 = V^5, \quad \text{etc.},$$

also have no positive integer solutions (the problems of the four fourth degrees, of the five fifth degrees, etc.) These problems staunchly resisted all efforts of solution until computers came to the rescue. At the dawn of the computer era, a counterexample to the five fifth degrees problem was found:

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

The four fourth degrees problem turned out to be much more difficult. The victory was obtained by cleverly combining methods of study of rational and elliptic curves with computer calculations. Noam Elkies obtained a counterexample:

$$2\,682\,440^4 + 15\,365\,639^4 + 18\,796\,760^4 = 20\,615\,673^4.$$

Soon afterwards, a smaller counterexample was found on a more powerful computer:

$$95\,800^4 + 217\,519^4 + 414\,560^4 = 422\,481^4.$$

The idea is, before we study the surface F given by $x^4 + y^4 + z^4 = 1$, to consider the simpler surface $F' = x^4 + y^4 + t^2 = 1$. If F has a rational point (x, y, z), then there is a rational point on F', namely (x, y, t), where $t = z^2$. It turns out that the surface F' can be presented as the union

[1]) Fermat's theorem for exponent 3 was stated already in the 10th century by the Arab mathematician al-Khojandi, a century later Omar Khayyam noted that the problem remains unsolved.

of rational curves, i.e., of plane second order curves. We can do this as follows: we consider the surface F'' given by the equation

$$(u^2+2)v^2 = -(3u^2-8u+6)w^2 - 2(u^2-2)w - 2u.$$

For a fixed u, this determines a rational curve that we denote by F''_u. The replacement

$$x = w+v,\ y = w-v,\ t = u(x^2+xy+y^2+x+y)+1-(x+y)^2$$

transforms the surface F' into the surface F''. Legendre's Theorem (in a somewhat modified form, it is valid for any nonsingular second order rational curve) gives us a necessary and sufficient condition for the existence of a rational point on the curve F''_u. Now let us consider a curve C' that has a rational point. The inverse image C of the curve C' on the surface F is an elliptic curve. We must search for the required points on C. We verify the solvability of the equation determining the curve C in remainders under division by not very large primes. And only if there are solutions for all these prime numbers, we search for the rational solution on the computer. This considerably diminishes the exhaustive search.

It is interesting that the equation $x^4+y^4+z^4 = 1$ has many rational solutions – for any real solution there is a rational one as near to it as we wish.

ADDENDUM 3
PYTHAGOREAN BRICKS

The problem about Pythagorean triangles can be formulated somewhat differently. Let us call a rectangle *Pythagorean* if the lengths X and Y of its sides, as well as the length Z of its diagonal, are positive integers (Fig. 16).

In this formulation, the problem has a natural generalisation. Let us say that a rectangular parallelepiped is a *Pythagorean brick* if its edges X, Y, Z, the diagonals U, V, W of its faces, and its main diagonal T are positive integers (Fig. 17). If T is not necessarily integer, then we say that the parallelepiped is a *weakly Pythagorean brick*.

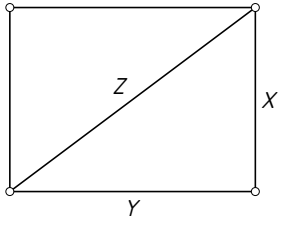


Fig. 16

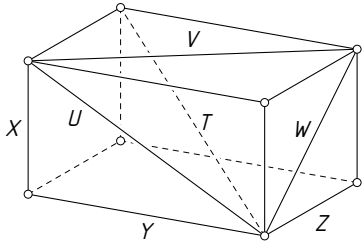


Fig. 17

Here is an example of a weakly Pythagorean brick: $X = 44$, $Y = 117$, $Z = 240$; for it we have $U = 125$, $V = 244$, $W = 267$.

Does there exist at least one Pythagorean brick? How can one describe all weakly Pythagorean bricks? The answer to these questions are at present unknown to humanity.

58. Reformulate these problems in the language of equations. What geometric object corresponds to these equations?

59. Describe all parallelepipeds with integer X, Y, Z, and T.

60. (Euler). Check that for any positive integer $n \geq 2$ the brick with sides

$$X = n^6 - 15n^5 + 15n^2 - 1, \quad Y = 6n^5 - 20n^3 + 6n, \quad Z = 8n^5 - 8n$$

is weakly Pythagorean.

ADDENDUM 4
HOW DIOPHANTUS SOLVED ARITHMETIC PROBLEMS

We are used to solving problems by using equations in which the unknowns are denoted by letters, and the arithmetical operations by symbols. We should, however, remember that modern notation appeared fairly late, only in the 16th—17th centuries. Ancient mathematicians used words only. This is how Diophantus describes the solution of the equation $x^3 + ax^2 = y^2$ (in the column on the right-hand side, the same things are written by using letters and symbols):

"Find a cubic number such that if we add to it a square number with the same side taken several times, we obtain a square number.	Find the (integer) solutions of the equation $x^3 + ax^2 = y^2$.
Assume that the cube has for its side one thing, i.e., there is one cube; assume that the number of times is ten and add to this cube ten times the square of the edge of the cube, which is a square, i.e., we have a cube plus ten squares equal to the square.	Take, for example, $a = 10$.
Assume that this square has for side a thing whose square is more than ten squares so as to make a decrease possible.	In order to have $x^3 > 0$, it is necessary that $y^2 > 10x^2$.
Assume that its side is four things, the square is then sixteen things.	Take $y = 4x$, then $y^2 = 16x^2$.
The cube plus ten squares is then sixteen squares. Subtract ten common squares, six squares remain that equal the cube.	We obtain $6x^2 = x^3$.
Divide it by the	We find $x = 6$.

square, obtaining one thing equal to six units. The cube is two hundred sixteen, the square of its side is thirty six; ten times that last quantity is three hundred sixty. Adding that to the cube, we obtain five hundred seventy six, this being a square whose side is twenty four.

Thus we have found a cubic number such that if to it we add ten times the square of its edge, the result of addition will be a square number; that is two hundred sixteen, i.e., its side is six. Which was required to find.".

Indeed,

$$6^3 = 216,$$
$$6^2 = 36,$$
$$10 \cdot 6^2 = 360,$$
$$6^3 + 10 \cdot 6^2 = 576 = 24^2.$$

Now let us try to reconstruct the general method that was used by Diophantus, which he tried to teach his reader.

Put $y = tx$, where t is an integer. The equation can be rewritten as $x^3 + ax^2 = t^2x^2$, i.e, $x + a = t^2$, $x = t^2 - a$, $y = t^3 - at$ for any t (Diophantus would have additionally required that $x > 0$, $y > 0$, i.e., $t^2 > a$.)

As far as we know, Diophantus did not understand that the equation determines a curve on which we must find integer points. For that one needs the notion of coordinate, which first appeared in the work of Descartes in the 17-th century. But in Diophantus' solution, we immediately discern the construction of lines passing through the singular (0,0) point of curve $y^2 = x^3 + ax$.

ANSWERS, HINTS, SOLUTIONS

3. *Answer*:

(3, 4, 5),	(18,24,30),	(24,45,51),	(39,52,65),	(13,84,85),
(6, 8,10),	(16,30,34),	(20,48,52),	(32,60,68),	(36,77,85),
(5,12,13),	(21,28,35),	(28,45,53),	(42,56,70),	(40,75,85),
(9,12,15),	(12,35,37),	(33,44,55),	(48,55,73),	(51,68,85),
(8,15,17),	(15,36,39),	(40,42,58),	(24,70,74),	(60,63,87),
(12,16,20),	(24,32,40),	(36,48,60),	(21,72,75),	(39,80,89),
(7,24,25),	(9,40,41),	(11,60,61),	(45,60,75),	(54,72,90),
(15,20,25),	(27,36,45),	(16,63,65),	(30,72,78),	(35,84,91),
(10,24,26),	(14,48,50),	(25,60,65),	(48,64,80),	(57,76,95),
(20,21,29),	(30,40,50),	(33,56,65),	(18,80,82),	(65,72,97).

5. Answer: a) $X = (15m^2 + n^2)r$, $Y = 2mnr$, $Z = (15m^2 - n^2)r$; b) $X = 9mnr$, $Y = 9(9n^2 - m^2)r$, $Z = m^2r$; in items a) and b), n and m are integers, while r is an appropriate rational number (these formulae are just one of the possible ways of expressing the answer).

c) The unique solution with $Z = 0$ is $X = Y = Z = 0$. Now let $Z \neq 0$. Suppose that (X, Y, Z) is a solution of the equation $X^2 + 3Y^2 = 5Z^2$ and the numbers X, Y, Z have no common prime divisors. Consider this equation "modulo 5": when divided by 5 the number X^2 can have the remainders 0, 1, or 4, while the number $3Y^2$, the remainders 0, 2, or 3. Therefore, since $X^2 + 3Y^2$ is divisible by 5, then both X and Y are divisible by 5, and it follows that Z is divisible by 5. This contradicts the assumption that the numbers X, Y, Z have no common prime divisors.

6. Let (x_0, y_0) be a rational point on the curve

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

Let us draw a line through (x_0, y_0) with angular coefficient t:

$$y = tx + (y_0 - tx_0),$$

and substitute y into the equation of the curve. We obtain an equation of degree no greater that two

$$A(t)x^2 + B(t)x + C(t) = 0$$

whose coefficients are, as is easy to see, polynomials t with rational coefficients (because x_0, y_0, a, b, c, d, e, f are rational numbers). Note that for any t_0, the numbers $A(t), B(t), C(t)$ cannot be simultaneously equal to zero, because that would mean that under the substitution $y = t_0x + (y_0 - t_0x_0)$ the polynomial

$$ax^2 + bxy + cy^2 + dx + ey + f$$

becomes identically equal to zero. Introduce a new coordinate system $(x'y')$ in which the line $y = t_0x + (y_0 - t_0x_0)$ is given by the equation $y' = 0$. In this system, our curve has the equation $F(x', y') = 0$, where F is a polynomial of degree no greater that two, and $F(x', 0) \equiv 0$. Therefore, $F(x', y')$ is divisible by y', so that $F(x', y') = y' \cdot G(x', y')$, where $G(x', y')$ is some polynomial. Returning to the previous coordinate system, we see that the polynomial $ax^2+bxy+cy^2+dx+ey+f$ is divisible by the polynomial $y - tx - (y_0 - tx_0)$, which contradicts the absolute irreducibility of our curve.

If $A(t) = a + bt + ct^2 = 0$, then the equation

$$A(t)x^2 + B(t)x + C(t) = 0$$

is of degree 1, but there are no more than two such values of t. For the other vaiues of t, the equation is quadratic. One of its roots is x_0, and by Vieta's Theorem, the other root is $-(B(t)/A(t)) - x_0$. Thus

$$x = -\frac{B(t)}{A(t)} - x_0, \quad y = t\left(-\frac{B(t)}{A(t)} - x_0\right) + (y_0 - tx_0)$$

and the above are the desired rational functions with rational coefficients. It remains to show that at least one of them is not a constant.

Assume that both are constant functions,

$$-\frac{B(t)}{A(t)} \equiv h_1, \quad t\left(-\frac{B(t)}{A(t)} - 2x_0\right) \equiv h_2.$$

Then $t(h_1 - 2x_0) \equiv h_2$, hence

$$h_1 = 2x_0, \quad -B(t)/A(t) = 2x_0,$$

$$A(t)x^2 + B(t)x + C(t) = A(t)x^2 - 2x_0A(t)x + C(t).$$

The number x_0 is always a root of this polynomial, and so we have $C(t) = x_0^2A(t)$. Let t_0 be a root of the equation $A(t) = 0$ (possibly complex). Then $A(t_0) = B(t_0) = C(t_0) = 0$, which, as we showed above, is impossible. Contradiction.

7. *Answer*: if and only if all the odd primes entering in the decomposition of the integer c into a product of primes in odd degrees have remainder 1 under division by 4.

In the solution of this problem, we use the results of problems 8 and 10–12.

We can assume that c is square free. If $c = x^2 + y^2$, then by problem 8, the number -1 must be a quadratic residue modulo c. Therefore, all the prime divisors of c must be of the form $4k + 1$ (see problem 12).

Conversely, let all the prime divisors of the square-free integer c be of the form $4k+1$ or $p = 2$ (the case $c = 1$ is trivial). Since the equalities $c_1 = x_1^2 + y_1^2$ and $c_2 = x_2^2 + y_2^2$ imply

$$c_1c_2 = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2,$$

it suffices to prove that any prime of the form $p = 4k+1$ can be presented as the sum of squares of two rational numbers (for $p = 2$, we have $2 = 1^2 + 1^2$).

The proof will be by induction. Our statement holds for $p = 5$: we have $5 = 2^2 + 1^2$; assume that it holds for all primes $p' = 4k' + 1$, $p' < p$. Let us prove it for p. According to problem 12, we can find an integer m such that $m^2 + 1 = np$. If $n = 1$, then everything is proved. In the converse case, we can assume that $|m| \le p/2$ (to see this, first replace m by its remainder under division by p, and then, if necessary, by $p - m$); naturally, $1 \le p/2$. Thus $n \le p/2 \le p$. All the prime divisors of np of the form $4k+3$ enter into np (and so into n as well) in even degrees. Let $n = n_{\text{sq.free}}\tilde{n}$, where $n_{\text{sq.free}}$ is square free. Then $n_{\text{sq.free}} \le n < p$; all the odd prime divisors p' of of the number $n_{\text{sq.free}}$ are less than p and are of the form $4k + 1$. By the induction hypothesis, they are representable in the form of the sum of squares of two rational numbers, and hence so are

$n_{\text{sq.free}}$ and n. Let $n = a^2 + b^2$. The next identity completes the proof:

$$p = \frac{m^2+1}{a^2+b^2} = \frac{(m^2+1)(a^2+b^2)}{(a^2+b^2)^2} = \frac{(ma+b)^2+(mb-a)^2}{(a^2+b^2)^2}$$
$$= \left(\frac{ma+b}{a^2+b^2}\right)^2 + \left(\frac{mb-a}{a^2+b^2}\right)^2.$$

A somewhat more delicate argument shows that in this case c is actually the sum of squares of two *integers*.

10. Let x be an integer. The remainder of x^2 when divided by a prime p depends only on the remainder of x when divided by p. Therefore, in order to find all the quadratic residues, it suffices to find the remainder of x^2 when divided by p of the numbers x^2, $x = 0, 1, \ldots, p-1$. Note that the integers x^2 and $(p-x)^2$ give the same remainders when divided by p. Among the numbers $0, 1, \ldots, p-1$, we can distinguish $(p-1)/2$ pairs $(x, p-x)$, and this leaves the number 0. Therefore, the number of quadratic residues is no more than $(p+1)/2$. On the other hand, if x^2 and y^2 give the same remainder when divided by p, then $x^2 - y^2 = (x-y)(x+y)$ is divisible by p, i.e., $x-y$ or $x+y$ is divisible by p. This means that either x and y, or x and $p-y$ give the same remainder when divided by p. Therefore, the number of quadratic residues is $(p+1)/2$.

11. The solution of this problem is based on the following statement.

Chinese Remainder Theorem. *Let M and N be coprime integers. Then for any integers x and y, there exists an integer z such that x and z give the same remainder when divided by M, while y and z give the same remainder when divided by N.*

Let $\tau(N)$ be the number of remainders modulo N which are quadratic residues modulo N. Let us prove that if N_1 and N_2 are coprime integers, then $\tau(N_1 N_2) = \tau(N_1)\tau(N_2)$. To this end, let us construct a one-to-one mapping that to each pair

(quadratic residue modulo N_1, quadratic residue modulo N_2)

assigns the quadratic residue modulo $N_1 N_2$ (here we consider only remainders under division by each of the numbers N_1 and N_2). Let

$$a \equiv u^2 \pmod{N_1},\ 0 \le a < N_1, \text{ and } b \equiv v^2 \pmod{N_2},\ 0 \le b < N_2.$$

Then, by the Chinese Remainder Theorem, there is an integer z such that

$$z \equiv a \pmod{N_1},\ z \equiv b \pmod{N_2}.$$

Assign to the pair (a, b) the remainder c under the division of z by $N_1 N_2$. This remainder does not depend on the choice of z, since any two numbers z and z' such that

$$z \equiv z' \equiv a \pmod{N_1}, \text{ and } z \equiv z' \equiv b \pmod{N_2}$$

differ by a multiple of N_1N_2. This easily follows from the fact that N_1 and N_2 are coprime. Let us prove that the remainder c is a quadratic residue modulo N_1N_2. Indeed, by the Chinese Remainder Theorem, there is an integer w such that

$$w \equiv u \,(\mathrm{mod}\ N_1), \text{ and } w \equiv v \,(\mathrm{mod}\ N_2).$$

Then

$$c \equiv w^2 \,(\mathrm{mod}\ N_1), \text{ and } c \equiv w^2 \,(\mathrm{mod}\ N_2),$$

and so, by virtue of the fact that N_1 and N_2 are coprime, we easily conclude that $c \equiv w^2 \,(\mathrm{mod}\ N_1N_2)$. Let us show that the constructed mapping is one-to-one.

Indeed, since by construction $c \equiv a \,(\mathrm{mod}\ N_1)$ and $c \equiv b \,(\mathrm{mod}\ N_2)$, to different pairs (a, b) correspond different residues c. Now if c is a quadratic residue modulo N_1N_2, then to the pair (a, b), in which a is the remainder of c when divided by N_1 and b is the remainder of c when divided by N_2, will indeed correspond precisely the remainder c.

Thus, $\tau(N_1N_2) = \tau(N_1)\tau(N_2)$, and therefore $\tau(M) = \tau(p_1) \cdot \ldots \cdot \tau(p_n)$. We know (see problem 10) that for odd primes p, we have

$$\tau(p) = \frac{p+1}{2} = \left[\frac{p}{2}\right] + 1.$$

For the number 2, we have a similar equality $\tau(2) = 2 = [2/2] + 1$, which can be easily verified. It remains to write out the final answer: the number of quadratic residue modulo M equals

$$\tau(M) = \left(\left[\frac{p_1}{2}\right] + 1\right) \cdot \ldots \cdot \left(\left[\frac{p_n}{2}\right] + 1\right),$$

the remaining $M - \tau(M)$ remainders are quadratic nonresidues.

Try to solve this problem for an arbitrary integer M.

12. To solve this problem we will need

Fermat's Little Theorem. *Let p be a prime, a be an arbitrary integer not divisible by p. Then a^{p-1} is divisible by p.*

Let p be an odd prime. By Fermat's Little Theorem, it follows that either $a^{(p-1)/2} - 1$ or $a^{(p-1)/2} + 1$ is divisible by p.

If a is a nonzero quadratic residue modulo p, i.e., the remainder of a when divided by p is equal to the remainder of x^2 when divided by p, then the remainder of $a^{(p-1)/2}$ when divided by p is equal to the remainder of $(x^2)^{(p-1)/2}$ when divided by p, i.e., equals 1. Hence, $a^{(p-1)/2} - 1$ is divisible by p. In other words, the nonzero quadratic residues under consideration are roots of the "equation modulo p" $x^{(p-1)/2} - 1 = 0$. Since the number of nonzero quadratic residue modulo p is equal to $(p-1)/2$, this equation has no other roots. Therefore, if a is a quadratic nonresidue modulo p, then $a^{(p-1)/2} + 1$ is divisible by p.

Now let $a = p - 1$. Then

$$a^{(p-1)/2} = (p-1)^{(p-1)/2} \equiv (-1)^{(p-1)/2} = \begin{cases} 1, & \text{if } p = 4k+1, \\ -1, & \text{if } p = 4k+3. \end{cases}$$

13. *Answer*: a) no; b) yes, for instance $(1/2, 1/2)$ is a solution.

14. *Hints*: a) if a and b are divisible by q, then we have

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

if and only if

$$\frac{a}{q}(qx)^2 + \frac{b}{q}(qy)^2 - qcz^2 = 0.$$

b) For example, suppose p divides b. Then $n^2 \equiv ac \pmod{p}$ (recall that ac is a nonzero quadratic residue modulo b and so modulo p as well). Then

$$ax^2 - cy^2 \equiv a\left(x - \frac{n}{a}\,y\right)\left(x + \frac{n}{a}\,y\right) \pmod{p}.$$

c) Apply the Chinese Remainder Theorem.

d) Consider all the triples of integers (x, y, z) such that

$$0 \le x < \sqrt{bc},\ 0 \le y < \sqrt{ca},\ 0 \le z < \sqrt{ab}.$$

The number of such triples is strictly greater that abc (except for the case $a = b = c = 1$). So we can find triples (x', y', z') and (x'', y'', z'') such that

$$L(x', y', z') = L(x'', y'', z'').$$

Then the triple $(x' - x'', y' - y'', z' - z'')$ will be a nonzero solution of the equation

$$ax^2 + by^2 - cz^2 \equiv 0 \,(\text{mod } abc)$$

and this triple will satisfy the required inequalities.

e) From the inequalities we easily obtain

$$-abc < ax^2 + by^2 - cz^2 < 2abc.$$

16. Suppose that a line intersects a second order curve at a singular point and at one other point. Let us prove that in that case the equation of the curve is divisible by the equation of the line.

Suppose, for instance, that the line is given by the equation $y = 0$, and the curve by $F(x, y) = 0$. The polynomial $F(x, 0)$ in the variable x has a root of multiplicity 2 (at the singular point) and one more root. But it is a polynomial of degree no greater than 2. Therefore, $F(x, 0) = 0$ for all x and $F(x, y)$ is divisible by y.

From the proved auxilliary statement, we deduce that if a second order curve $F(x, y) = 0$ has a singular point, then

$$F(x, y) = l_1(x, y) \cdot l_2(x, y),$$

where $l_1(x, y)$ and $l_2(x, y)$ are linear functions. (Attention: their coefficients can be complex numbers.)

Thus, a second order curve with a singular point is the union of two lines, and the singular point is the intersection of these lines. Similar arguments can be applied to third and fourth order curves.

Answer: on a second order curve there is no more than one singular point, on a third order curve, no more than three, on a fourth order curve, no more than six (for the proof in the latter case, you may use the following fact: there exists a second order curve passing through any five points). In all the cases considered, a curve with the maximal number of singular points is the union of several lines.

17. *Answer*: yes, it is possible. For example, the union of four lines, two of which are parallel.

20. *Answer*: for example, $y^3 + 3xy^2 - x^3 - 3x^2 - 3xy - 3y^2 + 3 = 0$. Check that this equation is that of the union of three lines passing through the points (x_1, x_2), (x_2, x_3), and (x_3, x_1), where (x_1, x_2, x_3) are the roots of the polynomial equation $x^3 - 3x + 1 = 0$ (which are irrational). The singular points of this curve" are the points (x_1, x_2), (x_2, x_3), and (x_3, x_1).

22. *Answer*: for

$$\begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix} = \alpha_1\beta_2\gamma_3+\alpha_2\beta_3\gamma_1+\alpha_3\beta_1\gamma_2-\alpha_1\beta_3\gamma_2-\alpha_2\beta_1\gamma_3-\alpha_3\beta_2\gamma_1 \neq 0.$$

23. Let (x_0, y_0) be the singular point. For the vertical line $x = x_0$, $y = t$, the multiplicity of the root $t = y_0$ of the equation $t^2 - x_0^3 - ax_0 - b = 0$ can be equal to 2 only if $y_0 = 0$. In this case, x_0 is a root of the equation $x^3 + ax + b = 0$. Now let us consider the line $x = x_0 + t$, $y = 0$. The equation $(x_0 + t)^3 + a(x_0 + t) + b = 0$, together with $x_0^3 + ax_0 + b = 0$, can be rewritten as $t^3 + 3x_0t^2 + (3x_0^2 + a)t = 0$. The multiplicity of the root t must be greater than 1, hence $a = -3x_0^2$. Substituting $x = x_0$ into the equation $x^3 - 3x_0^2x + b = 0$, we obtain $b = 2x_0^3$. Therefore, $\Delta = 4a^3 + 27b^2 = 0$.

Conversely, let $\Delta = 0$. Then (as can be proved by using the Vieta Theorem), the equation $x^3+ax+b = 0$ has a multiple root x_0. Substitute $x = x_0 + t$ into this equation; $t = 0$ is a multiple root of the obtained equation in t, hence $a = -3x_0^2$ and so we have $b = 2x_0^3$. Let us show that $(x_0, 0)$ is a singular point of the curve $y^2 = x^3-3x_0^2x+2x_0^3$. Substituting $x = x_0 + ut$, $y = vt$, we obtain $v^2t^2 = 3x_0u^2t^2 + u^3t^3$, hence $t = 0$ is a root of multiplicity no less than 2.

24. *Answer*: for

$$4\Big(b - \frac{a^2}{3}\Big)^3 + 27\Big(c - \frac{ab}{3} + \frac{2a^3}{27}\Big)^2 = 0.$$

25. *Hint*: for γ_1 take the coefficient of the tangent line at the inflection point.

31. *Answer*: if and only if

$$\frac{4a_1^3}{4a_1^3+27b_1^2}=\frac{4a_2^3}{4a_2^3+27b_2^2}.$$

32. Let us introduce a new system of coordinates in which the line $M(x,y)=0$ will be the x-axis, and so will be defined by the equation $y'=0$. In the new variables, the polynomial $F(x,y)$ will become $G(x',y')$ (the degree of the polynomial G will also be no greater than 3). The polynomial $G(x',0)$ of degree no greater than 3 has four distinct roots, and therefore is identically zero. In other words, $G(x',y')$ is divisible by y'. Returning to the old system of coordinates, we obtain the assertion of the problem.

33. *Hint*: with respect to the variable y, the difference (7) is of degree no greater than two.

40. The condition $3P=\mathbf{0}$ is equivalent to $2P=-P$. By the definition of the point $2P$, this means that the third intersection point with the tangent to the curve drawn through the point P coincides with the point P itself (see Fig. 12, d). Such points are called *inflection points*. The inflection points of the curve $y^2=x^3+ax+b$ are precisely those points where the second derivative of the function $y(x)=\sqrt{x^3+ax+b}$ vanishes.

An elliptic curve in Weierstrass form always contains eight inflexion points in complex coordinates, but only two of them can have real coordinates.

41. Let the rank of the curve be more than zero. Then it has a rational point P of infinite order (linearly independent with itself) and, therefore, there are infinitely many rational points $\ldots$, $-3P$, $-2P$, $-P$, P, $2P$, $3P$, $\ldots$ Let the rank of the curve be zero. This means that any rational point is not linearly independent, i.e., is a point of finite order. However, there is only a finite number of rational torsion points on an elliptic curve.

42. *Answer*: $P_1=(0,0)$, $-P_1=(0,-1)$, $3P_1=(-1,-1)$, $-3P_1=(-1,0)$ (Fig. 18).

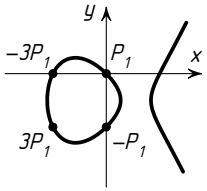


Fig. 18

49. *Hint*: both equations from Tunnell's criterion have no solutions.

50. In Table 1, each of the numbers from 1 to 100 that are squarefree is followed by the number of solutions to the equations of Tunnell's criterion, separated by a hyphen, while the nonsquarefree numbers are followed by their squarefree parts. The numbers satisfying Tunnell's criterion (which are conjecturally congruent) are shown in boldface. Table 2 presents the lengths of the sides of the corresponding triangles.

52. Let us find the inflection points of the curve $y^2 = x^3 - s^2x$ (they are precisely the required points of order 3, see problem 40). To this end, let us differentiate the equation of the curve twice:

$$2yy' = 3x^2 - s^2, \qquad 2(y')^2 + 2yy'' = 6x.$$

If $y'' = 0$, then $(y')^2 = 3x$. We have:

$$\begin{aligned}
4y^2(y')^2 &= (3x^2 - s^2)^2 && \text{(taking the square of } 2yy' = 3x^2 - s^2\text{)},\\
4(x^3 - s^2x)\cdot 3x &= (3x^2 - s^2)^2 && \text{(substituting } y^2 = x^3 - s^2x,\ (y')^2 = 2x\text{)},\\
12x^4 - 12s^2x^2 &= 9x^4 - 6x^2s^2 + s^4,\\
3x^4 - 6x^2s^2 - s^4 &= 0.
\end{aligned}$$

The discriminant of this biquadratic equation is

$$36s^4 + 12s^4 = 48s^4 = 3(4s^2)^2.$$

Therefore, x^2 is an irrational number.

Now let us consider points of order 4. Assume that $s \neq 1$. We will need the formula for doubling points on the curve E_s. Namely, if we put $Q = (x_0, y_0)$ and $2Q = (x_1, y_1)$, then

$$x_1 = \left(\frac{x_0^2 + s^2}{2x_0y_0}\right)^2.$$

If R is a fourth order point, then $2R$ is a point of order 2. Therefore, its abcissa x_1 is 0, or s, or $-s$, and since x_1 is positive, it follows that $x_1 = s$. Thus we immediately obtain a contradiction with the fact that the point (x_0, y_0) is rational. The case $s = 1$ is left to the reader.

53. *Hint*: first prove that the order of the point $\overline{P}$ divides the integer r.

56. *Hint*: -1 is a quadratic nonresidue modulo p.

58. *Answer*: for the Pythagorean brick, we have:

$$\begin{cases}
X^2 + Y^2 = U^2,\\
Y^2 + Z^2 = V^2,\\
Z^2 + X^2 = W^2,\\
X^2 + Y^2 + Z^2 = T^2;
\end{cases}$$

Table 1

1	2 — 2	**21**	0 — 0	**41**	16 — 32	**61**	0 — 0	81	*see* 1
2	2 — 2	**22**	0 — 0	42	0 — 8	**62**	0 — 0	82	8 — 8
3	4 — 4	**23**	0 — 0	43	12 — 12	**63**	*see* **7**	83	20 — 36
4	*see* 1	**24**	*see* **6**	44	*see* 11	64	*see* 1	**84**	*see* **21**
5	0 — 0	25	*see* 1	**45**	*see* **5**	**65**	16 — 32	**85**	0 — 0
6	0 — 0	26	4 — 12	**46**	0 — 0	66	4 — 16	**86**	0 — 0
7	0 — 0	27	*see* 3	**47**	0 — 0	67	4 — 12	**87**	0 — 0
8	*see* 2	**28**	*see* **7**	48	*see* 3	68	*see* 17	**88**	*see* **22**
9	*see* 1	**29**	0 — 0	49	*see* 1	**69**	0 — 0	89	20 — 48
10	4 — 4	**30**	0 — 0	50	*see* 2	**70**	0 — 0	90	*see* 10
11	4 — 12	**31**	0 — 0	51	16 — 24	**71**	0 — 0	91	8 — 24
12	*see* 3	32	*see* 2	**52**	*see* **13**	72	*see* 2	**92**	*see* **23**
13	0 — 0	33	12 — 16	**53**	0 — 0	73	12 — 16	**93**	0 — 0
14	0 — 0	**34**	4 — 8	**54**	*see* **6**	74	12 — 20	**94**	0 — 0
15	0 — 0	35	8 — 24	**55**	0 — 0	75	*see* 3	**95**	0 — 0
16	*see* 1	36	*see* 1	**56**	*see* **14**	76	*see* 19	**96**	*see* **6**
17	4 — 16	**37**	0 — 0	57	12 — 16	**77**	0 — 0	97	4 — 16
18	*see* 2	**38**	0 — 0	58	4 — 4	**78**	0 — 0	98	*see* 2
19	4 — 12	**39**	0 — 0	59	20 — 36	**79**	0 — 0	99	*see* 11
20	*see* **5**	40	*see* 10	**60**	*see* **15**	**80**	*see* **5**	100	*see* 1

Table 2

5	$\frac{3}{2}$, $\frac{20}{3}$, $\frac{41}{6}$	37	$\frac{777923}{6090}$, $\frac{450660}{777923}$, $\frac{605170417321}{4737551070}$	65	12, $\frac{65}{6}$, $\frac{97}{6}$
6	3, 4, 5			69	$\frac{437}{104}$, $\frac{624}{19}$, $\frac{65425}{1976}$
7	$\frac{24}{5}$, $\frac{35}{12}$, $\frac{337}{60}$	38	$\frac{5301}{425}$, $\frac{1700}{279}$, $\frac{1646021}{118575}$	70	15, $\frac{28}{3}$, $\frac{53}{3}$
13	$\frac{780}{323}$, $\frac{323}{30}$, $\frac{106921}{9690}$	39	$\frac{312}{10}$, $\frac{5}{2}$, $\frac{313}{10}$	71	$\frac{30317}{660}$, $\frac{1320}{427}$, $\frac{12974641}{281820}$
14	$\frac{21}{2}$, $\frac{8}{3}$, $\frac{65}{6}$	41	$\frac{40}{3}$, $\frac{123}{20}$, $\frac{881}{60}$	77	$\frac{525}{848}$, $\frac{18656}{75}$, $\frac{15820337}{63600}$
15	$\frac{15}{2}$, 4, $\frac{17}{2}$	46	$\frac{253}{42}$, $\frac{168}{11}$, $\frac{7585}{462}$	78	45, $\frac{52}{15}$, $\frac{677}{15}$
21	12, $\frac{7}{2}$, $\frac{25}{2}$	47	$\frac{11547216}{2097655}$, $\frac{98589785}{5773608}$, $\frac{217287944875297}{12111037689240}$	79	$\frac{335946000}{2950969}$, $\frac{233126551}{167973000}$, $\frac{56434050774922081}{495683115837000}$
22	$\frac{140}{3}$, $\frac{33}{35}$, $\frac{4901}{105}$				
23	$\frac{41496}{3485}$, $\frac{80155}{20748}$, $\frac{905141617}{72306780}$	53	$\frac{1472112483}{202332130}$, $\frac{21447205780}{1472112483}$, $\frac{4850493897329785961}{297855654284978790}$	85	$\frac{77}{6}$, $\frac{1020}{77}$, $\frac{8521}{462}$
				86	$\frac{2193}{91}$, $\frac{364}{51}$, $\frac{116645}{4641}$
29	$\frac{52780}{99}$, $\frac{99}{910}$, $\frac{48029801}{90090}$	55	$\frac{117}{10}$, $\frac{1100}{117}$, $\frac{17561}{1170}$	87	$\frac{3484}{1925}$, $\frac{167475}{1742}$, $\frac{322446497}{3353350}$
30	12, 5, 13	61	$\frac{6428003}{1423110}$, $\frac{173619420}{6428003}$, $\frac{250510625883241}{9147755349330}$	93	$\frac{56203}{1330}$, $\frac{7980}{1813}$, $\frac{2090761}{49210}$
31	$\frac{8897}{360}$, $\frac{720}{287}$, $\frac{2566561}{103320}$			94	$\frac{7728}{2057}$, $\frac{96679}{1932}$, $\frac{199428385}{3974124}$
34	$\frac{136}{15}$, $\frac{15}{2}$, $\frac{353}{30}$	62	$\frac{84560}{5727}$, $\frac{177537}{21140}$, $\frac{2056525601}{121068780}$	95	$\frac{1443}{34}$, $\frac{6460}{1443}$, $\frac{2093801}{49062}$

for the weak Pythagorean brick:

$$\begin{cases} X^2 + Y^2 = U^2, \\ Y^2 + Z^2 = V^2, \\ Z^2 + X^2 = W^2. \end{cases}$$

Dividing all the variables by one of them, say U, we obtain a system of four equations with six variables (respectively, of three equations with five variables). The corresponding geometric objects are *algebraic surfaces*. These surfaces lie in multidimensional spaces and have a finite number of singular points (count them!).

59. *Hint*: To describe all parallelepipeds with integer sides X, Y, Z and T is equivalent to finding the integer solutions of the equation $X^2 + Y^2 + Z^2 = T^2$. The only solution of this equation for $T = 0$ is $X = Y = Z = T = 0$. For all other solutions with $T \neq 0$, the equation can be divided by T^2. Thus the problem reduces to finding all the rational solutions of the equation

$$x^2 + y^2 + z^2 = 1, \text{ where } x = X/T,\ y = Y/T,\ z = Z/T.$$

This equation defines the unit sphere in the space $Oxyz$ (Fig. 19). Choose a rational point, say $A(0, 0, 1)$ on the sphere. It is easy to verify that any line AB, where $B(x, y, z)$ is another rational point on the sphere, intersects the plane Oxy at a rational point $C(a, b, 0)$ and, conversely, any line AC intersects the sphere at a rational point B. Thus there are "as many" rational points on the sphere, as on the plane. The

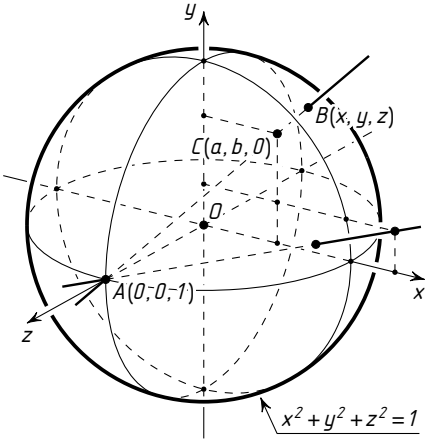


Fig. 19

numbers x, y, z can be expressed in terms of a, b, c as follows

$$x = \frac{2a}{a^2+b^2+1}, \quad y = \frac{2b}{a^2+b^2+1},$$
$$z = \frac{a^2+b^2-1}{a^2+b^2+1}.$$

Using this and setting $a = k/l$, $b = m/n$. we obtain the final *answer*:

$$X = 2kln^2r, \quad Y = 2l^2mnr,$$
$$Z = (k^2n^2 + l^2m^2 - l^2n^2)r,$$
$$T = (k^2n^2 + l^2m^2 + l^2n^2)r.$$

Here k, l, m, n are integers, r is an appropriate rational number, i.e., a rational number such that the numbers X, Y, Z, T are integers.

60. Let us show that the polynomials $X^2 + Y^2$, $Y^2 + Z^2$, $Z^2 + X^2$ are exact squares of polynomials with integer coefficients. Then, for any integer value n, the numbers U, V and W will also be integers. Thus,

$$X^2+Y^2=(n^6-15n^4+15n^2-1)^2+(6n^5-20n^3+6n)^2=$$
$$=(n^{12}-30n^{10}+255n^8-452n^6+255n^4-30n^2+1)+$$
$$+(36n^{10}-240n^8+472n^6-240n^4+36n^2)=$$
$$=n^{12}+6n^{10}+15n^8+20n^6+15n^4+6n^2+1=(n^6+3n^4+3n^2+1)^2,$$

$$Y^2+Z^2=(6n^5-20n^3+6n)^2+(8n^5-8n)^2=$$
$$=(36n^{10}-240n^8+472n^6-240n^4+36n^2)+(64n^{10}-128n^6+64n^2)=$$
$$=100n^{10}-240n^8+344n^6-240n^4+100n^2=(10n^5-12n^3+10n)^2,$$

$$Z^2+X^2=(8n^5-8n)^2+(n^6-15n^4+15n^2-1)^2=$$
$$=(64n^{10}-128n^6+64n^2)+(n^{12}-30n^{10}+255n^8-452n^6+255n^4-30n^2+1)=$$
$$=n^{12}+34n^{10}+255n^8-580n^6+255n^4+34n^2+1=(n^6+17n^4-17n^2-1)^2.$$

Thus $U=n^6+3n^4+3n^2+1$, $V=10n^5-12n^3+10n$, $W=n^6+17n^4-17n^2-1$.

CONTENTS