Little Mathematics Library

A.O. GELFOND

SOLVING EQUATIONS IN INTEGERS

Mir Publishers · Moscow

ИЗДАТЕЛЬСТВО · МИР ·

ПОПУЛЯРНЫЕ ЛЕКЦИИ ПО МАТЕМАТИКЕ

А. О. Гельфонд

РЕШЕНИЕ УРАВНЕНИЙ В ЦЕЛЫХ ЧИСЛАХ

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА

LITTLE MATHEMATICS LIBRARY

A. O. Gelfond

SOLVING EQUATIONS IN INTEGERS

Translated from the Russian
by
O. B. Sheinin

Mir Publishers
Moscow

First published 1981
Revised from the 1978 Russian edition

На английском языке

© Издательство «Наука»
Главная редакция физико-математической литературы, 1978
© English translation, Mir Publishers, 1981

Printed in the Union of Soviet Socialist Republics

Contents

Preface

This book is based on a lecture on the solution of equations in integers which I delivered in 1951 for the participants of a Mathematical Olympiad arranged by Moscow State University; I am glad to acknowledge the assistance rendered me by my former student, Assistant Professor N. M. Korobov, who took notes of my lecture and wrote the first two sections and part of the third section of the book.

High-school students will readily understand the subject-matter of the book.

A. Gelfond

Introduction

The theory of numbers is one of the oldest branches of mathematics. It is mainly concerned with the arithmetic properties of natural numbers, that is, positive integers.

A most important problem in what is called analytic theory of numbers is the problem of the distribution of prime numbers in the sequence of natural numbers. (A prime number is any positive integer greater than unity and divisible only by itself and, of course, by unity.) It concerns the regularity exhibited by prime numbers smaller than some number N for large values of N.

As long ago as the fourth century B. C. Euclid obtained the first results in the solution of this problem. He proved that the sequence of prime numbers is infinite. The next result was achieved in the second half of the 19th century by the great Russian mathematician P. L. Chebyshev.

Another fundamental problem in, or branch of, number theory concerns the representation of integers as sums of integers of some specified kind, for example, the possibility of representing odd numbers as sums of three prime numbers. This problem (the Goldbach conjecture) was solved by the great number theorist, the Soviet mathematician I. M. Vinogradov.

This book is devoted to an interesting branch of number theory, the solution of equations in integers.

The solution in integers of algebraic equations in more than one unknown with integral coefficients is a most difficult problem in the theory of numbers. The most eminent ancient mathematicians such as the Greek mathematician Pythagoras (sixth century B. C.) and the Alexandrian mathematician Diophantus (second and third centuries A. D.), and also the best mathematicians of more recent times such as Fermat (in the seventeenth century), Euler and Lagrange (in the eighteenth century) devoted much attention to these problems. The efforts of many generations of eminent mathematicians notwithstanding, this branch of the theory of numbers lacks mathematical methods of any generality, unlike the analytic theory of numbers in which many diverse problems can be solved by the method of trigonometric sums, due to Vinogradov.

As yet, a complete solution of equations in integers is possible only for equations of the second degree in two unknowns. Note that equations of any degree in one unknown are not really interesting: their solution in integers might be carried out by a finite number of trials. For equations of degree higher than the second in two or more unknowns the problem becomes rather complicated. Even the more simple problem of establishing whether the number of integral solutions is finite or infinite presents extreme difficulties.

The theoretical importance of equations with integral coefficients is quite great as they are closely linked with many problems of number theory. Moreover, these equations are sometimes encountered in physics and so they are also important in practice. Lastly, the elements of the theory of equations with integral coefficients as presented in this book are suitable for broadening the mathematical outlook of high-school students and students of pedagogical institutes.

Certain of the main results in the theory of the solution of equations in integers have been given here. Proofs of the theorems involved are supplied when they are sufficiently simple.

§ 1. Equations in One Unknown

Let us consider a linear equation in one unknown

$$a_1x + a_0 = 0 \qquad (1)$$

with integral coefficients a_1 and a_0. The solution of this equation

$$x = -\frac{a_0}{a_1}$$

is an integer only when a_0 is divisible by a_1. Thus equation (1) is not always solvable in integers. For instance, equation $3x - 27 = 0$ possesses an integral solution $x = 9$, while equation $5x + 21 = 0$ has no such solution.

The same is true in the case of equations of degree higher than the first. For example, quadratic equation $x^2 + x - 2 = 0$ has the integral solutions $x_1 = 1$ and $x_2 = -2$, whereas equation $x^2 - 4x + 2 = 0$ is not solvable in integers; its roots $x_{1,2} = 2 \pm \sqrt{2}$ are irrational numbers.

The determination of the integral roots of the nth degree equation

$$a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0 \quad (n \geqslant 1) \qquad (2)$$

with integral coefficients is not difficult. Indeed, let $x = a$ be an integral root of this equation. Then

$$a_na^n + a_{n-1}a^{n-1} + \ldots + a_1a + a_0 = 0$$

$$a_0 = -a(a_na^{n-1} + a_{n-1}a^{n-2} + \ldots + a_1)$$

The latter equality means that a_0 is divisible by a. Consequently any integral root of equation (2) is a divisor of its free term a_0.

Check all the divisors of a_0 one by one; those which transform equation (2) into an identity are the integral solutions sought. For example, the divisors of the free term of equation

$$x^{10} + x^7 + 2x^3 + 2 = 0$$

are 1, -1, 2 and -2. Only one divisor, -1, is a root of the equation; hence this equation possesses only one integral root $x = -1$.

Applying the same method it is easy to show that equation

$$x^6 - x^5 + 3x^4 + x^2 - x + 3 = 0$$

has no integral solutions.

The solution in integers of equations in several unknowns is much more interesting.

§ 2. Linear Equations in Two Unknowns

Let us consider a linear equation in two unknowns

$$ax + by + c = 0 \tag{3}$$

where a and b are non-zero integers and c is an arbitrary integer. We shall suppose that the coefficients a and b have no common divisors (except, of course, unity)*. Indeed, if the greatest common divisor of these coefficients, $d = (a, b)$, is not unity, then $a = a_1 d$, $b = b_1 d$, and equation (3) may be written as

$$(a_1 x + b_1 y) d + c = 0$$

It can have integral solutions only if c is divisible by d. In other words, in the case when $(a, b) = d \neq 1$, all the coefficients of equation (3) must be divisible by d. Cancelling d from the equation, we arrive at equation

$$a_1 x + b_1 y + c_1 = 0 \quad \left(c_1 = \frac{c}{d}\right)$$

whose coefficients a_1 and b_1 are relatively prime.

We shall first consider the case $c = 0$. Equation (3) becomes

$$ax + by = 0 \tag{3'}$$

* Such numbers as a and b are called *relatively prime* integers. We shall denote the greatest common divisor of a and b by (a, b). For relatively prime numbers a and b, we have $(a, b) = 1$.

Solving it with respect to x, we obtain

$$x = -\frac{b}{a}y$$

Obviously, x will be an integer if and only if y is divisible by a, or, in other words, if y is a multiple of a,

$$y = at$$

where t is an arbitrary integer ($t = 0, \pm 1, \pm 2, \ldots$). Substituting this value of y in the previous equation, we obtain

$$x = -\frac{b}{a}at = -bt$$

and formulae

$$x = -bt, \quad y = at \quad (t = 0, \pm 1, \pm 2, \ldots)$$

furnish all the integral solutions of equation (3′).

We now consider the case $c \neq 0$. Let us show first of all that in order to find all the integral solutions of equation (3), it is sufficient to find any one solution, i. e. it is sufficient to find integers x_0, y_0 for which

$$ax_0 + by_0 + c = 0$$

THEOREM 1. *Let a and b be relatively prime and suppose $[x_0, y_0]$ is any solution* of equation*

$$ax + by + c = 0 \tag{3}$$

Then formulae

$$x = x_0 - bt, \quad y = y_0 + at \tag{4}$$

where $t = 0, \pm 1, \pm 2, \ldots,$ yield all the solutions of equation (3).

Proof. Let $[x, y]$ be an arbitrary solution of equation (3). Then equalities

$$ax + by + c = 0, \quad ax_0 + by_0 + c = 0$$

render

$$ax - ax_0 + by - by_0 = 0; \quad y - y_0 = \frac{a(x_0 - x)}{b}$$

* A pair of integers x and y which satisfy the equation will be called its *solution* and denoted by $[x, y]$.

Since $y - y_0$ is an integer and a and b are relatively prime, $x_0 - x$ must be divisible by b, i. e. $x_0 - x$ has the form

$$x_0 - x = bt$$

where t is an integer. But then

$$y - y_0 = \frac{abt}{b} = at$$

and we get

$$x = x_0 - bt, \quad y = y_0 + at$$

Thus, it is proved that each solution $[x, y]$ has the form presented as (4). It remains for us to check that any pair of numbers $[x_1, y_1]$ obtained by formulae (4) for an integer $t = t_1$ will be a solution of equation (3). To do this, substitute $x_1 = x_0 - bt_1$, $y_1 = y_0 + at_1$ into the left-hand side of equation (3):

$$ax_1 + by_1 + c = ax_0 - abt_1 + by_0 + abt_1 + c = ax_0 + by_0 + c$$

Now $[x_0, y_0]$ is a solution, and so $ax_0 + by_0 + c = 0$ and, consequently,

$$ax_1 + by_1 + c = 0$$

i. e. $[x_1, y_1]$ is a solution of equation (3). The proof of the theorem is now complete.

Hence, if one solution of equation $ax + by + c = 0$ is known, all the other solutions can be determined from arithmetic progressions whose general terms are

$$x = x_0 - bt, \quad y = y_0 + at \quad (t = 0, \pm 1, \pm 2, \ldots)$$

Note that for the case $c = 0$ the formulae found previously

$$x = -bt, \quad y = at$$

may be derived from the formulae just derived by setting $x_0 = y_0 = 0$. This is legitimate because the values $x = 0$, $y = 0$ are a solution of equation

$$ax + by = 0$$

But how is one to find a solution $[x_0, y_0]$ of equation (3) in the general case when $c \neq 0$? Consider an equation

$$127x - 52y + 1 = 0$$

Let us transform the ratio of the coefficients of the unknowns, beginning by isolating the integral part of the improper fraction

127/52:

$$\frac{127}{52} = 2 + \frac{23}{52}$$

The proper fraction 23/52 is of course equal to $\frac{1}{52/23}$, so that

$$\frac{127}{52} = 2 + \frac{1}{52/23}$$

Now we shall apply the same transformation to the improper fraction 52/23 in the denominator of the last equality:

$$\frac{52}{23} = 2 + \frac{6}{23} = 2 + \frac{1}{23/6}$$

The initial fraction is thus equal to

$$\frac{127}{52} = 2 + \cfrac{1}{2 + \cfrac{1}{23/6}}$$

Again, let us repeat the same process for the fraction 23/6:

$$\frac{23}{6} = 3 + \frac{5}{6} = 3 + \frac{1}{6/5}$$

Then

$$\frac{127}{52} = 2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{6/5}}}$$

Lastly, we shall isolate the integral part of the improper fraction 6/5:

$$\frac{6}{5} = 1 + \frac{1}{5}$$

The final result is

$$\frac{127}{52} = 2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{5}}}}$$

This expression is a *terminating continued fraction.* If we omit the last term, the one-fifth, and transform the new continued fraction so obtained into a common fraction and subtract it from the initial fraction 127/52, we get

$$2+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{1}}}=2+\cfrac{1}{2+\cfrac{1}{4}}=2+\frac{4}{9}=\frac{22}{9}$$

$$\frac{127}{52}-\frac{22}{9}=\frac{1143-1144}{52\cdot 9}=-\frac{1}{52\cdot 9}$$

Reducing this expression to a common denominator and rejecting it we get

$$127\cdot 9-52\cdot 22+1=0$$

A comparison of this equality with equation

$$127x-52y+1=0$$

shows that $x=9$, $y=22$ is a solution of the equation and by the theorem all its solutions are contained in the arithmetic progressions

$$x=9+52t,\quad y=22+127t\quad (t=0,\ \pm 1,\ \pm 2,\ \ldots)$$

The result obtained suggests that in the general case of the equation $ax+by+c=0$ the solution may also be derived by expanding the ratio of the coefficients of the unknowns as a continued fraction, omitting the last term, and continuing calculations as we did above.

To prove this supposition we shall need some properties of continued fractions. Consider an irreducible fraction a/b. Let us divide a by b and denote the quotient by q_1 and the remainder by r_2:

$$a=q_1b+r_2,\quad r_2<b$$

Now divide b by r_2, denoting the quotient by q_2 and the remainder by r_3. Then

$$b=q_2r_2+r_3,\quad r_3<r_2$$

Continuing this process we obtain

$$r_2=q_3r_3+r_4,\quad r_4<r_3$$

$$r_3 = q_4 r_4 + r_5, \quad r_5 < r_4$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

The quantities q_1, q_2, ... are called *partial quotients*, and the process of calculating them just described is known as the *Euclidean algorithm*. As noted above, the remainders $r_2, r_3, \ldots,$ satisfy inequalities

$$b > r_2 > r_3 > r_4 \ldots \geqslant 0 \tag{5}$$

and thus constitute a sequence of decreasing nonnegative numbers.

Since the number of nonnegative integers which do not exceed b cannot be infinite, the remainder r will vanish at some step and the process of forming the partial quotients will cease. Let r_n be the last non-zero remainder in sequence (5). Then $r_{n+1} = 0$ and the Euclidean algorithm for the numbers a and b will be

$$\left.\begin{aligned} a &= q_1 b + r_2 \\ b &= q_2 r_2 + r_3 \\ r_2 &= q_3 r_3 + r_4 \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \\ r_{n-1} &= q_n r_n \end{aligned}\right\} \tag{6}$$

Let us write these equalities in the form

$$\frac{a}{b} = q_1 + \frac{1}{b/r_2}$$

$$\frac{b}{r_2} = q_2 + \frac{1}{r_2/r_3}$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$\frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{r_{n-1}/r_n}$$

$$\frac{r_{n-1}}{r_n} = q_n$$

By substituting the expression for b/r_2 from the second equation into the first equality and the expression for r_2/r_3 from the third equation (which is not written out above) into the second equality and so on, we obtain the expansion of a/b as a continued fraction:

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdot \, \cdot \, \cdot + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}$$

The expression obtained by omitting all terms of a continued fraction starting with some particular term is called a *convergent.* The first convergent δ_1 is obtained by omitting all terms starting with $1/q_2$:

$$\delta_1 = q_1 < \frac{a}{b}$$

the second convergent, δ_2, is obtained by omitting all terms starting with $1/q_3$:

$$\delta_2 = q_1 + \frac{1}{q_2} > \frac{a}{b}$$

Similarly,

$$\delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}} < \frac{a}{b}$$

$$\delta_4 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4}}} > \frac{a}{b}$$

etc.

Because of their method of formation the convergents satisfy the obvious inequalities

$$\delta_1 < \delta_3 < \ldots < \delta_{2k-1} < \frac{a}{b}$$

$$\delta_2 > \delta_4 > \ldots > \delta_{2k} > \frac{a}{b}$$

Let us write the kth convergent δ_k as a fraction

$$\delta_k = \frac{P_k}{Q_k} \quad (1 \leqslant k \leqslant n)$$

and find the rule for forming the numerators and denominators of convergents. We begin with the first three convergents δ_1, δ_2 and δ_3:

$$\delta_1 = q_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}; \quad P_1 = q_1, \; Q_1 = 1$$

$$\delta_2 = q_1 + \frac{1}{q_2} = \frac{q_1 q_2 + 1}{q_2} = \frac{P_2}{Q_2}; \; P_2 = q_1 q_2 + 1; \; Q_2 = q_2$$

$$\delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}} = q_1 + \frac{q_3}{q_2 q_3 + 1} = \frac{q_1 q_2 q_3 + q_1 + q_3}{q_2 q_3 + 1} = \frac{P_3}{Q_3}$$

$$P_3 = q_1 q_2 q_3 + q_1 + q_3; \quad Q_3 = q_2 q_3 + 1$$

From these we obtain

$$P_3 = P_2 q_3 + P_1; \quad Q_3 = Q_2 q_3 + Q_1$$

By applying mathematical induction* we can prove that the similar relations

$$P_k = P_{k-1} q_k + P_{k-2}, \quad Q_k = Q_{k-1} q_k + Q_{k-2} \tag{7}$$

hold for all $k \geqslant 3$.

Let equalities (7) be valid for some $k \geqslant 3$. By the definition of the convergents it immediately follows that if in the expression for δ_k, q_k is replaced by $q_k + \dfrac{1}{q_{k+1}}$, δ_k becomes δ_{k+1}. By the induction hypothesis,

$$\delta_k = \frac{P_k}{Q_k} = \frac{P_{k-1} q_k + P_{k-2}}{Q_{k-1} q_k + Q_{k-2}}$$

The substitution of q_k by $q_k + \dfrac{1}{q_{k+1}}$ in the expression for δ_k changes the latter to δ_{k+1} so that

* See I. S. Sominsky, *The Method of Mathematical Induction*, Mir Publishers, Moscow.

$$\delta_{k+1} = \frac{P_{k-1}\left(q_k + \dfrac{1}{q_{k+1}}\right) + P_{k-2}}{Q_{k-1}\left(q_k + \dfrac{1}{q_{k+1}}\right) + Q_{k-2}} = \frac{P_k + \dfrac{1}{q_{k+1}} P_{k-1}}{Q_k + \dfrac{1}{q_{k+1}} Q_{k-1}} =$$

$$= \frac{P_k q_{k+1} + P_{k-1}}{Q_k q_{k+1} + Q_{k-1}}$$

Hence, as $\delta_{k+1} = \dfrac{P_{k+1}}{Q_{k+1}}$, it follows that

$$P_{k+1} = P_k q_k + P_{k-1}, \quad Q_{k+1} = Q_k q_{k+1} + Q_{k-1}$$

Thus, if equalities (7) hold for some $k \geqslant 3$ they are also valid for $k + 1$. For $k = 3$ equalities (7) are indeed satisfied, so they are valid for every $k \geqslant 3$.

Let us now show that the difference between consecutive convergents $\delta_k - \delta_{k-1}$ satisfies the relation

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}} \quad (k > 1) \tag{8}$$

Indeed

$$\delta_k - \delta_{k-1} = \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{P_k Q_{k-1} - Q_k P_{k-1}}{Q_k Q_{k-1}}$$

Using formulae (7) we can transform the numerator of this fraction

$$P_k Q_{k-1} - Q_k P_{k-1} = (P_{k-1} q_k + P_{k-2}) Q_{k-1} -$$
$$- (Q_{k-1} q_k + Q_{k-2}) P_{k-1} = -(P_{k-1} Q_{k-2} - Q_{k-1} P_{k-2})$$

The expression in brackets is obtained from the initial one by replacing k by $k - 1$.

Repeating similar transformations we get a chain of equalities

$$\begin{aligned} P_k Q_{k-1} - Q_k P_{k-1} &= (-1)(P_{k-1} Q_{k-2} - Q_{k-1} P_{k-2}) = \\ &= (-1)^2 (P_{k-2} Q_{k-3} - Q_{k-2} P_{k-3}) = \ldots \\ \ldots &= (-1)^{k-2} (P_2 Q_1 - Q_2 P_1) = \\ &= (-1)^{k-2} (q_1 q_2 + 1 - q_2 q_1) = (-1)^{k-2} \end{aligned}$$

whence it follows that

$$\delta_k - \delta_{k-1} = \frac{P_k Q_{k-1} - Q_k P_{k-1}}{Q_k Q_{k-1}} = \frac{(-1)^{k-2}}{Q_k Q_{k-1}} = \frac{(-1)^k}{Q_k Q_{k-1}}$$

If the expansion of a/b into a continued fraction contains n terms, then the nth convergent δ_n will coincide with a/b. Applying equality (8) for $k = n$, we get

$$\begin{gathered} \delta_n - \delta_{n-1} = \frac{(-1)^n}{Q_n Q_{n-1}} \\ \frac{a}{b} - \delta_{n-1} = \frac{(-1)^n}{bQ_{n-1}} \end{gathered} \tag{9}$$

We return now to the solution of equation

$$ax + by + c = 0, \quad (a, b) = 1 \tag{10}$$

We rewrite relation (9) in the form

$$\frac{a}{b} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^n}{bQ_{n-1}}$$

Reducing the fractions to a common denominator and discarding it we obtain

$$aQ_{n-1} - bP_{n-1} = (-1)^n$$

$$aQ_{n-1} + b(-P_{n-1}) + (-1)^{n-1} = 0$$

Let us multiply this expression by $(-1)^{n-1}c$. Then

$$a[(-1)^{n-1}cQ_{n-1}] + b[(-1)^n cP_{n-1}] + c = 0$$

Hence *the pair of numbers* $[x_0, y_0]$, *such that*

$$x_0 = (-1)^{n-1}cQ_{n-1}, \quad y_0 = (-1)^n cP_{n-1} \tag{11}$$

is a solution of equation (10); *according to theorem 1, all solutions of this equation are of the form*

$$x = (-1)^{n-1}cQ_{n-1} - bt, \quad y = (-1)^n cP_{n-1} + at$$

$$(t = 0, \ \pm 1, \ \pm 2, \ldots)$$

This fully solves the problem of determining all the integral solutions of linear equations in two unknowns.

§ 3. Equations of the Second Degree in Three Unknowns (Examples)

EXAMPLE 1. Consider equation

$$x^2 + y^2 = z^2 \tag{12}$$

From a geometrical point of view, the determination of integral solutions of this equation amounts to finding all Pythagorean triangles, i. e. right triangles whose legs x, y and hypotenuse z are represented by integers.

Let us denote the greatest common divisor of the numbers x and y by d: $d = (x, y)$. Then

$$x = x_1 d, \quad y = y_1 d$$

and equation (12) becomes

$$x_1^2 d^2 + y_1^2 d^2 = z^2$$

This means that z^2 is divisible by d^2, and hence z is a multiple of d: $z = z_1 d$.

Equation (12) can now be written as

$$x_1^2 d^2 + y_1^2 d^2 = z_1^2 d^2$$

Cancelling d^2 we get

$$x_1^2 + y_1^2 = z_1^2$$

This is an equation of the same type as the initial one, (12), only x_1 and y_1 have no common divisors (except, of course, unity). So when solving equation (12) we can restrict ourselves to the case when x and y are relatively prime.

Thus we may suppose that $(x, y) = 1$. Then at least one of the quantities, x and y (say x), is odd. Transferring y^2 into the right-hand side of equation (12) we get

$$x^2 = z^2 - y^2, \quad x^2 = (z + y)(z - y) \tag{13}$$

We shall denote the greatest common divisor of the expressions $z + y$ and $z - y$ by d_1. Then

$$z + y = ad_1, \quad z - y = bd_1 \tag{14}$$

where a and b are relatively prime. Now substituting the values of $z + y$ and $z - y$ into (13) we obtain

$$x^2 = abd_1^2$$

Since a and b possess no common divisors, the latter equality is possible only if these numbers are perfect squares*:

$$a = u^2, \quad b = v^2$$

* The product of two relatively prime numbers is a perfect square only if each factor is a perfect square.

But then

$$x^2 = u^2v^2d_1^2$$

and

$$x = uvd_1 \tag{15}$$

Now determine y and z from equalities (14). Adding them together we get

$$2z = ad_1 + bd_1 = u^2d_1 + v^2d_1; \quad z = \frac{u^2 + v^2}{2}d_1 \tag{16}$$

while subtracting the second one of equations (14) from the first we get

$$2y = ad_1 - bd_1 = u^2d_1 - v^2d_1; \quad y = \frac{u^2 - v^2}{2}d_1. \tag{17}$$

From (15) it follows that, x being odd, u, v and d_1 are also odd. Moreover, $d_1 = 1$, since otherwise from the equations

$$x = uvd_1 \quad \text{and} \quad y = \frac{u^2 - v^2}{2}d_1$$

it would follow that x and y have a common divisor $d_1 \neq 1$, which contradicts the supposition that they are relatively prime. The numbers u and v are connected with the relatively prime numbers a and b by the equations

$$a^2 = u^2, \quad b = v^2$$

and so are relatively prime themselves; $v < u$ since $b < a$, as can be seen from (14).

Substituting $d_1 = 1$ into equalities (15)-(17) we get *formulae*

$$x = uv, \quad y = \frac{u^2 - v^2}{2}, \quad z = \frac{u^2 + v^2}{2} \tag{18}$$

which, with odd and relatively prime u and v ($v < u$), furnish all the triplets of positive integers x, y, z which do not possess common divisors and which satisfy equation (12). By a substitution of the expressions for x, y and z in equation (12), it is easy to verify that for arbitrary u and v the numbers (18) satisfy this equation.

For the initial values of relatively prime u and v, formulae (18) yield the following frequently encountered equalities

$$3^2 + 4^2 = 5^2 \quad (v = 1,\ u = 3)$$

$$5^2 + 12^2 = 13^2 \quad (v = 1,\ u = 5)$$

$$15^2 + 8^2 = 17^2 \quad (v = 3,\ u = 5)$$

As was noted above, formulae (18) give only those solutions of equation

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

in which the numbers x, y and z do not have common divisors. All the rest positive integral solutions of this equation can be obtained by multiplying solutions (18) by an arbitrary common factor d. The method used for determining all the solutions of equation (12) can also be employed to find all the solutions of other equations of the same type.

EXAMPLE 2. Find all the positive integral solutions of equation

$$x^2 + 2y^2 = z^2 \tag{19}$$

if the numbers x, y and z are pairwise relatively prime.

Note that if the triplet x, y, z is a solution of equation (19) and the numbers x, y and z possess no common divisors (except, of course, unity), then they are pairwise relatively prime. Indeed, let x and y be multiples of a prime number p $(p > 2)$. Then from equality

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

with an integral left-hand side it follows that z is a multiple of p. The same conclusion holds if x and z, or y and z are multiples of p.

Notice that x must be an odd number for the greatest common divisor of x, y and z to be equal to unity. For if x is even, then the left-hand side of equation (19) is an even number so that z is also even. But then x^2 and z^2 are multiples of 4. From this it follows that $2y^2$ is divisible by 4, in other words that y must also be an even number. Thus, if x is even then all three numbers x, y, z must be even. Thus, in a solution not having a common divisor different from unity x must be odd. From this it immediately follows that z must also be odd. Transferring x^2 into the right-hand side of equation (19) we get

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

But $z + x$ and $z - x$ have the greatest common divisor 2. Let their greatest common divisor be d. Then

$$z + x = kd, \quad z - x = ld$$

where k and l are integers. Adding together these equalities, then subtracting the second one from the first we arrive at

$$2z = d(k + l), \quad 2x = d(k - l)$$

But z and x are odd and relatively prime. Therefore the greatest common divisor of $2x$ and $2z$ must be equal to 2, that is $d = 2$.

Thus, either $\frac{z + x}{2}$ or $\frac{z - x}{2}$ is odd. Therefore either

$$z + x \quad \text{and} \quad \frac{z - x}{2}$$

are relatively prime or

$$\frac{z + x}{2} \text{ and } z - x$$

are relatively prime.

In the first case equality

$$(z + x)\frac{z - x}{2} = y^2$$

leads to

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

while in the second case from

$$\frac{z + x}{2}(z - x) = y^2$$

it follows that

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

where n and m are positive integers and m is odd. Solving these two systems of equations with respect to x and z, and finding y, we obtain either

$$z = \frac{1}{2}(n^2 + 2m^2), \quad x = \frac{1}{2}(n^2 - 2m^2), \quad y = mn$$

or

$$z = \frac{1}{2}(n^2 + 2m^2), \quad x = \frac{1}{2}(2m^2 - n^2), \quad y = mn$$

respectively, where m is odd. Combining these two expressions we derive the general formulae

$$x = \pm\frac{1}{2}(n^2 - 2m^2), \quad y = mn, \quad z = \frac{1}{2}(n^2 + 2m^2)$$

where m is odd. But for z and x to be integers, n must be even. Putting $n = 2b$ and $m = a$, we finally obtain *general formulae which yield all the solutions of equation* (19) *in positive integers x, y and z having no common divisors greater than unity*:

$$x = \pm(a^2 - 2b^2), \quad y = 2ab, \quad z = a^2 + 2b^2 \tag{19'}$$

where a and b are positive and relatively prime and a is odd. No other restrictions are imposed on a and b except that x should be positive. Formulae (19′) do indeed provide all the solutions in integral and relatively prime x, y and z, since on the one hand we have proved that in this case x, y, z must be represented by formulae (19′), while, on the other hand, any numbers a and b complying with the conditions formulated above furnish such relatively prime numbers x, y, z as constitute a solution of equation (19).

§ 4. Equations of the Type $x^2 - Ay^2 = 1$. Finding All Solutions of This Equation

We now come to the solution in integers of equations of the second degree in two unknowns of the type

$$x^2 - Ay^2 = 1 \tag{20}$$

where A is a positive integer other than a perfect square. To find an approach to the solution of such equations, let us expand irrational numbers such as $\sqrt{A}$ into continued fractions. From Euclid's algorithm it follows that any rational number may be expanded into a continued fraction with a finite number of terms. For irrational numbers the situation is different: their expansions into continued fractions are infinite.

Let us find, for example, the continued fraction expansion of the irrational number $\sqrt{2}$. Consider an obvious identity

$$(\sqrt{2} - 1)(\sqrt{2} + 1) = 1$$

or

$$\sqrt{2} - 1 = \frac{1}{\sqrt{2} + 1}$$

$$\sqrt{2} - 1 = \frac{1}{2 + (\sqrt{2} - 1)}$$

Replacing the difference $\sqrt{2} - 1$ in the denominator of the last identity by the expression

$$\frac{1}{2+(\sqrt{2}-1)}$$

which is obviously equal to it, we receive

$$\sqrt{2}-1=\cfrac{1}{2+\cfrac{1}{2+(\sqrt{2}-1)}};\quad \sqrt{2}=1+\cfrac{1}{2+\cfrac{1}{2+(\sqrt{2}-1)}}$$

Again we replace the bracketed term, in the denominator of the last equation, by the fraction equal to it from the same identity. Then

$$\sqrt{2}=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+(\sqrt{2}-1)}}}$$

Continuing this process, we arrive at the following expansion of $\sqrt{2}$ into an infinite continued fraction

$$\sqrt{2}=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+}}}}\qquad (21)$$
$$\ddots$$

Note that the method of expansion based on identities of the type

$$(\sqrt{m^2+1}-m)(\sqrt{m^2+1}+m)=1$$

is not suitable for all irrational numbers $\sqrt{A}$. It may obviously be used when the integer A may be expressed as $A=m^2+1$ where m is a non-zero integer. (In particular, the case $m=1$ leads to the expansion for $A=\sqrt{2}$, $m=2$ corresponds to $A=\sqrt{5}$ etc.) However, comparatively simple methods also exist for the expansion of $\sqrt{A}$ into continued fractions in the general case.

As before, in the case of finite continued fractions, we shall form for the infinite continued fraction (21) a sequence of convergents $\delta_1, \delta_2, \delta_3, \ldots$

$$\delta_1=1, \qquad\qquad \delta_1<\sqrt{2}$$

$$\delta_2 = 1 + \frac{1}{2} = \frac{3}{2}, \qquad \delta_2 > \sqrt{2}$$

$$\delta_3 = 1 + \cfrac{1}{2 + \cfrac{1}{2}} = \frac{7}{5}, \quad \delta_3 < \sqrt{2} \tag{22}$$

$$\delta_4 = \ldots = \frac{17}{12}, \qquad \delta_4 > \sqrt{2}$$

etc.

From the way these convergents are formed it follows that

$$\delta_1 < \delta_3 < \ldots < \sqrt{2}$$
$$\delta_2 > \delta_4 > \ldots > \sqrt{2}$$

In general, if we are given the continued fraction expansion of some irrational number α

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}}$$

then the convergents satisfy the inequalities

$$\delta_1 < \delta_3 < \ldots < \delta_{2k+1} < \ldots < \alpha < \ldots$$
$$\ldots < \delta_{2k} < \ldots < \delta_4 < \delta_2 \tag{23}$$

Let us write the convergent δ_k as

$$\delta_k = \frac{P_k}{Q_k}$$

Expressions (7)

$$P_k = P_{k-1}q_k + P_{k-2}, \quad Q_k = Q_{k-1}q_k + Q_{k-2}$$

derived in § 2 for the case of finite continued fractions are also valid for infinite fractions, as in the derivation of (7) we did not make use of the fact that the continued fraction was finite. Hence relation (8) between consecutive convergents

$$\delta_k - \delta_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}} \tag{24}$$

also remains valid.

Assume for example $k_1 = 3$ and $k_2 = 4$ and expand $\sqrt{2}$ into a continued fraction. Equalities (22) will then lead to

$$\delta_3 - \delta_2 = \frac{7}{5} - \frac{3}{2} = \frac{-1}{10}$$

$$\delta_4 - \delta_3 = \frac{17}{12} - \frac{7}{5} = \frac{1}{60}$$

which coincides with the results given by formula (24).

Consider now formula (24) for the subscript $2k$:

$$\delta_{2k} - \delta_{2k+1} = -(\delta_{2k+1} - \delta_{2k}) = -\frac{(-1)^{2k+1}}{Q_{2k+1}Q_{2k}} = \frac{1}{Q_{2k+1}Q_{2k}}$$

We shall now prove the validity of inequality

$$0 < P_{2k} - \alpha Q_{2k} < \frac{1}{Q_{2k+1}} \tag{25}$$

The left inequality is obvious, for, according to inequalities (23),

$$\alpha < \delta_{2k} = \frac{P_{2k}}{Q_{2k}}; \quad \alpha Q_{2k} < P_{2k}; \quad 0 < P_{2k} - \alpha Q_{2k}$$

The deduction of the other inequality (25) is also a rather simple procedure. From (23),

$$\delta_{2k+1} < \alpha < \delta_{2k}$$

so

$$\delta_{2k} - \alpha < \delta_{2k} - \delta_{2k+1} = \frac{1}{Q_{2k}Q_{2k+1}}$$

Substituting P_{2k}/Q_{2k} for δ_{2k}, we get

$$\frac{P_{2k}}{Q_{2k}} - \alpha < \frac{1}{Q_{2k}Q_{2k+1}}$$

Multiplying this inequality by Q_{2k} we arrive at the desired result:

$$P_{2k} - \alpha Q_{2k} < \frac{1}{Q_{2k+1}}$$

We now apply the results obtained to the solution of equation

$$x^2 - 2y^2 = 1 \tag{26}$$

Let us transform the left-hand side of this equation:

$$x^2 - 2y^2 = (x - \sqrt{2}y)(x + \sqrt{2}y)$$

and assume $x = P_{2k}$ and $y = Q_{2k}$, where P_{2k} and Q_{2k} are the numerator and the denominator, respectively, of the corresponding convergent in the expansion of $\sqrt{2}$. Then

$$P_{2k}^2 - 2Q_{2k}^2 = (P_{2k} - \sqrt{2}\,Q_{2k})(P_{2k} + \sqrt{2}\,Q_{2k}) \qquad (27)$$

The left-hand side of this equality, and therefore the right-hand side too, is an integer. We shall show that this integer is greater than zero but less than two and so is equal to unity. To do this write inequality (25) for $\alpha = \sqrt{2}$:

$$0 < P_{2k} - \sqrt{2}\,Q_{2k} < \frac{1}{Q_{2k+1}}. \qquad (28)$$

From this it is clear that both factors of the right-hand side of (27) are positive, and so

$$P_{2k}^2 - 2Q_{2k}^2 > 0$$

On the other hand,

$$P_{2k} - \sqrt{2}\,Q_{2k} < \frac{1}{Q_{2k+1}} =$$

$$= \frac{1}{Q_{2k}q_{2k+1} + Q_{2k-1}} = \frac{1}{2\,Q_{2k} + Q_{2k-1}} < \frac{1}{2\,Q_{2k}}$$

But, because of inequalities (23),

$$\delta_{2k} = \frac{P_{2k}}{Q_{2k}} > \sqrt{2}$$

Hence

$$\sqrt{2}\,Q_{2k} < P_{2k}$$

$$P_{2k} + \sqrt{2}\,Q_{2k} < 2\,P_{2k}$$

and the factors on the right-hand side of (27) satisfy inequalities

$$P_{2k} - \sqrt{2}\,Q_{2k} < \frac{1}{2\,Q_{2k}}$$

$$P_{2k} + \sqrt{2}\,Q_{2k} < 2\,P_{2k}$$

Multiplying these inequalities together gives

$$P_{2k}^2 - 2\,Q_{2k}^2 < \frac{P_{2k}}{Q_{2k}}$$

Using inequality (28) we arrive at

$$P_{2k}^2 - 2Q_{2k}^2 < \frac{\sqrt{2}\,Q_{2k} + \dfrac{1}{Q_{2k+1}}}{Q_{2k}} = \sqrt{2} + \frac{1}{Q_{2k}Q_{2k+1}}$$

For any $k \geqslant 1$

$$\frac{1}{Q_{2k}Q_{2k+1}} \leqslant \frac{1}{Q_2Q_3} = \frac{1}{10}$$

therefore

$$P_{2k}^2 - 2Q_{2k}^2 < \sqrt{2} + \frac{1}{10} < 2$$

We have thus proved that for any $k \geqslant 1$ the integer $P_{2k}^2 - 2Q_{2k}^2$ satisfies inequalities

$$0 < P_{2k}^2 - 2Q_{2k}^2 < 2$$

Hence

$$P_{2k}^2 - 2Q_{2k}^2 = 1$$

This means that for any $k \geqslant 1$ the numbers $x = P_{2k}$, $y = Q_{2k}$ yield the solution of the equation

$$x^2 - 2y^2 = 1$$

We do not yet know whether or not the solutions of equation (26) found above are all the solutions of that equation.

The question now naturally arises, how do we find all the solutions of equation

$$x^2 - Ay^2 = 1 \tag{29}$$

in integers x and y for integral $A > 0$ and irrational $\sqrt{A}$? We shall show that we can do this if we can find at least one solution of equation (29). As evidenced by equation (26) such equations do have solutions. So we shall now consider the problem of how to obtain all the solutions of equation (29) from a single particular solution which we shall call a minimum or least solution leaving open for the moment the question of whether or not equation (29) always has at least one solution in integers other than the trivial solution $x = 1$, $y = 0$.

Let us suppose that equation (29) does have a non-trivial solution $[x_0, y_0]$, $x_0 > 0$, $y_0 > 0$, and

$$x_0^2 - Ay_0^2 = 1 \tag{30}$$

(Remember that a solution is a pair of integers $[x_0, y_0]$ satisfying the equation.) We shall call this solution *minimal* if for $x = x_0$ and $y = y_0$ the binomial $x + \sqrt{A}\, y$, $\sqrt{A} > 0$, assumes the least possible value among all the possible values which it will take when all the possible positive integral solutions of equation (29) are substituted for x and y. For example, the least solution of equation (26) is $x = 3$, $y = 2$ because for these values of x and y the binomial $x + \sqrt{2}\, y$ assumes the value $3 + 2\sqrt{2}$. Indeed, equation (26) admits of no other solutions with small positive integers x and y; the smallest values of x and y constitute the next solution: $x = 17$, $y = 12$ and it is clear that $17 + 12\sqrt{2}$ is greater than $3 + 2\sqrt{2}$. Note that *equation* (29) *does not have two least solutions*. For, assume that solutions $[x_1, y_1]$ and $[x_2, y_2]$ give the same value to the binomial $x + \sqrt{A}\, y$. Then

$$x_1 + \sqrt{A}\, y_1 = x_2 + \sqrt{A}\, y_2 \tag{31}$$

However, $\sqrt{A}$ is an irrational number while x_1, y_1, x_2, y_2 are integers. Hence, as it immediately follows from Eq. (31)

$$x_1 - x_2 = (y_2 - y_1)\sqrt{A}$$

which is impossible because $x_1 - x_2$ is an integer and $(y_2 - y_1)\sqrt{A}$, being a product of an integer and an irrational number, is irrational. And we know that an integer cannot be irrational. The contradiction disappears if $x_1 = x_2$ and $y_1 = y_2$, i. e. if we take not two different solutions, but one. Thus, if a least solution does exist, it is unique.

Observe now another very important property of the solutions of equation (29). Let $[x_1, y_1]$ be a solution of this equation. Then

$$x_1^2 - Ay_1^2 = 1$$

or

$$(x_1 + \sqrt{A}y_1)(x_1 - \sqrt{A}y_1) = 1 \tag{32}$$

Now raise both terms of equality (32) to the positive integral power n:

$$(x_1 + \sqrt{A}y_1)^n (x_1 - \sqrt{A}y_1)^n = 1 \tag{33}$$

Raising the factor on the left-hand side to the power n according to the binomial theorem, we get

$$(x_1 + \sqrt{A}y_1)^n = x_1^n + nx_1^{n-1}\sqrt{A}y_1 +$$

$$+ \frac{n(n-1)}{2} x_1^{n-2} A y_1^2 + \ldots + (\sqrt{A})^n y_1^n = x_n + \sqrt{A}\, y_n \tag{34}$$

where x_n and y_n will be integers since the first, the third term, and, in general, the odd terms of the binomial expansion are integers while the even terms are integers multiplied by $\sqrt{A}$. Collecting separately the odd and the even terms of the expansion we obtain (34). We shall now prove that the numbers x_n and y_n will also be a solution of equation (29). The proof is simple: changing the sign of $\sqrt{A}$ in equality (34), we obtain

$$(x_1 - \sqrt{A}y_1)^n = x_n - \sqrt{A}y_n \tag{35}$$

Multiplying (34) and (35) term by term and using expression (33) we finally have

$$(x_1 + \sqrt{A}y_1)^n(x_1 - \sqrt{A}y_1)^n = \\ = (x_n + \sqrt{A}y_n)(x_n - \sqrt{A}y_n) = x_n^2 - Ay_n^2 = 1 \tag{36}$$

or, in other words, $[x_n, y_n]$ *is also a solution of equation* (29).

Now we can prove the basic theorem concerning solutions of equation (29):

THEOREM II. *Any solution of equation* (29)

$$x^2 - Ay^2 = 1$$

with positive A and irrational $\sqrt{A}$ is of the form $[\pm x_n, \pm y_n]$ *where*

$$\left.\begin{aligned} x_n &= \frac{1}{2}[(x_0 + y_0\sqrt{A})^n + (x_0 - y_0\sqrt{A})^n] \\ y_n &= \frac{1}{2\sqrt{A}}[(x_0 + y_0\sqrt{A})^n - (x_0 - y_0\sqrt{A})^n] \end{aligned}\right\} \tag{37}$$

and $[x_0, y_0]$ *is the least solution of the equation.*

Proof. Suppose the converse, namely, that there exists a positive integral solution $[x', y']$ of equation (29) such that the equality

$$x' + \sqrt{A}y' = (x_0 + \sqrt{A}y_0)^n \tag{38}$$

does not hold for any positive integer n. Consider a sequence of numbers

$$x_0 + \sqrt{A}\,y_0,\ (x_0 + \sqrt{A}\,y_0)^2,\ (x_0 + \sqrt{A}\,y_0)^3, \ldots$$

It is a sequence of positive and indefinitely increasing numbers, since $x_0 \geqslant 1$, $y_0 \geqslant 1$ and $x_0 + \sqrt{A}y_0 > 1$.

By definition of $[x_0, y_0]$ as the least solution,

$$x' + \sqrt{A}y' > x_0 + \sqrt{A}y_0$$

there always exists an integer $n \geqslant 1$ such that

$$(x_0 + \sqrt{A}y_0)^n < x' + \sqrt{A}y' < (x_0 + \sqrt{A}y_0)^{n+1} \tag{39}$$

But $x_0 - \sqrt{A}y_0 > 0$ because

$$(x_0 + \sqrt{A}y_0)(x_0 - \sqrt{A}y_0) = x_0^2 - Ay_0^2 = 1 > 0$$

Hence, when all terms of inequalities (39) are multiplied by the same positive number $(x_0 - \sqrt{A}\, y_0)^n$ the inequality signs are retained, and we will have

$$(x_0 + \sqrt{A}y_0)^n(x_0 - \sqrt{A}y_0)^n < (x' + \sqrt{A}y')(x_0 - \sqrt{A}y_0)^n <$$
$$< (x_0 + \sqrt{A}y_0)^{n+1}(x_0 - \sqrt{A}y_0)^n \qquad (40)$$

Since

$$(x_0 + \sqrt{A}y_0)^n(x_0 - \sqrt{A}y_0)^n = (x_0^2 - Ay_0^2)^n = 1 \qquad (41)$$

we have

$$(x_0 + \sqrt{A}y_0)^{n+1}(x_0 - \sqrt{A}y_0)^n = x_0 + \sqrt{A}y_0 \qquad (42)$$

In addition to this

$$(x' + \sqrt{A}y')(x_0 - \sqrt{A}y_0)^n = (x' + \sqrt{A}y')(x_n - \sqrt{A}y_n) =$$
$$= x'x_n - Ay'y_n + \sqrt{A}(y'x_n - x'y_n) = \bar{x} + \sqrt{A}\bar{y} \qquad (43)$$

where $\bar{x}$ and $\bar{y}$ are integers and

$$x_n - \sqrt{A}y_n = (x_0 - \sqrt{A}y_0)^n$$

Making use of relations (41)-(43) and inequalities (40), we obtain inequalities

$$1 < \bar{x} + \sqrt{A}\bar{y} < x_0 + \sqrt{A}y_0 \qquad (44)$$

We shall show that the pair of integers $\bar{x}$ and $\bar{y}$ is a solution of equation (29). To do this, multiply termwise, Eq. (43), i. e. equation

$$\bar{x} + \sqrt{A}\bar{y} = (x' + \sqrt{A}y')(x_0 - \sqrt{A}y_0)^n \qquad (45)$$

and equation

$$\bar{x} - \sqrt{A}\bar{y} = (x' - \sqrt{A}y')(x_0 + \sqrt{A}y_0)^n \qquad (46)$$

which is immediately obtained from (43) by a change of the sign of $\sqrt{A}$. As $[x', y']$ and $[x_0, y_0]$ are solutions of equation (29), the result will be

$$(\bar{x} + \sqrt{A}\bar{y})(\bar{x} - \sqrt{A}\bar{y}) = \bar{x}^2 - A\bar{y}^2 =$$
$$= (x' + \sqrt{A}\, y')(x' - \sqrt{A}\, y')(x_0 + \sqrt{A}\, y_0)^n(x_0 - \sqrt{A}\, y_0)^n =$$
$$= (x'^2 - Ay'^2)(x_0^2 - Ay_0^2)^n = 1 \qquad (47)$$

The last step is to prove that both $\bar{x}$ and $\bar{y}$ are positive. First of all, note that $\bar{x} \neq 0$, otherwise (47) would give us

$$-Ay_0^2 = 1$$

which is impossible because $A > 0$. Moreover, if $y = 0$ the same equality (47) furnishes $\bar{x}^2 = 1$, but inequalities (44) yield $\bar{x} > 1$, a contradiction. Finally, note that the signs of $\bar{x}$ and $\bar{y}$ coincide. For if we suppose that the signs of $\bar{x}$ and $\bar{y}$ are opposite, then those of $\bar{x}$ and $-\bar{y}$ are the same. Let us compare the moduli of the numbers $\bar{x} + \sqrt{A}\bar{y}$ and $\bar{x} - \sqrt{A}\bar{y}$. The modulus of the first number must be less than of the second because, in the first case, two numbers with the same sign are subtracted one from the other while in the second case they are added together. But we already know that

$$\bar{x} + \sqrt{A}\bar{y} > 1$$

and so $\bar{x} - \sqrt{A}\bar{y}$ is also greater than unity in modulus. But

$$(\bar{x} + \sqrt{A}\bar{y})(\bar{x} - \sqrt{A}\bar{y}) = \bar{x}^2 - A\bar{y}^2 = 1$$

and we have arrived at a contradiction, because the product of two numbers, each with modulus greater than unity, must also be greater than unity in absolute value. Hence the signs of the two numbers, $\bar{x}$ and $\bar{y}$, are the same and $\bar{x} \neq 0$ and $\bar{y} \neq 0$. Inequalities (44) lead then directly to the conclusion that $\bar{x} > 0$ and $\bar{y} > 0$. And so, by supposing that there exists a solution $[x', y']$ of equation (29)

$$x^2 - Ay^2 = 1, \quad A > 0$$

such that (38) does not hold for any positive integer n, we have been able to construct another positive integral solution $[\bar{x}, \bar{y}]$ of the same equation ($x > 0$, $y > 0$ are integers) satisfying inequalities (44), which contradict the definition of the least solution $[x_0, y_0]$. We have thus proved that the supposition that there exist solutions not given by formula (38) leads us to a contradiction. In other words we have proved that all solutions of our equation may be obtained from formula (38).

Thus each solution $[x, y]$ of equation (29) may be derived from the expression

$$x + \sqrt{A}y = (x_0 + \sqrt{A}y_0)^n, \quad n \geqslant 0 \tag{48}$$

where $[x_0, y_0]$ is the least solution. Changing the sign of $\sqrt{A}$ in equality (48), we also get equality

$$x - \sqrt{A}y = (x_0 - \sqrt{A}y_0)^n \tag{49}$$

Adding the two equalities, then subtracting the latter from the former, and finally dividing the sum by 2 and the difference by $2\sqrt{A}$, we obtain

$$\left.\begin{aligned} x = x_n &= \frac{1}{2}[(x_0 + \sqrt{A}y_0)^n + (x_0 - \sqrt{A}y_0)^n] \\ y = y_n &= \frac{1}{2\sqrt{A}}[(x_0 + \sqrt{A}y_0)^n - (x_0 - \sqrt{A}y_0)^n] \end{aligned}\right\} \qquad (50)$$

These are explicit expressions for any positive solution $[x, y]$. Each solution can be derived from them by an arbitrary choice of the signs of x_n and y_n.

For example, since we saw above that the least solution of equation $x^2 - 2y^2 = 1$ is $x = 3$, $y = 2$, all the solutions of this equation are contained in formulae

$$x_n = \frac{1}{2}[(3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n]$$

$$y_n = \frac{1}{2\sqrt{2}}[(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n]$$

The least solution [3, 2] corresponds to $n = 1$; for $n = 2$ and 3 the solutions are [17, 12] and [99, 70] respectively, etc.

Note that the numbers x_n and y_n increase with n as terms of a geometrical progression with a common ratio $x_0 + \sqrt{A}y_0$. Indeed

$$0 < x_0 - \sqrt{A}y_0 < 1$$

because

$$(x_0 + \sqrt{A}y_0)(x_0 - \sqrt{A}\,y_0) = 1.$$

Therefore, $(x_0 - \sqrt{A}\,y_0)^n$ tends to zero with increasing n.

Note also that if equation (29) possesses at least one non-trivial solution, or, in other words, at least one solution with $y \neq 0$, then it will also have a least solution and, consequently, all its solutions can be derived from formulae (50). The existence of a non-trivial solution for any positive integer A with $\sqrt{A}$ irrational will be discussed in § 5.

§ 5. Equations of the Second Degree in Two Unknowns: the General Case

We shall prove in this section that for an arbitrary positive integer A with $\sqrt{A}$ irrational, the equation

$$x^2 - Ay^2 = 1 \qquad (51)$$

always has a non-trivial solution; in other words, there exists a pair of non-zero integers x_0 and y_0 satisfying the equation. We shall first describe a method for expanding an arbitrary positive number into a continued fraction. (Previously, when expanding $\sqrt{2}$ into a continued fraction (see § 4), we made use of the special properties of that number.) Let α be any positive number. Then there always exists an integer less than or equal to α, and greater than $\alpha - 1$. This integer is called the *integral part* of α and is denoted by $[\alpha]$. The difference between α and its integral part is called the *fractional part* of α and is designated by $\{\alpha\}$. The relation between these two quantities

$$\alpha - [\alpha] = \{\alpha\}$$

or

$$\alpha = [\alpha] + \{\alpha\} \tag{52}$$

is a direct consequence of their definitions.

Note also that the fractional part of a number, being the difference between a positive number and the greater integer not exceeding it, is nonnegative and always less than unity. For example, the integral part of 27/5 is 5 and its fractional part is 2/5; for $\sqrt{2}$ the respective numbers are 1 and $\sqrt{2} - 1$, for $\sqrt[3]{52}$, 3 and $\sqrt[3]{52} - 3$, etc.

The notions just introduced may be used for the expansion of positive numbers into continued fractions. Suppose

$$[\alpha] = q_1, \quad \{\alpha\} = \frac{1}{\alpha_1}$$

Then

$$\alpha = q_1 + \frac{1}{\alpha_1} \tag{53}$$

As $\{\alpha\}$ is always less than unity, α_1 is always greater than unity. If α were an integer then its fractional part would be equal to zero so that α_1 would be infinite and we would have $\alpha = q_1$. However, as we are discussing the continued fraction expansion of irrational numbers, we can leave aside this particular case and say that α_1 is a positive number greater than unity. With this number α_1 we can proceed as we did with α, and write

$$\alpha_1 = q_2 + \frac{1}{\alpha_2}, \quad q_2 = [\alpha_1], \quad \frac{1}{\alpha_2} = \{\alpha_1\}$$

Repeating this process, we obtain a series

$$\left.\begin{array}{ll}
\alpha = q_1 + \dfrac{1}{\alpha_1}, & q_1 = [\alpha] \\
\alpha_1 = q_2 + \dfrac{1}{\alpha_2}, & q_2 = [\alpha_1] \\
\alpha_2 = q_3 + \dfrac{1}{\alpha_3}, & q_3 = [\alpha_2] \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\
\alpha_{n-1} = q_n + \dfrac{1}{\alpha_n}, & q_n = [\alpha_{n-1}] \\
\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot
\end{array}\right\} \tag{54}$$

For rational numbers α (or, which is the same, for $\alpha = a/b$, where a and b are positive integers) this sequential calculation furnishes the same result as the Euclidean algorithm with integers $q_1, q_2, q_3, \ldots, q_n, \ldots$ being the partial quotients (see formula (6) in § 2). Here, as also in § 2, the process must break off. On the other hand, when α is irrational this process must be infinite. For if α_n were an integer for some n, then α_{n-1} would be rational, and so also $\alpha_{n-2}, \alpha_{n-3}, \ldots$ and, lastly, α_1 would be rational. Consecutive substitutions eliminating $\alpha_1, \alpha_2, \ldots$ $\ldots, \alpha_{n-1}$ from formulae (54) lead to a continued fraction

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{\ddots}{\qquad + \cfrac{1}{q_n + \cfrac{1}{\alpha_n}}}}} \tag{55}$$

or, since n may be taken arbitrarily large, we can write it in the form of an infinite continuous fraction

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{\ddots}{\qquad + \cfrac{1}{q_n +}}}}$$

As mentioned in § 4, relation (8) between the convergents is not dependent on the finiteness or infinity of the continued fraction and so it holds also in this case. From expression (8), as we have seen, follows inequality (25) for even convergents. This inequality will again be used to prove the existence of a solution of equation (51), but the reasoning will be more complicated than in the particular case when $A = 2$.

THEOREM III. *For any positive integer A and irrational $\sqrt{A}$ equation* (51)

$$x^2 - Ay^2 = 1$$

possesses a non-trivial positive solution $[x_0, y_0]$.

Proof. Because of certain complications in the proof of the existence of solutions to equation (51) we shall break up the proof into several steps. The first step will prove the existence of a positive integer k such that equation

$$x^2 - Ay^2 = k \tag{56}$$

has an infinite number of positive integral solutions. Let us consider the binomial $x^2 - Ay^2$. We shall replace x and y respectively by the numerators and denominators of the consecutive even convergents of the irrational number $\alpha = \sqrt{\text{A}}$. Then

$$z_{2n} = P_{2n}^2 - AQ_{2n}^2 = (P_{2n} - \alpha Q_{2n})(P_{2n} + \alpha Q_{2n}) \tag{57}$$

But since

$$0 < P_{2n} - \alpha Q_{2n} < \frac{1}{Q_{2n+1}}$$

it directly follows that

$$0 < P_{2n} + \alpha Q_{2n} = 2\alpha Q_{2n} + P_{2n} - \alpha Q_{2n} < 2\alpha Q_{2n} + \frac{1}{Q_{2n+1}}$$

Let us use the last two inequalities to estimate z_{2n}. By substituting greater quantities for both factors on the right-hand side of (57) we get for z_{2n} the inequality

$$0 < z_{2n} < \frac{1}{Q_{2n+1}}\left(2\alpha Q_{2n} + \frac{1}{Q_{2n+1}}\right) < 2\alpha + 1 \tag{58}$$

since Q_{2n} is less than Q_{2n+1}. If we replace x and y by P_{2n} and Q_{2n} respectively in the binomial

$$z = x^2 - Ay^2$$

z will assume an integral positive value. Thus, all the numbers

$z_2, z_4, \ldots, z_{2n}, \ldots$ will be positive integers, none of which exceed the same number $2\alpha + 1$. But since $\alpha = \sqrt{A}$ is irrational, its continued fraction is infinite and so the sequence of pairs of numbers P_{2n} and Q_{2n} is also infinite. Now since there are not more than $[2\alpha + 1]$ integers between 1 and the number $2\alpha + 1$ (which is definite and does not depend on n), the infinite sequence of positive integers $z_2, z_4, \ldots, z_{2n}, \ldots$ is made up of a finite number of different terms. In other words, the infinite number series $z_2, z_4, \ldots, z_{2n}, \ldots$ is just the sequence of integers $1, 2, 3, \ldots, [2\alpha + 1]$ repeated in some way or other and it is not even necessary for all these integers to occur in the series. Note also that since the quantity of different terms of the infinite series $z_2, z_4, \ldots, z_{2n}, \ldots$ is finite, at least one term (one number), k $(1 \leqslant k \leqslant [2\alpha + 1])$, is repeated an infinite number of times. In other words, among the pairs of numbers $[P_2, Q_2]$, $[P_4, Q_4]$, $\ldots$, $[P_{2n}, Q_{2n}], \ldots$ there is an infinite set of pairs for which $z = x^2 - Ay^2$ assumes the same value k upon substitution of these numbers in place of x and y. Thus, we have proved the existence of a positive integer k for which equation (56) possesses an infinite number of integral solutions $[x, y]$. Let us enumerate once again these number pairs which are solutions of equation (56) for given k denoting them by $[u_1, v_1]$, $[u_2, v_2]$, $\ldots$ $\ldots$, $[u_n, v_n]$, $\ldots$. We will then have

$$u_n^2 - Av_n^2 = k \tag{59}$$

The sequence of pairs $[u_1, v_1]$, $[u_2, v_2]$, $\ldots$, $[u_n, v_n]$, $\ldots$ will of course be part of the sequence of numerators and denominators of the even convergents of α. If we could assert that $k = 1$, then we would have proved that equation (51) has an infinite number of integral solutions. Since we cannot assert this, let us assume that $k > 1$ (in the contrary case when $k = 1$ everything is proved), and go on to the second step of our proof.

We shall now prove that among the pairs of integers $[u_1, v_1]$, $[u_2, v_2]$, $\ldots$, $[u_n, v_n]$, $\ldots$ there will be infinitely many pairs yielding the same remainders when divided by k. To put it another way, we shall prove that there exist two nonnegative integers, p and q, both less than k, such that for an infinite number of pairs $[u_1, v_1]$, $[u_2, v_2]$, $\ldots$, $[u_n, v_n]$, $\ldots$ the equalities

$$u_n = a_n k + p, \quad v_n = b_n k + q \tag{60}$$

hold, where a_n and b_n are the quotients upon division of u_n and v_n by k, and p and q the remainders. For, if we divide u_n and v_n by the integer k, $k > 1$, then we obtain relations of the form (60), where as always the remainders upon division lie between zero and $k-1$. Since the only possible remainders upon the division of the numbers u_n by k are the numbers $0, 1, 2, \ldots, k-1$, and likewise the remainders upon the division of v_n by k can only be these same numbers $0, 1, 2, \ldots, k-1$, then the number of possible pairs of remainders upon the division of the numbers u_n and v_n by k will be $k \cdot k = k^2$. This is also obvious because a pair of remainders $[p_n, q_n]$ corresponds to each pair $[u_n, v_n]$ and the number of different values assumed by each of the numbers p_n and q_n separately is not greater than k. Consequently, the number of different pairs of remainders is not greater than k^2. Thus to each pair of integers $[u_n, v_n]$ there corresponds a pair of remainders $[p_n, q_n]$ on division by k. But the number of different pairs of remainders is finite, does not exceed k^2, while the number of pairs $[u_n, v_n]$ is infinite. This means that since the number of different pairs in the sequence $[p_1, q_1], [p_2, q_2], \ldots, [p_n, q_n], \ldots$ is finite, at least one pair of remainders is repeated an infinite number of times. Denoting this pair of remainders $[p, q]$, we see that there exists an infinite set of pairs $[u_n, v_n]$ for which relations (60) hold. Since not all the pairs satisfy (60) for certain definite p and q, whose existence we have just proved, we shall renumber all those pairs $[u_n, v_n]$ which satisfy (60) denoting them by $[R_n, S_n]$. And so, the infinite sequence of pairs $[R_1, S_1], [R_2, S_2], \ldots, [R_n, S_n], \ldots$ is a subsequence of the sequence $[u_n, v_n]$ which, in turn, is a subsequence of the sequence of numerators and denominators of the even convergents of α. The pairs of numbers $[R_1, S_1], [R_2, S_2], \ldots, \ldots, [R_n, S_n], \ldots$ satisfy equation (59) and yield the same remainders, p and q, on division by k.

Now that we have established the existence of an infinite set of such pairs of positive integers R_n and S_n, we can go on to the third and last step of our proof. Note first of all that the pairs $[R_n, S_n]$, being the numerators and denominators of convergents, must be pairs of relatively prime numbers, i. e. pairs of numbers which do not possess common divisors. Indeed, if we replace k by $2k$ in relation (24) and set $\delta_{2k} = \frac{P_{2k}}{Q_{2k}}$, $\delta_{2k-1} = \frac{P_{2k-1}}{Q_{2k-1}}$, then from the equation

$$\frac{P_{2k}}{Q_{2k}} - \frac{P_{2k-1}}{Q_{2k-1}} = \frac{1}{Q_{2k}Q_{2k-1}}$$

multiplying both sides by $Q_{2k}Q_{2k-1}$, we get

$$P_{2k}Q_{2k-1} - Q_{2k}P_{2k-1} = 1 \qquad (61)$$

This relation between four integers, P_{2k}, Q_{2k}, P_{2k-1} and Q_{2k-1}, shows that if P_{2k} and Q_{2k} have a common divisor greater than unity, then its whole left-hand side must be divisible by this common divisor. But the right-hand side of equality (61) is unity, which cannot be divided by any integer greater than unity. Thus it is established that the numbers R_n and S_n, which can only be the numerators and denominators of convergents, are relatively prime. From relation (7) it also immediately follows that

$$Q_2 < Q_4 < \ldots < Q_{2n} < \ldots$$

From the fact that the numbers R_n and S_n are relatively prime and from the fact that the numbers $S_1, S_2, \ldots, S_n, \ldots$, which are taken from the sequence of numbers Q_{2n} all differing from one another, are also all different from one another, it immediately follows that in the infinite sequence of fractions

$$\frac{R_1}{S_1}, \cdot \frac{R_2}{S_2}, \ldots, \frac{R_n}{S_n}, \ldots$$

there are no numbers equal to one another. Let us write two equalities following from the definition of the numbers R_n and S_n:

$$R_1^2 - AS_1^2 = (R_1 - \alpha S_1)(R_1 + \alpha S_1) = k \qquad (62)$$

and

$$R_2^2 - AS_2^2 = (R_2 - \alpha S_2)(R_2 + \alpha S_2) = k \qquad (63)$$

where, as above, $\alpha = \sqrt{A}$.

Also,

$$(R_1 - \alpha S_1)(R_2 + \alpha S_2) = R_1R_2 - AS_1S_2 + \alpha(R_1S_2 - S_1R_2) \qquad (64)$$

since $\alpha^2 = A$. Similarly

$$(R_1 + \alpha S_1)(R_2 - \alpha S_2) = R_1R_2 - AS_1S_2 - \alpha(R_1S_2 - S_1R_2) \quad (65)$$

When divided by k, R_n and S_n leave remainders p and q independent of n. Consequently, because of relations (60),

$$R_n = c_nk + p, \quad S_n = d_nk + q \qquad (66)$$

A series of easy transformations and substitutions leads to

$$\begin{aligned} R_1R_2 - AS_1S_2 &= R_1(c_2k + p) - AS_1(d_2k + q) = \\ &= R_1[(c_2 - c_1)k + c_1k + p] - AS_1[(d_2 - d_1)k + d_1k + q] = \\ &= R_1[(c_2 - c_1)k + R_1] - AS_1[(d_2 - d_1)k + S_1] = \qquad (67) \\ &= k[R_1(c_2 - c_1) - AS_1(d_2 - d_1)] + R_1^2 - AS_1^2 = \\ &= k[R_1(c_2 - c_1) - AS_1(d_2 - d_1) + 1] = kx_1 \end{aligned}$$

where x_1 is an integer because $R_1^2 - AS_1^2 = k$. Analogously

$$\begin{aligned} &R_1S_2 - S_1R_2 = \\ &= R_1\left[(d_2 - d_1)k + d_1k + q\right] - S_1\left[(c_2 - c_1)k + c_1k + p\right] = \\ &= R_1\left[(d_2 - d_1)k + S_1\right] - S_1\left[(c_2 - c_1)k + R_1\right] = \\ &= k\left[R_1(d_2 - d_1) - S_1(c_2 - c_1)\right] = ky_1 \end{aligned} \tag{68}$$

where y_1 is again an integer. We can assert that y_1 is not equal to zero. For suppose $y_1 = 0$, then

$$ky_1 = R_1S_2 - R_2S_1 = 0$$

whence

$$\frac{R_1}{S_1} = \frac{R_2}{S_2}$$

which is impossible as we established that all the fractions R_n/S_n are different.

Equalities (67) and (65) show that

$$(R_1 - \alpha S_1)(R_2 + \alpha S_2) = kx_1 + \alpha ky_1 = k(x_1 + \alpha y_1) \tag{69}$$

and

$$(R_1 + \alpha S_1)(R_2 - \alpha S_2) = kx_1 - \alpha ky_1 = k(x_1 - \alpha y_1) \tag{70}$$

Multiplying (62) and (63) termwise and taking into account expressions (69) and (70), we arrive at

$$\begin{aligned} &k^2 = (R_1^2 - AS_1^2)(R_2^2 - AS_2^2) = \\ &\quad = (R_1 - \alpha S_1)(R_2 + \alpha S_2)(R_1 + \alpha S_1)(R_2 - \alpha S_2) = \\ &\quad = k_2(x_1 + \alpha y_1)(x_1 - \alpha y_1) = k^2(x_1^2 - Ay_1^2) \end{aligned} \tag{71}$$

Cancelling k^2 out of the result, we finally get

$$x_1^2 - Ay_1^2 = 1 \tag{72}$$

But $y_1 \neq 0$ which means that $x_1 \neq 0$, otherwise the left-hand side would be negative while the right-hand side would be equal to unity. Thus, even under the assumption that $k \neq 1$, we have determined two non-zero integers, x_1 and y_1, which satisfy equation (51). The theory of equations of this type is now complete since we know that they do possess a solution for any positive integer A and irrational $\sqrt{A}$; and we know how to construct all the solutions with the aid of the least solution whose existence has been proved.

In practice the least solutions should be sought by trial and error, choosing the values of x_0 and y_0.

We have fully treated the equation

$$x^2 - Ay^2 = 1$$

when $A > 0$ and $\alpha = \sqrt{A}$ is irrational.

If $A > 0$ and $\alpha = \sqrt{A}$ is an integer, then this equation may be written in the form

$$x^2 - \alpha^2 y^2 = (x + \alpha y)(x - \alpha y) = 1$$

and since α is an integer and x_0, y_0 are integers satisfying the equation, we must have

$$x_0 + \alpha y_0 = 1, \quad x_0 - \alpha y_0 = 1$$

or

$$x_0 + \alpha y_0 = -1, \quad x_0 - \alpha y_0 = -1$$

because the product of two integers is unity if and only if each of these integers is either $+1$ or -1. Each of the systems of two equations in two unknowns x_0 and y_0 admits of only trivial integral solutions, $x_0 = 1$, $y_0 = 0$ and $x_0 = -1$, $y_0 = 0$ respectively. *Hence, when A is equal to the square of an integer, equation* (51) *has only trivial solutions in integers* $x_0 = \pm 1$, $y_0 = 0$. *When A is a negative integer, equation* (51) *has the same trivial integral solutions.* (When $A = -1$, it also has the (symmetrical) trivial solutions $x_0 = 0$, $y_0 = \pm 1$.)

Let us now consider a more general equation

$$x^2 - Ay^2 = C \tag{73}$$

where A and C are integers, A is positive and $\alpha = \sqrt{A}$ is irrational. We have already seen that when $C = 1$ this equation always possesses an infinite number of integral solutions (see Theorem III). But for arbitrary values of C and A, this equation may not have a solution at all.

EXAMPLE. Show that the *equation*

$$x^2 - 3y^2 = -1 \tag{74}$$

possesses no integral solution. First note that the square of an odd number, when divided by 8, always leaves a remainder equal to 1. Indeed, since any odd number α may be written as $a = 2N + 1$, where N is an integer, we have

$$a^2 = (2N + 1)^2 = 4N^2 + 4N + 1 = 4N(N + 1) + 1 = 8M + 1 \tag{75}$$

where M is an integer, as either N or $N+1$ must be even. Suppose now that $[x_0, y_0]$ is a solution of equation (74). Then the two numbers, x_0 and y_0, cannot have the same parity, that is, one must be even, and the other odd. If x_0 and y_0 were both either even or odd, then $x_0^2 - 3y_0^2$ would be an even number and could not be equal to 1. If x_0 were odd, and y_0 even, then x_0^2 divided by 4 would leave a remainder of 1, while $-3y_0^2$ would be divisible by 4. Hence the remainder upon the division of $x_0^2 - 3y_0^2$ by 4 would be unity. This is impossible because the right-hand side of equation (74), when divided by 4, leaves a remainder of -1 or $3 = 4 - 1$. Lastly, if x_0 is even and y_0 is odd, then x_0^2 is divisible by 4, and, according to (75), $-3y_0^2$ may be written in the form

$$-3y_0^2 = -3(8M+1) = -24M - 3 = 4(-6M-1)+1$$

and so yields a remainder of 1 when divided by 4. Hence once again the remainder upon the division of $x_0^2 - 3y_0^2$ by 4 must be 1, which is impossible, as we have seen. Thus, no integers x_0, y_0 can satisfy equation (74).

We shall not consider the problem of specifying conditions, imposed on C and A, under which equation (73) will have solutions. It is a difficult one and is solved with the aid of the general theory of quadratic irrationalities which belongs to the algebraic number theory. We shall only discuss the case when equation (73) has non-trivial solutions. As above, we shall call a solution $[x', y']$ non-trivial if $x', y' \neq 0$.

Thus, suppose equation (73) admits of a non-trivial solution $[x', y']$, in other words, suppose that

$$x'^2 - Ay'^2 = C \tag{76}$$

Consider for the same A equation

$$x^2 - Ay^2 = 1 \tag{77}$$

For $A > 0$ and $\alpha = \sqrt{A}$ irrational this latter equation possesses an infinite number of integral solutions $[\bar{x}, \bar{y}]$, each of which may be determined by

$$\bar{x} = \pm x_n, \quad \bar{y} = \pm y_n$$

where x_n and y_n are determined by formulae (50) of § 4. Since $[\bar{x}, \bar{y}]$ is a solution of equation (77),

$$\bar{x}^2 - A\bar{y}^2 = (\bar{x} + \alpha\bar{y})(\bar{x} - \alpha\bar{y}) = 1$$

In its turn, equality (76) can be written as

$$(x' + \alpha y')(x' - \alpha y') = C$$

Multiplying the last two equations term by term we get

$$(x' + \alpha y')(\bar{x} + \alpha\bar{y})(x' - \alpha y')(\bar{x} - \alpha\bar{y}) = C \tag{78}$$

But

$$(x' + \alpha y')(\bar{x} + \alpha\bar{y}) = x'\bar{x} + Ay'\bar{y} + \alpha(x'\bar{y} + y'\bar{x})$$

and, similarly,

$$(x' - \alpha y')(\bar{x} - \alpha\bar{y}) = x'\bar{x} + Ay'\bar{y} - \alpha(x'\bar{y} + y'\bar{x})$$

Using these two results, we can rewrite (78) in the form

$$[x'\bar{x} + Ay'\bar{y} + \alpha(x'\bar{y} + y'\bar{x})][x'\bar{x} + Ay'\bar{y} - \alpha(x'\bar{y} + y'\bar{x})] = C$$

or as

$$(x'\bar{x} + Ay'\bar{y})^2 - A(x'\bar{y} + y'\bar{x})^2 = C$$

We have thus proved that if $[x', y']$ is a solution of equation (73) then this equation is also satisfied by the pair of numbers $[x, y]$,

$$x = x'\bar{x} + Ay'\bar{y}, \quad y = x'\bar{y} + y'\bar{x} \tag{79}$$

where $[\bar{x}, \bar{y}]$ is an arbitrary solution of equation (77). Therefore we have proved that *if equation* (73) *has at least one solution then it has an infinite number of solutions.*

We must not assert of course that formulae (79) provide all the solutions of equation (73). In the theory of algebraic numbers it is proved that all the integral solutions of equation (73) may be obtained by taking a certain finite number of solutions, depending on A and C, and generating them with the aid of formulae (79). When A is negative or equal to the square of an integer, equation (73) cannot have more than a finite number of solutions. The proof of this proposition is simple and we leave it for the reader. The solutions in integers of the most general equation of the second degree in two unknowns

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0 \tag{80}$$

where A, B, C, D, E, and F are integers, may be reduced, by change of variables, to the solution of equations of type (73) with a positive or negative A. Hence the behaviour of the solutions, if they exist, is the same as that for equations of type (73).

Summing up what has been proved, we can say that *equations of the second degree in two unknowns of type* (80) *may either have no integral solutions at all, or have only a finite number of solutions, or they may have an infinite number of solutions. In the* *last case all the solutions can be obtained from a finite number of generalized geometric progressions* (79). A comparison of the behaviour of integral solutions of equations of the second degree in two unknowns with the behaviour of the solutions of linear equations reveals an extremely important fact. Whereas the solutions of linear equations, if they exist, form arithmetic progressions, the solutions of equations of the second degree, when they are infinite in number, are taken from a finite number of generalized geometric progressions. In other words, pairs of integers which provide solutions of an equation of the second degree occur much less frequently than in the case of linear equations. This is not accidental. It turns out that equations in two unknowns of degree higher than the second, generally speaking, have only a finite number of solutions. Exceptions to this rule are extremely rare.

§ 6. Equations in Two Unknowns of Degree Higher Than the Second

Equations in two unknowns of degree higher than the second almost always, with rare exceptions, have only a finite number of solutions in integers x and y. Let us consider first of all equation

$$a_0x^n + a_1x^{n-1}y + a_2x^{n-2}y^2 + \ldots + a_ny^n = c \qquad (81)$$

where n is an integer greater than two and all the numbers a_0, a_1, a_2, $\ldots$, a_n and c are integers.

At the beginning of this century, A. Thue proved that *this equation possesses only a finite number of solutions in integers x and y, with the possible exception of cases when the homogeneous left-hand side is a power*

(1) *of a homogeneous linear binomial*

$$(ax + by)^n = c_0$$

or (2) *of a homogeneous quadratic trinomial*

$$(ax^2 + bxy + cy^2)^n = c_0$$

In both these instances integral solutions can exist only if c_0 is the nth power of some integer and, consequently, if equation (81) reduces to an equation of the first or of the second degree respectively.

Thue's method is too complicated for us to describe here. We shall confine ourselves to a few notes explaining how the finiteness of the number of solutions of equation (81) is demonstrated.

Divide both sides of equation (81) by y^n, then

$$a_0\left(\frac{x}{y}\right)^n + a_1\left(\frac{x}{y}\right)^{n-1} + \ldots + a_{n-1}\frac{x}{y} + a_n = \frac{c}{y^n} \qquad (82)$$

For the sake of simplicity we shall suppose not only that all the roots of the equation

$$a_0z^n + a_1z^{n-1} + \ldots + a_{n-1}z + a_n = 0 \qquad (83)$$

are different from one another and $a_0a_n \neq 0$, but also that these roots cannot be the solutions of any equations of a lower degree with integral coefficients. This case is the essential one for our discussion.

In courses of higher algebra it is proved that any algebraic equation has at least one root, whence, since any polynomial in z is divisible by $z - \alpha$ if α is its root, it follows very simply that any polynomial may be represented as

$$a_0z^n + a_1z^{n-1} + \ldots + a_n = a_0(z - \alpha_1)(z - \alpha_2)\ldots(z - \alpha_n) \qquad (84)$$

where α_1, α_2, ..., α_n are its n (different) roots. Using this expression for a polynomial in the form of a product, we can rewrite equation (82) in the form

$$a_0\left(\frac{x}{y} - \alpha_1\right)\left(\frac{x}{y} - \alpha_2\right)\ldots\left(\frac{x}{y} - \alpha_n\right) = \frac{c}{y^n} \qquad (85)$$

Suppose there exist an infinite number of integral solutions $[x_k, y_k]$ to equation (85). This means that there exist solutions with y_k arbitrarily large in absolute value. If there existed an infinite number of pairs with y_k bounded, less in absolute value than some definite number, and with x_k arbitrarily large, then there would be a contradiction, as with such x_k the left-hand side would be arbitrarily large, while the right-hand side would remain bounded. Now suppose y_k is a very large number. Then the right-hand side of equation (85) will be small and this means its left-hand side must also be small. But the left-hand side of the equation is a product of n factors containing x_k/y_k and a_0 which, being an integer, is not less than unity. Consequently, the left term can become small only if at least one of the factors

$$\frac{x_k}{y_k} - \alpha_m$$

is small in modulus. Clearly, this difference can be small only when α_m is real, in other words, when the relation $\alpha_m = a + bi$,

$b \neq 0$ does not hold. In the opposite case the modulus of our difference cannot be arbitrarily small, since

$$\left|\frac{x_k}{y_k} - a - bi\right| = \sqrt{\left(\frac{x_k}{y_k} - a\right)^2 + b^2} > |b|$$

Two differences, that is two factors of the left member of equation (85), cannot be small in modulus simultaneously because

$$\left|\left(\frac{x_k}{y_k} - \alpha_m\right) - \left(\frac{x_k}{y_k} - \alpha_s\right)\right| = |\alpha_m - \alpha_s| \neq 0 \qquad (86)$$

as the numbers α_m are all different. If one of the two factors is less in modulus than $\frac{1}{2}|\alpha_m - \alpha_s|$, then, because of relation (86), the other one must be greater than $\frac{1}{2}|\alpha_m - \alpha_s|$. This is a consequence of the fact that the absolute value of a sum does not exceed the sum of the absolute values. Since the numbers α_m are all different, the smallest difference in absolute values, $|\alpha_m - \alpha_s|$, will be greater than zero ($m \neq s$). Denoting it by $2d$, we will have that if for some sufficiently large y_k (which we can assume since y_k increases indefinitely),

$$\left|\frac{x_k}{y_k} - \alpha_m\right| < d$$

then

$$\left|\frac{x_k}{y_k} - \alpha_s\right| > d, \quad s = 1, 2, \ldots, n, \quad s \neq m \qquad (87)$$

Then, since the modulus of a product is equal to the product of the moduli of its factors, it follows from equation (85) that

$$|a_0|\left|\frac{x_k}{y_k} - \alpha_1\right| \ldots \left|\frac{x_k}{y_k} - \alpha_{m-1}\right|\left|\frac{x_k}{y_k} - \alpha_m\right|\left|\frac{x_k}{y_k} - \alpha_{m+1}\right| \ldots$$

$$\ldots\left|\frac{x_k}{y_k} - \alpha_n\right| = \frac{|c|}{|y_k|^n} \qquad (88)$$

If in this equation we replace each of the differences $\left|\frac{x_k}{y_k} - \alpha_s\right|$, $s \neq m$ by the smaller quantity d and replace $|a_0|$ by unity, which must be smaller than the integer $| a_0 |$, then the left-hand side of equality (88) will become less than the right-hand side, and we get the inequality

$$d^{n-1}\left|\frac{x_k}{y_k} - \alpha_m\right| < \frac{|c|}{|y_k|^n}$$

or

$$\left|\frac{x_k}{y_k} - \alpha_m\right| < \frac{c_1}{|y_k|^n}, \quad c_1 = \frac{|c|}{d^{n-1}} \qquad (89)$$

where c_1 does not depend on x_n and y_n. There are not more than n numbers α_m, while the set of pairs $[x_k, y_k]$ which satisfy inequality (89) for some m is infinite. Therefore, there exists a certain m for which, with the corresponding α_m, this inequality is valid an infinite number of times. In other worlds, if equation (81) has an infinite number of integral solutions, then the algebraic equation (83) with integral coefficients possesses a root α for which inequality

$$\left|\alpha - \frac{p}{q}\right| < \frac{A}{q^n} \qquad (90)$$

holds for arbitrarily large values of q. Here, p and q are integers, A is a constant, independent of them, and n is the degree of an equation of which α is a root.

If α were an arbitrary real number, it would have been possible to choose it so that there were indeed an infinite number of solutions to equation (90) in integers p and q. But in our case α is the root of an algebraic equation with integral coefficients. Such numbers are called *algebraic* and they possess special properties. The *degree of an algebraic number* is the degree of the algebraic equation of least degree with integral coefficients, which is satisfied by this number.

A. Thue proved that for an algebraic number α of degree n the inequality

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\frac{n}{2}+1}}, \quad n \geqslant 3 \qquad (91)$$

can have only a finite number of integral solutions $[p, q]$. But if $n \geqslant 3$ the right-hand side of inequality (90) for a sufficiently large q will become less than the right-hand side of inequality (91) since $n > \frac{n}{2} + 1$. Therefore, if inequality (91) can have only a finite number of solutions in integers p and q, then inequality (90) must certainly have only a finite number of solutions. This means that equation (81) can have only a finite number of solutions in integers when all the roots of equation (83) cannot be roots of an equation with integral coefficients of degree lower than n. It is not difficult to ascertain that for $n = 2$ and given A inequality (90) does indeed have an infinite number of integral solutions in p and q. The theorem by A. Thue was subsequently strengthened significantly. It should be mentioned that the method he used to prove his theorem did not allow him to find an upper bound for the solutions, in other words, a bound for the possible values of $|x|$ and $|y|$ for given coefficients $a_0, a_1, \ldots, a_n$ and c. This question still remains open. However, the method due to Thue enables us to discover an upper bound, though a rather crude one, for the number of solutions of equation (83). For certain classes of equations of type (83) this bound may be made much more precise. For example, the Soviet mathematician B. N. Delone proved that, except for the trivial solution [0, 1], equation

$$ax^3 + y^3 = 1$$

where a is an integer, cannot have more than one integral solution $[x, y]$. He also demonstrated that equation

$$ax^3 + bx^2y + cxy^2 + dy^3 = 1$$

where the coefficients a, b, c, d are integers can have no more than five solutions.

Let now $P(x, y)$ denote an arbitrary polynomial in x and y with integral coefficients A_{ks}:

$$P(x, y) = \sum A_{ks}x^k y^s$$

We shall say that the *polynomial is irreducible* if it cannot be represented as a product of two other polynomials with integral coefficients, each of which is not equal to a number.

By using a special and extremely complicated method Siegel proved that equation

$$P(x, y) = 0$$

where $P(x, y)$ is an irreducible polynomial in x and y of degree higher than the second (i. e. a polynomial which includes terms, or a single term, $A_{ks}x^k y^s$ with $k + s > 2$), may have an infinite number of integral solutions $[x, y]$ only when there exist numbers $a_n, a_{n-1}, \ldots, a_0, a_{-1}, \ldots, a_{-n}$ and $b_n, b_{n-1}, \ldots, b_0, b_{-1}, \ldots, b_{-n}$, where n is some integer, such that when expressions where n is some integer, such that when expressions

$$x = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_0 + \frac{a_{-1}}{t} + \ldots + \frac{a_{-n}}{t^n}$$

$$y = b_n t^n + b_{n-1} t^{n-1} + \ldots + b_0 + \frac{b_{-1}}{t} + \ldots + \frac{b_{-n}}{t^n}$$

are substituted into our equation for x and y an identity

$$P(x, y) \equiv 0$$

is obtained with respect to t.

§ 7. Algebraic Equations in Three Unknowns of Degree Higher Than the Second. Some Exponential Equations

Is the number of integral solutions of an equation finite or not? Though we can give an answer to this question for equations in two unknowns, we can only answer it for very particular types of equations in three or more unknowns of degree higher than the second. Nevertheless, in these particular cases a more difficult problem of actually determining all the integral solutions can be solved. Consider for example the so-called Fermat's last theorem. Pierre Fermat, an eminent French mathematician, asserted that for any integer $n \geqslant 3$ equation

$$x^n + y^n = z^n \tag{92}$$

has no solutions in positive integers x, y, z. The case $xyz = 0$ is excluded by the requirement that the unknowns be positive. He even claimed to have a proof of this proposition (evidently, using the method of infinite descent, see below), but it has never been found. When the German mathematician E. Kummer subsequently attempted to prove Fermat's theorem, he for some time thought he has succeeded. However he discovered that one proposition, correct for usual integers, does not hold for the more complicated number formations which naturally arise in research connected with the problem. This was that the factorization of what are called *algebraic integers*, in other words, roots of algebraic equations with integral rational coefficients and with a unit coefficient of the leading term, into undecomposable prime integral factors of the same algebraic nature is not unique. The factorization of the ordinary integers is of course unique. For example, $6 = 2 \cdot 3$, with no other factorization being possible in the domain of ordinary integers.

Consider now the set of all algebraic integers of the type

$m + n\sqrt{-5}$ where m and n are ordinary integers, and note that both the sum and the product of two such numbers are again numbers of the same set. A set of numbers which contains any sums and products of the numbers in it is called a *ring.* By definition the ring under discussion contains the numbers 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$. It is easy to ascertain that each of these numbers is a prime; none of them can be represented as a product of two integers of the ring neither of which are equal to unity. However,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

so that in our ring the number 6 does not factorize uniquely into prime factors.

Non-uniqueness in the factorization into prime factors also occurs in other, more complicated, rings of algebraic integers. Having discovered this, Kummer realized that his proof of Fermat's theorem in the general case was false. In order to overcome the difficulties connected with the non-uniqueness of the factorization into factors Kummer constructed the theory of ideals, which is extremely important in modern algebra and number theory. Even with the aid of his new theory, Kummer was unable to prove Fermat's theorem in the general case, and proved it only for those n which are divisible by at least one of what are known as regular prime numbers. We shall not go into what is meant by the concept of regular prime number. It is not even known at the present time whether there is a finite number of regular prime numbers or infinitely many of them.

At the present time, Fermat's last theorem has been proved for many values of n and, in particular, for any n divisible by a prime number less than 100. Fermat's last theorem turned out to be extremely important for the development of mathematics in general because the attempts to prove it led to the discovery of the theory of ideals. It should be mentioned that this theory was independently constructed in quite another way and for a different reason by E. I. Zolotarev, an eminent Russian mathematician who regrettably died in the prime of his creative life. These days, a proof of Fermat's last theorem, especially a proof based on the concepts of the theory of divisibility of numbers, would have only curiosity value. If, however, a proof were attained by a new and fruitful method, then its importance, or, rather, the importance of the method itself, might be quite great. Even now amateurs continue to attack Fermat's theorem by elementary methods. All such attempts are doomed to failure. Elementary arguments proceeding from the theory of divisibility of numbers were used by Kummer and were further developed by some of the most eminent mathematicians, yet nothing important was obtained.

We shall now prove Fermat's theorem for the case $n = 4$, since the *method of infinite descent* on which the proof is based is very interesting.

THEOREM IV. *Fermat's equation*

$$x^4 + y^4 = z^4 \tag{93}$$

has no solutions in integers x, y, z, $xyz \neq 0$.

Proof. We shall prove an even stronger proposition, namely, that equation

$$x^4 + y^4 = z^2 \tag{94}$$

has no solution in integers x, y, z, $xyz \neq 0$. From this theorem it immediately follows that equation (93) has no solution. If equation (94) has a solution in non-zero integers x, y, z, then we may assume that these numbers are pairwise relatively prime. For if there is a solution in which x and y have a greatest common divisor $d > 1$, then

$$x = dx_1, \quad y = dy_1$$

where $(x_1, y_1) = 1$. Dividing both sides of equation (94) by d^4, we have

$$x_1^4 + y_1^4 = \left(\frac{z}{d^2}\right)^2 = z_1^2 \tag{95}$$

But x_1 and y_1 are integers, therefore $z_1 = z/d^2$ is also an integer. Now, if z_1 and y_1 had a common divisor $k > 1$, then, because of expression (95), x_1^2 would have to be divisible by k, which means x_1 and k could not have been relatively prime. Hence we have proved that if there exists a solution to equation (94) in non-zero integers, then there also exists a solution in non-zero and pairwise relatively prime integers. Therefore it is sufficient for us to prove that equation (94) does not have solutions in non-zero pairwise relatively prime integers. In the following proof, when we say that equation (94) has a solution, we mean that it has a solution in positive pairwise relatively prime integers.

In § 3 we proved that all the positive integral and pairwise relatively prime solutions of equation (12)

$$x^2 + y^2 = z^2 \tag{96}$$

are determined by formula (18) and have the form

$$x = uv, \quad y = \frac{u^2 - v^2}{2}, \quad z = \frac{u^2 + v^2}{2} \tag{97}$$

where u and v are any pair of odd and relatively prime positive numbers.

Let us give another form for formulae (97) determining all the solutions of equation (96). Since u and v are odd numbers, then setting

$$\frac{u+v}{2}=a, \quad \frac{u-v}{2}=b \tag{98}$$

we determine u and v by

$$u=a+b, \quad v=a-b \tag{99}$$

where a and b are integers with different parity (one is even and the other odd). Equalities (98) and (99) show that to any pair of odd and relatively prime numbers u and v there corresponds a pair of relatively prime numbers a and b of different parity and that to any pair of relatively prime numbers a and b of different parity there corresponds a pair of relatively prime odd numbers u and v. Therefore substituting a and b for u and v respectively in formulae (97) we find that all the triplets of positive and pairwise relatively prime integers x, y, z (x odd), which are solutions of equation (96), are determined by formulae

$$x=a^2-b^2, \quad y=2ab, \quad z=a^2+b^2 \tag{100}$$

where a and b are any two relatively prime numbers of different parity, on the condition that $x>0$. These formulae show that the two numbers, x and y, are of different parity. Now, if $[x_0, y_0, z_0]$ is a solution of equation (94), then

$$[x_0^2]^2+[y_0^2]^2=z_0^2$$

so that the triplet $[x_0^2, y_0^2, z_0]$ satisfies equation (96). But then there must exist two relatively prime numbers a and b, $a>b$, of different parity, such that

$$x_0^2=a^2-b^2, \quad y_0^2=2ab, \quad z_0=a^2+b^2 \tag{101}$$

We have assumed here for the sake of definiteness that x_0 is odd and y_0 even. In the contrary case nothing is changed since x_0 could be changed for y_0 and vice versa. We already known from equality (75) of § 5 that the square of an odd number divided by 4 leaves a remainder of 1. Therefore from equality

$$x_0^2=a^2-b^2 \tag{102}$$

it follows that a is odd and b even. If otherwise, the left-hand side of equality (102) divided by 4 would leave a remainder of 1 while the right-hand side would leave a remainder of -1, as we assumed a to be even and b odd. Since a is odd and $(a, b) = 1$, we have $(a, 2b) = 1$. But then from equality

$$y_0^2 = 2ba$$

it follows that

$$a = t^2, \quad 2b = s^2 \tag{103}$$

where t and s are some integers. But it follows from relation (102) that $[x_0, b, a]$ is a solution of equation (96) and therefore

$$x_0 = m^2 - n^2, \quad b = 2mn, \quad a = m^2 + n^2$$

where m and n are some relatively prime numbers of different parity. From (103) we have

$$mn = \frac{b}{2} = \left(\frac{s}{2}\right)^2$$

whence, as m and n are relatively prime, it follows that

$$m = p^2, \quad n = q^2 \tag{104}$$

where p and q are non-zero integers. Since $a = t^2$ and $a = m^2 + n^2$, it follows that

$$q^4 + p^4 = t^2 \tag{105}$$

But

$$z_0 = a^2 + b^2 > a^2$$

Therefore

$$0 < t = \sqrt{a} < \sqrt[4]{z_0} < z_0 \quad (z_0 < 1) \tag{106}$$

Setting $q = x_1$, $p = y_1$ and $t = z_1$ we see that if there exists a solution $[x_0, y_0, z_0]$, then there must exist another solution $[x_1, y_1, z_1]$ for which $0 < z_1 < z_0$. This process of obtaining solutions of equation (94) may be continued indefinitely, and we obtain a sequence of solutions

$$[x_0, y_0, z_0], [x_1, y_1, z_1], \ldots, [x_n, y_n, z_n], \ldots$$

in which the positive integers $z_0, z_1, z_2, \ldots, z_n, \ldots$ decrease monotonically; in other words, inequalities

$$z_0 > z_1 > z_2 > \ldots > z_n > \ldots$$

hold for them. But positive integers cannot form an infinite and monotonically decreasing sequence as there cannot be more than z_0 terms in it. We have thus come to a contradiction by assuming that equation (94) has at least one solution in integers x, y, z, $xyz \neq 0$. This serves as a proof that equation (94) does not have a solution. Accordingly equation (93) has no solutions in positive integers $[x, y, z]$ either, since, if otherwise, if $[x, y, z]$ were a solution of equation (93), then $[x, y, z^2]$ would be a solution to (94).

The method of proof we have employed, consisting in using one solution to construct an innumerable sequence of solutions with indefinitely decreasing positive z, is called the method of infinite descent.

As was remarked above, Fermat's last theorem in the general case does not yet yield to this method because of the non-uniqueness of the factorization of the integers of an algebraic ring into prime factors from the same ring.

Note that we have demonstrated the non-existence of integral solutions not only for equation (94), but also for equation

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

It is interesting to note that equation

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

possesses an infinite number of positive integral solutions. For example, one solution is $[2, 3, 5]$. It is left to the reader to find general expressions for all such solutions of this equation in integers x, y, z.

We shall now consider another example which illustrates the method of infinite descent, but the argument will be somewhat different.

EXAMPLE. *Prove that equation*

$$x^4 + 2y^4 = z^2 \tag{107}$$

has no solutions in non-zero integers x, y, z. Let us suppose that a positive integral solution $[x_0, y_0, z_0]$ does exist. These numbers may be immediately assumed to be relatively prime, since if they had a greatest common divisor $d > 1$, then the numbers $\frac{x_0}{d}, \frac{y_0}{d}, \frac{z_0}{d}$ would also be solutions of equation (107). Moreover, the existence of a common divisor for any two numbers would mean that all three of them had a common divisor. Let us also assume that z_0 is the least of all the possible values of z in the positive integral solutions of equation (107). Now since $[x_0, y_0, z_0]$ satisfies equation (107), $[x_0^2, y_0^2, z_0]$ will be a solution of equation

$$x^2 + 2y^2 = z^2 \tag{108}$$

Using formulae (19′) from § 3 which provide all the positive integral solutions of equation (108), we see that there exist positive integers a and b with $(a, b) = 1$ and a odd, such that

$$x_0^2 = \pm(a^2 - 2b^2), \quad y_0^2 = 2ab, \quad z_0 = a^2 + 2b^2 \tag{109}$$

From $y_0^2 = 2ab$ it follows that b must be even since y_0 is even, y_0^2 is divisible by 4 and a is odd. Now as $b/2$ and a are relatively prime, equality

$$\left(\frac{y_0}{2}\right)^2 = a\frac{b}{2}$$

directly yields

$$a = m^2, \quad \frac{b}{2} = n^2$$

where m and n are positive integers and $(m, 2n) = 1$. But from equalities (109) it follows that

$$x_0^2 = \pm(a^2 - 2b^2) = \pm\left[a^2 - 8\left(\frac{b}{2}\right)^2\right] \tag{110}$$

where x_0 and a are odd. We have seen that the square of an odd number divided by 4 leaves a remainder of 1. Therefore, the left-hand side of equality (110), upon division by 4, gives a remainder of 1 while $a^2 - 8\left(\frac{b}{2}\right)^2$, when divided by 4, also leaves a remainder of 1. This means that the bracket on the right-hand side of (110) may be taken only with the plus sign. Now (110) may be written in the form

$$x_0^2 = m^4 - 8n^4$$

or in the form

$$x_0^2 + 2(2n^2)^2 = (m^2)^2 \tag{111}$$

where x_0, n and m are positive and relatively prime integers. Thus, the numbers x_0, $2n^2$ and m^2 constitute a solution of equation (108) and are relatively prime. Again, according to formula (19′) of § 3, there may be found integers p and q, with p odd and $(p, q) = 1$, such that

$$2n^2 = 2pq, \quad m^2 = p^2 + 2q^2, \quad x_0 = \pm(p^2 - 2q^2) \tag{112}$$

But since $(p, q) = 1$ and $n^2 = pq$, we have

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

where s and r are relatively prime integers. Finally, from here there follows the relation

$$s^4 + 2r^4 = m^2 \tag{113}$$

which shows that the triplet s, r, m is a solution of equation (107). But from the results

$$z_0 = a^2 + 2b^2, \quad a = m^2$$

obtained above it follows that $z_0 > m$. Thus, proceeding from a solution $[x_0, y_0, z_0]$, we have found another solution $[s, r, m]$, in which $0 < m < z_0$. This contradicts the assumption we made that z_0 was the least possible value. Thus we have arrived at a contradiction by assuming the existence of a solution to equation (107), and we have proved that this equation is unsolvable in non-zero integers.

We leave it to the reader to show that equations

$$x^4 + 4y^4 = z^2, \quad x^4 - y^4 = z^2$$
$$x^4 - y^4 = 2z^2, \quad x^4 - 4y^4 = z^2$$

have no positive integral solutions.

We shall conclude with a few remarks about exponential equations. *The equation*

$$a^x + b^y = c^z \tag{114}$$

where a, b and c are integers, not equal to any power of 2 *or to zero can have no more than a finite number of solutions in integers* x, y, z. The same proposition with a weak condition being added is valid for arbitrary algebraic numbers a, b and c. Moreover, equation

$$A\alpha_1^{x_1} \ldots \alpha_n^{x_n} + B\beta_1^{y_1} \ldots \beta_m^{y_m} + C\gamma_1^{z_1} \ldots \gamma_p^{z_p} = 0 \tag{115}$$

where A, B and C, $ABC \neq 0$, are integers, $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$, and $\gamma_1, \ldots, \gamma_n$ are integers and the numbers

$$\alpha = \alpha_1 \ldots \alpha_n, \ \beta = \beta_1 \ldots \beta_m, \ \gamma = \gamma_1 \ldots \gamma_p$$

are relatively prime, can only have a finite number of integral solutions $[x_1, \ldots, x_n, y_1, \ldots, y_m, z_1, \ldots, z_p]$. A generalization of this proposition with A, B and C and α_i, β_k and γ_s being algebraic numbers is also possible. Equations of the type (115) and their generalizations are of great interest because, as is shown in the theory of algebraic numbers, to each algebraic equation of type (81), there corresponds a certain exponential equation of type (115) and to each solution of equation (81) there corresponds a solution of equation (115) in integers. This correspondence extends to equations of a more general type than (81) and (115).

The book is devoted to one of the most interesting branches of number theory, the solution of equations in integers. The solution in integers of algebraic equations in more than one unknown with integral coefficients is a most difficult problem in the theory of numbers. The theoretical importance of equations with integral coefficients is quite great as they are closely connected with many problems of number theory. Moreover, these equations are sometimes encountered in in physics and so they are also important in practice. The elements of the theory of equations with integral coefficients as presented in this book are suitable for broadening the mathematical outlook of high-school students and students of pedagogical institutes. Some of the main results in the theory of the solution of equations in integers have been given and proofs of the theorems involved are supplied when they are sufficiently simple.

Mir Publishers
Moscow

ИЗДАТЕЛЬСТВО МИР