А.О.Гельфонд

РЕШЕНИЕ УРАВНЕНИЙ В ЦЕЛЫХ ЧИСЛАХ

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ К ПЕРВОМУ ИЗДАНИЮ

В основу этой книги положена лекция по уравнениям в целых числах, прочитанная мною в 1951 г. на математической олимпиаде в МГУ. Я пользуюсь здесь случаем выразить благодарность за оказанную мне помощь моему ученику, доценту Н. М. Коробову, написавшему по конспекту моей лекции первый, второй и часть третьего параграфа.

Книга доступна школьникам старших классов.

А. Гельфонд

ВВЕДЕНИЕ

Теория чисел изучает в основном арифметические свойства чисел натурального ряда, другими словами — целых положительных чисел, и принадлежит к числу старейших отделов математики. Одной из центральных задач так называемой аналитической теории чисел является задача о распределении простых чисел в натуральном ряде. Простым числом называется любое целое положительное число, большее единицы, делящееся без остатка только на себя и единицу. Задача о распределении простых чисел в натуральном ряде заключается в изучении правильности поведения числа простых чисел, меньших некоторого числа N, при больших значениях N. Первый результат в этом направлении мы находим ещё у Евклида (IV век до н. э.), именно доказательство бесконечности ряда простых чисел, а второй результат после Евклида был получен великим русским математиком П. Л. Чебышевым во второй половине XIX века. Другая основная задача теории чисел — это задача о представлении целых чисел суммами целых чисел определённого типа, например проблема представления нечётных чисел суммой трёх простых чисел. Последняя проблема, проблéма Гольдбаха, была решена сравнительно недавно крупнейшим современным представителем теории чисел — советским математиком И. М. Виноградовым.

Предлагаемая вниманию читателя книга посвящена также одному из наиболее интересных разделов теории чисел, а именно, — решению уравнений в целых числах.

Решение в целых числах алгебраических уравнений с целыми коэффициентами более чем с одним неизвестным представляет собой одну из труднейших проблем теории чисел. Этими задачами много занимались самые выдающиеся математики древности, например греческий математик Пифагор (VI век до н. э.), александрийский математик Диофант (II — III век н. э.) и лучшие математики более близкой к нам эпохи — П. Ферма (XVII век), Л. Эйлер (XVIII век), Лагранж (XVIII век) и другие. Несмотря на усилия многих поколений выдающихся математиков, в этой области отсутствуют сколько-нибудь общие методы типа метода тригонометрических сумм И. М. Виноградова, позволяющего решать самые различные проблемы аналитической теории чисел.

Проблема решения уравнений в целых числах решена до конца только для уравнений второй степени с двумя неизвестными. Отметим, что для уравнений любой степени с одним неизвестным она не представляет сколько-нибудь существенного интереса, так как эта задача может быть решена с помощью конечного числа проб. Для уравнений выше второй степени с двумя или более неизвестными весьма трудна не только задача нахождения всех решений в целых числах, но даже и более простая задача установления существования конечного или бесконечного множества таких решений.

Решение уравнений в целых числах имеет не только теоретический интерес. Такие уравнения иногда встречаются в физике.

Теоретический интерес уравнений в целых числах достаточно велик, так как эти уравнения тесно связаны со многими проблемами теории чисел. Кроме того,

элементарные части теории таких уравнений, изложенные в этой книге, могут быть с успехом использованы для расширения математического кругозора учащихся средней школы, учительских институтов и педвузов.

В этой книге изложены некоторые основные результаты, полученные в теории решения уравнений в целых числах. Теоремы, формулируемые в ней, снабжены доказательствами в тех случаях, когда эти доказательства достаточно просты.

§ 1. УРАВНЕНИЯ С ОДНИМ НЕИЗВЕСТНЫМ

Рассмотрим уравнение первой степени с одним неизвестным

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

Пусть коэффициенты уравнения a_1 и a_0 — целые числа. Ясно, что решение этого уравнения

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

будет целым числом только в том случае, когда a_0 нацело делится на a_1. Таким образом, уравнение (1) не всегда разрешимо в целых числах; так, например, из двух уравнений $3x-27=0$ и $5x+21=0$ первое имеет целое решение $x=9$, а второе в целых числах неразрешимо.

С тем же обстоятельством мы встречаемся и в случае уравнений, степень которых выше первой: квадратное уравнение $x^2+x-2=0$ имеет целые решения $x_1=1$, $x_2=-2$; уравнение $x^2-4x+2=0$ в целых числах неразрешимо, так как его корни $x_{1,2}=2\pm\sqrt{2}$ иррациональны.

Вопрос о нахождении целых корней уравнения n-й степени с целыми коэффициентами

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

решается легко. Действительно, пусть $x=a$ — целый корень этого уравнения. Тогда

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

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

Из последнего равенства видно, что a_0 делится на a без остатка; следовательно, каждый целый корень уравнения (2) является делителем свободного члена уравнения. Для нахождения целых решений уравнения надо выбрать те из делителей a_0, которые при подстановке в уравнение обращают его в тождество. Так, например, из чисел 1, -1, 2 и -2, представляющих собой все делители свободного члена уравнения

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

только -1 является корнем. Следовательно, это уравнение имеет единственный целый корень $x=-1$. Тем же методом легко показать, что уравнение

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

в целых числах неразрешимо.

Значительно больший интерес представляет решение в целых числах уравнений со многими неизвестными.

§ 2. УРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ С ДВУМЯ НЕИЗВЕСТНЫМИ

Рассмотрим уравнение первой степени с двумя неизвестными

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

где a и b — целые числа, отличные от нуля, а c — произвольное целое. Будем считать, что коэффициенты a и b не имеют общих делителей кроме единицы *). Действительно, если общий наибольший делитель этих коэффициентов $d=(a, b)$ отличен от единицы, то справедливы равенства $a=a_1d$, $b=b_1d$; уравнение (3) принимает вид

$$(a_1x+b_1y)\,d+c=0$$

и может иметь целые решения только в том случае, когда c делится на d. Таким образом, в случае $(a, b)=d\neq 1$ все коэффициенты уравнения (3) должны делиться нацело на d, и, сокращая (3) на d, придём к

*) Такие числа a и b называют *взаимно простыми*; обозначая через (a, b) общий наибольший делитель чисел a и b, для взаимно простых чисел получим $(a, b)=1$.

уравнению

$$a_1x+b_1y+c_1=0 \qquad \left(c_1=\frac{c}{d}\right),$$

коэффициенты которого a_1 и b_1 взаимно просты.

Рассмотрим сперва случай, когда $c=0$. Уравнение (3) перепишется так:

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

Решая это уравнение относительно x, получим:

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

Ясно, что x будет принимать целые значения в том и только том случае, когда y делится на a без остатка. Но всякое целое y, кратное a, можно записать в виде

$$y=at,$$

где t принимает произвольные целые значения ($t=0, \pm 1, \pm 2, \ldots$). Подставим это значение y в предыдущее уравнение, тогда

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

и мы получаем формулы, содержащие все целые решения уравнения (3'):

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

Перейдём теперь к случаю $c\neq 0$.

Покажем прежде всего, что для нахождения всех целых решений уравнения (3) достаточно найти какое-нибудь одно его решение, т. е. найти такие целые числа x_0, y_0, для которых

$$ax_0+by_0+c=0.$$

Теорема I. *Пусть a и b взаимно просты и $[x_0, y_0]$— какое-нибудь решение *) уравнения*

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

Тогда формулы

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

при $t=0, \pm 1, \pm 2, \ldots$ дают все решения уравнения (3).

*) Пару целых чисел x и y, которые удовлетворяют уравнению, будем называть *решением* и записывать $[x, y]$.

Доказательство. Пусть $[x, y]$ — произвольное решение уравнения (3). Тогда из равенств

$$ax + by + c = 0 \text{ и } ax_0 + by_0 + c = 0$$

получаем:

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

Так как $y - y_0$ — целое число и числа a и b взаимно просты, то $x_0 - x$ должно нацело делиться на b, т. е. $x_0 - x$ имеет вид

$$x_0 - x = bt,$$

где t — целое. Но тогда

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

и получаем:

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

Таким образом доказано, что всякое решение $[x, y]$ имеет вид (4). Остаётся ещё проверить, что всякая пара чисел $[x_1, y_1]$, получаемая по формулам (4) при целом $t = t_1$, будет решением уравнения (3). Чтобы провести такую проверку, подставим величины $x_1 = x_0 - bt_1$, $y_1 = y_0 + at_1$ в левую часть уравнения (3)

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

но так как $[x_0, y_0]$ — решение, то $ax_0 + by_0 + c = 0$ и, следовательно,

$$ax_1 + by_1 + c = 0,$$

т. е. $[x_1, y_1]$ — решение уравнения (3), чем теорема полностью доказана.

Итак, если известно одно решение уравнения $ax + by + c = 0$, то все остальные решения найдутся из арифметических прогрессий, общие члены которых имеют вид

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

Заметим, что в случае, когда $c = 0$, найденные раньше формулы решений

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

могут быть получены из только что выведенных формул

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

если выбрать $x_0 = y_0 = 0$, что можно сделать, так как значения $x = 0$, $y = 0$ являются, очевидно, решением уравнения

$$ax + by = 0.$$

Как же найти какое-нибудь одно решение $[x_0, y_0]$ уравнения (3) в общем случае, когда $c \neq 0$? Начнём с примера.

Пусть дано уравнение

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

Преобразуем отношение коэффициентов при неизвестных.

Прежде всего, выделим целую часть неправильной дроби $\frac{127}{52}$:

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

Правильную дробь $\frac{23}{52}$ заменим равной ей дробью $\frac{1}{\frac{52}{23}}$.

Тогда получим:

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

Проделаем такие же преобразования с полученной в знаменателе неправильной дробью $\frac{52}{23}$:

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

Теперь исходная дробь примет вид

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

Повторим те же рассуждения для дроби $\frac{23}{6}$:

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

Тогда

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

Выделяя целую часть неправильной дроби $\frac{6}{5}$:

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

придём к окончательному результату:

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

Мы получили выражение, которое называется *конечной цепной* или *непрерывной дробью*. Отбросим последнее звено этой цепной дроби — одну пятую, превратим получающуюся при этом новую цепную дробь в простую и вычтем её из исходной дроби $\frac{127}{52}$:

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

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

Приведём полученное выражение к общему знаменателю и отбросим его, тогда

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

Из сопоставления полученного равенства с уравнением

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

следует, что $x=9$, $y=22$ будет решением этого уравнения и согласно теореме все его решения будут содержаться в прогрессиях

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

Полученный результат наводит на мысль о том, что и в общем случае для нахождения решения уравнения $ax+by+c=0$ надо разложить отношение коэффициентов при неизвестных в цепную дробь, отбросить её последнее звено и проделать выкладки, подобные тем, которые были проведены выше.

Для доказательства этого предположения будут нужны некоторые свойства цепных дробей.

Рассмотрим несократимую дробь $\frac{a}{b}$. Обозначим через q_1 частное и через r_2 остаток от деления a на b. Тогда получим:

$$a = q_1 b + r_2, \qquad r_2 < b.$$

Пусть, далее, q_2 — частное и r_3 — остаток от деления b на r_2. Тогда

$$b = q_2 r_2 + r_3, \qquad r_3 < r_2,$$

точно так же

$$\begin{aligned} r_2 &= q_3 r_3 + r_4, & r_4 &< r_3, \\ r_3 &= q_4 r_4 + r_5, & r_5 &< r_4, \\ &\cdots\cdots\cdots\cdots & & \end{aligned}$$

Величины $q_1, q_2, \ldots$ называются *неполными частными*. Приведённый выше процесс образования неполных частных называется *алгоритмом Евклида*. Остатки от деления $r_2, r_3, \ldots$ удовлетворяют неравенствам

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

т. е. образуют ряд убывающих неотрицательных чисел.

Так как число неотрицательных целых чисел, не превосходящих b, не может быть бесконечным, то на некотором шаге процесс образования неполных частных оборвётся из-за обращения в нуль очередного остатка r. Пусть r_n — последний отличный от нуля остаток в ряде (5), тогда $r_{n+1} = 0$ и алгоритм Евклида для чисел a и b примет вид

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

Перепишем полученные равенства в виде

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

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

. . . . . .

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

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

Заменяя значение $\frac{b}{r_2}$ в первой строке этих равенств соответствующим значением из второй строки, значение $\frac{r_2}{r_3}$ — выражением из третьей строки и т. д., получим разложение $\frac{a}{b}$ в цепную дробь

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

Выражения, получающиеся из цепной дроби при отбрасывании всех её звеньев, начиная с некоторого звена, назовём *подходящими дробями*. Первая подходящая дробь δ_1 получится при отбрасывании всех звеньев, начиная с $\frac{1}{q_2}$:

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

Вторая подходящая дробь δ_2 получается отбрасыванием всех звеньев, начиная с $\frac{1}{q_3}$:

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

Точно так же

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

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

и т. д.

В силу способа образования подходящих дробей возникают очевидные неравенства

$$\delta_1 < \delta_3 < \ldots < \delta_{2k-1} < \frac{a}{b}; \quad \delta_2 > \delta_4 > \ldots > \delta_{2k} > \frac{a}{b}.$$

Запишем k-ю подходящую дробь δ_k в виде

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

и найдём закон образования числителей и знаменателей подходящих дробей. Преобразуем первые подходящие дроби δ_1, δ_2 и δ_3:

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

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

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

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

Отсюда получаем:

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

Применяя индукцию*), докажем, что соотношения того же вида

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

выполняются для всех $k \geqslant 3$.

Действительно, пусть равенства (7) выполняются для некоторого $k \geqslant 3$. Из определения подходящих дробей непосредственно следует, что при замене в выражении δ_k

*) См. книжку этой серии И. С. Соминский, Метод математической индукции, Гостехиздат, 1950.

величины q_k на $q_k+\frac{1}{q_{k+1}}$ δ_k перейдёт в δ_{k+1}. Согласно индукционному предположению

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

Заменяя здесь q_k на $q_k+\frac{1}{q_{k+1}}$, получим:

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

$$=\frac{P_kq_{k+1}+P_{k-1}}{Q_kq_{k+1}+Q_{k-1}}.$$

Отсюда, так как $\delta_{k+1}=\frac{P_{k+1}}{Q_{k+1}}$, следует, что

$$P_{k+1}=P_kq_k+P_{k-1},\qquad Q_{k+1}=Q_kq_{k+1}+Q_{k-1}.$$

Таким образом, из выполнения равенств (7) для некоторого $k\geqslant 3$ следует выполнение их для $k+1$. Но для $k=3$ равенства (7) выполняются, и следовательно, их справедливость установлена для всех $k\geqslant 3$.

Покажем теперь, что разность соседних подходящих дробей $\delta_k-\delta_{k-1}$ удовлетворяет соотношению

$$\delta_k-\delta_{k-1}=\frac{(-1)^k}{Q_kQ_{k-1}}\qquad (k>1). \tag{8}$$

Действительно,

$$\delta_k-\delta_{k-1}=\frac{P_k}{Q_k}-\frac{P_{k-1}}{Q_{k-1}}=\frac{P_kQ_{k-1}-Q_kP_{k-1}}{Q_kQ_{k-1}}.$$

Пользуясь формулами (7), преобразуем числитель полученной дроби

$$P_kQ_{k-1}-Q_kP_{k-1}=(P_{k-1}q_k+P_{k-2})Q_{k-1}-(Q_{k-1}q_k+Q_{k-2})P_{k-1}=$$
$$=-(P_{k-1}Q_{k-2}-Q_{k-1}P_{k-2}).$$

Выражение, стоящее в скобках, получается из исходного заменой k на $k-1$. Повторяя такие же преобразования

для получающихся выражений, получим, очевидно, цепь равенств:

$$\begin{aligned} P_kQ_{k-1}-Q_kP_{k-1}&=(-1)(P_{k-1}Q_{k-2}-Q_{k-1}P_{k-2})=\\ &=(-1)^2(P_{k-2}Q_{k-3}-Q_{k-2}P_{k-3})=\\ &=\ldots=(-1)^{k-2}(P_2Q_1-Q_2P_1)=\\ &=(-1)^{k-2}(q_1q_2+1-q_2q_1)=(-1)^{k-2}. \end{aligned}$$

Отсюда следует, что

$$\delta_k-\delta_{k-1}=\frac{P_kQ_{k-1}-Q_kP_{k-1}}{Q_kQ_{k-1}}=\frac{(-1)^{k-2}}{Q_kQ_{k-1}}=\frac{(-1)^k}{Q_kQ_{k-1}}.$$

Если разложение $\frac{a}{b}$ в цепную дробь имеет n звеньев, то n-я подходящая дробь δ_n совпадает с $\frac{a}{b}$. Применяя равенство (8), при $k=n$ получим:

$$\begin{aligned} \delta_n-\delta_{n-1}&=\frac{(-1)^n}{Q_nQ_{n-1}},\\ \frac{a}{b}-\delta_{n-1}&=\frac{(-1)^n}{bQ_{n-1}}. \end{aligned} \tag{9}$$

Вернёмся теперь к решению уравнения

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

Перепишем соотношение (9) в виде

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

Приводя к общему знаменателю и отбрасывая его, получим:

$$\begin{aligned} aQ_{n-1}-bP_{n-1}&=(-1)^n,\\ aQ_{n-1}+b(-P_{n-1})+(-1)^{n-1}&=0. \end{aligned}$$

Умножим это соотношение на $(-1)^{n-1}c$. Тогда

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

Отсюда следует, что *пара чисел* $[x_0, y_0]$,

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

является решением уравнения (10) *и согласно теореме все решения этого уравнения имеют вид*

$$x=(-1)^{n-1}cQ_{n-1}-bt, \quad y=(-1)^ncP_{n-1}+at$$
$$(t=0, \pm1, \pm2, \ldots).$$

Полученный результат полностью решает вопрос о нахождении всех целочисленных решений уравнения первой степени с двумя неизвестными. Перейдём теперь к рассмотрению некоторых уравнений второй степени.

§ 3. ПРИМЕРЫ УРАВНЕНИЙ ВТОРОЙ СТЕПЕНИ С ТРЕМЯ НЕИЗВЕСТНЫМИ

Пример I. Рассмотрим уравнение второй степени с тремя неизвестными:

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

Геометрически решение этого уравнения в целых числах можно истолковать как нахождение всех пифагоровых треугольников, т. е. прямоугольных треугольников, у которых и катеты x, y, и гипотенуза z выражаются целыми числами.

Обозначим через d общий наибольший делитель чисел x и y: $d=(x, y)$. Тогда

$$x=x_1d, \quad y=y_1d,$$

и уравнение (12) примет вид

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

Отсюда следует, что z^2 делится на d^2 и, значит, z кратно d: $z=z_1d$.

Теперь уравнение (12) можно записать в виде

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

сокращая на d^2, получим:

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

Мы пришли к уравнению того же вида, что и исходное, причём теперь величины x_1 и y_1 не имеют общих делителей, кроме 1. Таким образом, при решении уравнения (12) можно ограничиться случаем, когда x и y взаимно просты. Итак, пусть $(x, y)=1$. Тогда хотя бы одна из величин x и y (например, x) будет нечётной. Перенося y^2 в правую часть уравнения (12), получим:

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

Обозначим через d_1 общий наибольший делитель выражений $z+y$ и $z-y$. Тогда

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

где a и b взаимно просты.

Подставляя в (13) значения $z+y$ и $z-y$, получим:

$$x^2=abd_1^2.$$

Так как числа a и b не имеют общих делителей, то полученное равенство возможно только в том случае, когда a и b будут полными квадратами *):

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

Но тогда

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

и

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

Найдём теперь y и z из равенств (14). Сложение этих равенств даёт:

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

Вычитая второе из равенств (14) из первого, получим:

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

В силу нечётности x из (15) получаем, что u, v и d_1 также нечётны. Более того, $d_1=1$, так как иначе из равенств

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

следовало бы, что величины x и y имеют общий делитель $d_1\neq 1$, что противоречит предположению об их взаимной простоте. Числа u и v связаны со взаимно простыми числами a и b равенствами

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

и в силу этого сами взаимно просты; $v<u$, так как $b<a$, что ясно из равенств (14).

---

*) Известно, что произведение двух взаимно простых чисел может быть полным квадратом только тогда, когда каждый сомножитель — полный квадрат.

Подставляя в равенства (15), (16) и (17) $d_1=1$, получим *формулы*:

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

дающие при нечётных взаимно простых u *и* v $(v<u)$ *все свободные от общих делителей тройки целых положительных чисел* x, y, z, *удовлетворяющие уравнению* (12). Простой подстановкой x, y и z в уравнение (12) легко проверить, что при любых u и v числа (18) удовлетворяют этому уравнению.

Для начальных значений u и v формулы (18) приводят к следующим часто встречающимся равенствам:

$$3^2+4^2=5^2 \quad (v=1, \quad u=3),$$
$$5^2+12^2=13^2 \quad (v=1, \quad u=5),$$
$$15^2+8^2=17^2 \quad (v=3, \quad u=5).$$

Как уже было сказано, формулы (18) дают только те решения уравнения

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

в которых числа x, y и z не имеют общих делителей. Все остальные целые положительные решения этого уравнения получаются домножением решений, содержащихся в формулах (18), на произвольный общий множитель d.

Тем же путём, каким мы получили все решения уравнения (12), могут быть получены и все решения других уравнений того же типа.

Пример II. Найдём все решения уравнения

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

в целых положительных, попарно взаимно простых числах x, y, z.

Заметим, что если x, y, z есть решение уравнения (19) и x, y, z не имеют общего делителя, отличного от 1, то они и попарно взаимно просты. Действительно, если x и y кратны простому числу $p>2$, то из равенства

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

следует, так как его левая часть — целое число, что z кратно p. То же самое будет, если x и z или y и z делятся на p.

Заметим, что x должно быть числом нечётным для того, чтобы общий наибольший делитель x, y, z был равен 1. Действительно, если x чётно, то левая часть уравнения (19) будет чётным числом и, значит, z также будет чётным. Но x^2 и z^2 будут тогда кратны 4. Отсюда следует, что $2y^2$ должно делиться на 4, другими словами, что y тоже должно быть чётным числом. Значит, если x чётно, то все числа x, y, z должны быть чётными. Итак, в решении без общего, отличного от 1 делителя x должно быть нечётным. Отсюда уже следует, что и z должно быть тоже нечётным. Перенося x^2 в правую часть, мы получаем:

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

Но $z+x$ и $z-x$ имеют общим наибольшим делителем 2. Действительно, пусть их общий наибольший делитель будет d. Тогда

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

где k и l — целые числа. Складывая и вычитая эти равенства, мы будем иметь:

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

Но z и x нечётны и взаимно просты. Поэтому общий наибольший делитель $2x$ и $2z$ будет 2. Отсюда следует, что $d = 2$.

Итак, или $\frac{z+x}{2}$, или $\frac{z-x}{2}$ нечётно. Поэтому или числа

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

взаимно просты, или взаимно просты числа

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

В первом случае из равенства

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

следует, что

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

а во втором случае из равенства

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

следует

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

где n и m — целые, m — нечётное число и $n>0$, $m>0$. Решая эти две системы уравнений относительно x и z и находя y, мы получаем или

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

или

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

где m нечётно. Объединяя эти две формы представления решения x, y, z, мы получаем общую формулу

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

где m нечётно. Но, для того чтобы z и x были целыми числами, необходимо, чтобы n было чётным. Полагая $n=2b$ и $m=a$, мы получим окончательно *общие формулы, дающие все решения уравнения* (19) *в целых положительных, без общего делителя, большего* 1, *числах* x, y, z:

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

где a *и* b *положительны, взаимно просты и* a *нечётно.* При этих условиях величины a и b выбираются произвольно, но так, чтобы x было положительно. Формулы (19′) действительно дают все решения в целых положительных и взаимно простых числах x, y, z, так как, с одной стороны, мы доказали, что x, y, z в этом случае должны представляться по формулам (19′), а с другой стороны, если мы зададим числа a и b, удовлетворяющие нашим условиям, то x, y, z будут действительно взаимно просты и будут решением уравнения (19).

§ 4. УРАВНЕНИЯ ВИДА $x^2 - Ay^2 = 1$. НАХОЖДЕНИЕ ВСЕХ РЕШЕНИЙ ЭТОГО УРАВНЕНИЯ

Перейдём теперь к решению в целых числах уравнений второй степени с двумя неизвестными, имеющих вид

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

где A — целое положительное число, не являющееся полным квадратом. Для того чтобы найти подход к решению таких уравнений, познакомимся с разложениями в цепные дроби иррациональных чисел вида $\sqrt{A}$. Из алгоритма Евклида следует, что всякое рациональное число разлагается в цепную дробь с конечным числом звеньев. Иначе обстоит дело с иррациональными числами. Соответствующие им цепные дроби бесконечны. Найдём, например, разложение в цепную дробь иррационального числа $\sqrt{2}$.

Преобразуем очевидное тождество

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

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

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

заменяя разность $\sqrt{2}-1$, полученную в знаменателе, равным ей в силу тождества выражением

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

получим:

$$\sqrt{2}-1 = \frac{1}{2+\dfrac{1}{2+(\sqrt{2}-1)}}; \qquad \sqrt{2} = 1 + \frac{1}{2+\dfrac{1}{2+(\sqrt{2}-1)}}.$$

Снова заменим скобку, стоящую в знаменателе последнего равенства, равной ей дробью из того же тождества, тогда

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

Продолжая этот процесс, получим следующее разложение $\sqrt{2}$ в бесконечную цепную дробь:

$$\sqrt{2}=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\ddots}}}}} \tag{21}$$

Заметим, что применённый выше метод разложения в цепную дробь, основанный на использовании тождества вида

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

годится не для всякой иррациональности $\sqrt{A}$. Этот метод, очевидно, можно применять в тех случаях, когда целое число A может быть представлено в виде $A=m^2+1$, где m — некоторое целое, отличное от нуля. (В частности, при $m=1$ получаем разложение $\sqrt{2}$; $m=2$ приводит к разложению $\sqrt{5}$ и т. д.). Однако и в общем случае известны сравнительно несложные методы для разложения $\sqrt{A}$ в бесконечную цепную дробь *).

Как и раньше, в случае конечных цепных дробей, образуем для бесконечной цепной дроби (21) последовательность подходящих дробей $\delta_1, \delta_2, \delta_3, \ldots$

$$\begin{aligned}
&\delta_1=1, && \delta_1<\sqrt{2};\\
&\delta_2=1+\frac{1}{2}=\frac{3}{2}, && \delta_2>\sqrt{2};\\
&\delta_3=1+\cfrac{1}{2+\cfrac{1}{2}}=\frac{7}{5}, && \delta_3<\sqrt{2};\\
&\delta_4=\ldots=\frac{17}{12}, && \delta_4>\sqrt{2}
\end{aligned} \tag{22}$$

и т. д.

Из способа образования подходящих дробей следует, что

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

*) См., например, книгу И. В. Арнольда «Теория чисел», глава VI (Учпедгиз, 1939 г.) или А. Я. Хинчин «Цепные дроби» (Гостехиздат, 1949 г.).

Вообще, если задано разложение в бесконечную цепную дробь некоторого иррационального числа α,

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

то для подходящих дробей выполняются неравенства:

$$\delta_1 < \delta_3 < \ldots < \delta_{2k+1} < \ldots < \alpha < \ldots < \delta_{2k} < \ldots < \delta_4 < \delta_2. \quad (23)$$

Представим подходящую дробь δ_k в виде

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

Соотношения (7)

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

полученные раньше для конечных цепных дробей, сохраняются и для бесконечных цепных дробей, так как при выводе этих соотношений мы нигде не использовали то, что цепная дробь является конечной. Поэтому сохраняется также и соотношение (8) между соседними подходящими дробями:

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

Например, для подходящих дробей разложения $\sqrt{2}$ в цепную дробь при $k=3$ и $k=4$ получим из (22):

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

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

что, естественно, совпадает с результатом, указанным в (24).

Из (24), в частности, следует, что

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

Покажем теперь, что справедливо неравенство

$$0 < P_{2k} - \alpha Q_{2k} < \frac{1}{Q_{2k+1}}. \quad (25)$$

Действительно, левая часть этого неравенства получается сразу, так как согласно (23)

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

Доказательство правой части неравенства (25) также проходит без труда. В силу (23)

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

следовательно,

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

Отсюда, заменяя δ_{2k} на $\frac{P_{2k}}{Q_{2k}}$, получаем:

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

Умножая это неравенство на Q_{2k}, приходим к желаемому результату

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

Применим теперь полученные результаты к решению уравнения

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

Преобразуем левую часть этого уравнения

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

Положим $x = P_{2k}$ и $y = Q_{2k}$, где P_{2k} и Q_{2k} — числитель и знаменатель соответствующей подходящей дроби из разложения $\sqrt{2}$ в цепную дробь. Тогда

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

Левая, а значит, и правая, часть полученного равенства является целым числом. Покажем, что это целое число больше нуля, но меньше двух и, следовательно, равно единице. Для этого применим неравенство (25) при $\alpha = \sqrt{2}$:

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

Отсюда видно, что оба сомножителя правой части (27) положительны и, значит,

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

С другой стороны,

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

Но в силу (23)

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

Отсюда

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

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

и мы получаем два неравенства для сомножителей правой части равенства (27):

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

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

Перемножение этих неравенств даёт:

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

Применяя неравенство (28), получим отсюда:

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

и так как для всех $k \geqslant 1$

$$\frac{1}{Q_{2k}Q_{2k+1}} \leqslant \frac{1}{Q_2 Q_3} = \frac{1}{10},$$

то

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

Таким образом мы доказали, что целое число $P_{2k}^2 - 2Q_{2k}^2$ при любом $k \geqslant 1$ удовлетворяет неравенствам

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

Следовательно,

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

т. е. числа $x = P_{2k}$, $y = Q_{2k}$ при любом $k \geqslant 1$ дают решение уравнения

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

Мы пока не знаем, будут ли найденные нами решения уравнения (26) представлять собой все решения этого уравнения.

Теперь уже естественно возникает вопрос о том, как получить все решения в целых числах x и y уравнения

$$x^2 - Ay^2 = 1 \qquad (29)$$

при $A > 0$ целом и $\sqrt{A}$ иррациональном. Как мы покажем, это можно сделать, если известно хотя бы одно решение уравнения (29). На примере уравнения (26) мы видели, что такие уравнения имеют решения. Мы займёмся сейчас вопросом о том, как получить все решения уравнения (29) из одного определённого его решения, которое мы будем называть минимальным, или наименьшим, оставляя пока открытым вопрос о том, всегда ли уравнение (29) имеет хотя бы одно решение в целых числах, отличное от тривиального $x = 1$, $y = 0$.

Допустим, что уравнение (29) имеет нетривиальное решение $[x_0, y_0]$, $x_0 > 0$, $y_0 > 0$, и

$$x_0^2 - Ay_0^2 = 1. \qquad (30)$$

(Напомним, что решением называется пара целых чисел $[x_0, y_0]$, удовлетворяющих уравнению.) Мы будем называть это решение $[x_0, y_0]$ *наименьшим,* если при $x = x_0$ и $y = y_0$ двучлен $x + \sqrt{A}y$, $\sqrt{A} > 0$, будет иметь наименьшую возможную величину из всех возможных его значений, которые он будет принимать при подстановке вместо x и y всех возможных целых положительных (отличных от нуля) решений уравнения (29). Например, для уравнения (26) наименьшим решением будет $x=3$, $y=2$, так как $x + \sqrt{2}y$ при этих значениях x и y примет значение $3 + 2\sqrt{2}$, и не существует другого решения уравнения (26), что сразу видно при попытке подбора малых целых положительных чисел, могущих быть решениями,

которое давало бы двучлену $x+\sqrt{2}\,y$ значение, не большее, чем $3+2\sqrt{2}$. Действительно, следующее по величине решение уравнения (26) будет $x=17$, $y=12$, и ясно, что $17+12\sqrt{2}$ больше чем $3+2\sqrt{2}$. Заметим также, что *не существует двух наименьших решений уравнения* (29). Допустим обратное, т. е. что есть решения $[x_1, y_1]$ и $[x_2, y_2]$, которые дают одно и то же значение двучлену $x+\sqrt{A}\,y$. Тогда

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

Но $\sqrt{A}$ — иррациональное число, а x_1, y_1, x_2, y_2 — целые числа. Значит, как это непосредственно следует из равенства (31),

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

что невозможно, так как x_1-x_2 — целое число, $(y_2-y_1)\sqrt{A}$ как произведение целого числа на иррациональное будет иррациональным, а целое число не может быть числом иррациональным. Противоречие это пропадает, если $x_1=x_2$ и $y_1=y_2$,—другими словами, когда мы берём не два различных решения, а одно. Итак, если существует наименьшее решение, то только одно. Заметим теперь ещё одно очень важное свойство решений уравнения (29). Пусть $[x_1, y_1]$ будет решением уравнения (29). Тогда

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

или

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

Возведём теперь обе части равенства (32) в целую положительную степень n:

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

Осуществляя возведение в степень по правилу степени бинома, мы получаем:

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

$$+\frac{n(n-1)}{2}x_1^{n-2}Ay_1^2+\ldots+(\sqrt{A})^n\,y_1^n=x_n+\sqrt{A}\,y_n, \tag{34}$$

где x_n и y_n будут целыми числами, так как первый, третий и вообще все нечётные члены разложения по правилу степени бинома будут целыми числами, а чётные члены будут целыми числами, умноженными на $\sqrt{A}$. Собирая в отдельности целые слагаемые и числа, кратные $\sqrt{A}$, мы получаем равенство (34). Числа x_n и y_n, как мы сейчас докажем, будут также решением уравнения (29). Действительно, из равенства (34), меняя знак у $\sqrt{A}$, мы получаем равенство

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

Перемножая почленно равенства (34) и (35) и воспользовавшись равенством (33), мы будем окончательно иметь:

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

другими словами, что $[x_n, y_n]$ *есть также решение уравнения* (29).

Теперь мы можем доказать основную теорему относительно решений уравнения (29).

Теорема II. *Всякое решение уравнения* (29)

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

при положительном A *и иррациональном* $\sqrt{A}$ *имеет вид* $[\pm x_n, \pm y_n]$, *где*

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

а $[x_0, y_0]$ *— наименьшее решение.*

Доказательство. Допустим обратное, — именно, что существует такое решение в целых положительных числах уравнения (29) $[x', y']$, что равенство

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

невозможно ни при каком целом положительном n. Рассмотрим ряд чисел

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

Это — ряд положительных неограниченно растущих чисел, так как $x_0 \geqslant 1$, $y_0 \geqslant 1$ и $x_0 + \sqrt{A}\, y_0 > 1$. Вследствие того,

что $[x_0, y_0]$ — наименьшее решение, по определению наименьшего решения

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

Поэтому всегда найдётся такое целое $n \geqslant 1$, что

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

Но $x_0 - \sqrt{A}\, y_0 > 0$, так как

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

Поэтому от умножения всех членов неравенств (39) на одно и то же положительное число $(x_0 - \sqrt{A}\, y_0)^n$ знаки неравенств сохранятся, и мы будем иметь:

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

Так как

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

то

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

Кроме того,

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

где $\bar{x}$ и $\bar{y}$ — целые числа и

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

Воспользовавшись соотношениями (41), (42), (43) и неравенствами (40), мы получим неравенства

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

Покажем, что пара целых чисел $\bar{x}$ и $\bar{y}$ будет решением уравнения (29). Действительно, перемножая почленно равенство (43), т. е. равенство

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

и равенство

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

которое получается из (43) непосредственно, если переменить знак у $\sqrt{A}$, получаем:

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

так как $[x', y']$ и $[x_0, y_0]$ — решения уравнения (29). Докажем, наконец, что $\bar{x}>0$ и $\bar{y}>0$. Прежде всего ясно, что $\bar{x}$ не равно нулю. Действительно, если $\bar{x}=0$, то из равенства (47) мы будем иметь:

$$-Ay_0^2=1,$$

что невозможно, так как $A>0$. Далее, если $y=0$, то $x^2=1$, но из неравенств (44) $\bar{x}>1$, что невозможно. Наконец, заметим, что знаки x и $\bar{y}$ должны быть одинаковы. Действительно, если предположить, что знаки $\bar{x}$ и $\bar{y}$ различны, то $\bar{x}$ и $-\bar{y}$ будут иметь уже одинаковые знаки. Если мы сравним тогда абсолютные величины чисел $\bar{x}+\sqrt{A}\,\bar{y}$ и $\bar{x}-\sqrt{A}\,\bar{y}$, то абсолютная величина первого из этих чисел должна быть меньше абсолютной величины второго числа, так как в первом числе вычитаются одно из другого два числа одинаковых знаков, а в другом складываются. Но мы уже знаем, что

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

значит, $\bar{x}-\sqrt{A}\,\bar{y}$ также по абсолютной величине больше единицы. Но

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

и мы пришли к противоречию, так как произведение двух чисел, каждое из которых по абсолютной величине больше единицы, также должно иметь абсолютную величину, бóльшую единицы. Итак, знаки $\bar{x}$ и $\bar{y}$ одинаковы и $\bar{x}\neq 0$ и $\bar{y}\neq 0$. Но тогда из неравенства (44) уже сразу следует, что $\bar{x}>0$ и $\bar{y}>0$. Итак, предположив, что существует решение уравнения

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

$[x', y']$ такое, что равенство (38) невозможно ни при каком целом положительном n, мы сумели построить решение этого уравнения $[\bar{x}, \bar{y}]$, $\bar{x} > 0$, $\bar{y} > 0$, $\bar{x}$ и $\bar{y}$ — целые, удовлетворяющее неравенствам (44), которые противоречат определению наименьшего решения $[x_0, y_0]$. Этим мы и доказали, что предположение существования решения, не представляющегося по формуле (38), приводит нас к противоречию. Другими словами, мы доказали, что все решения нашего уравнения могут быть получены из формулы (38).

Итак, всякое решение $[x, y]$ уравнения (29) получается из соотношения

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

где $[x_0, y_0]$ — наименьшее решение. Меняя в этом последнем равенстве знак у $\sqrt{A}$, мы будем иметь также равенство

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

Складывая и вычитая эти равенства и деля обе части соответственно на 2 или $2\sqrt{A}$, мы получаем:

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

другими словами, — явные выражения для любого решения $[x, y]$ при положительных x и y. Всякое решение получается из этих, если брать произвольные знаки при x_n и y_n.

Например, так как мы уже видели выше, что наименьшим решением для уравнения $x^2 - 2y^2 = 1$ будет $x = 3$, $y = 2$, то все решения этого уравнения будут содержаться в формулах:

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

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

откуда при $n = 1, 2, 3$ мы получаем решения: [3, 2], [17, 12], [99, 70].

Заметим, что числа x_n и y_n с ростом n растут со скоростью геометрической прогрессии со знаменателем $x_0+\sqrt{A}\,y_0$, так как вследствие равенства

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

мы можем утверждать, что

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

и, значит, что $(x_0-\sqrt{A}\,y_0)^n$ всегда стремится к нулю с ростом n.

Заметим теперь, что если уравнение (29) имеет хотя бы одно нетривиальное решение, — другими словами, хотя бы одно решение при $y\neq 0$, — то будет существовать наименьшее решение этого уравнения и тогда все его решения могут быть получены из формул (50). Вопрос о существовании нетривиального решения этого уравнения при произвольном целом положительном A и $\sqrt{A}$ иррациональном мы пока оставляли открытым, а теперь вернёмся к нему.

§ 5. ОБЩИЙ СЛУЧАЙ УРАВНЕНИЯ ВТОРОЙ СТЕПЕНИ С ДВУМЯ НЕИЗВЕСТНЫМИ

Мы докажем в этом параграфе, что при любом целом положительном A и иррациональном $\sqrt{A}$ уравнение

$$x^2-Ay^2=1 \tag{51}$$

всегда имеет нетривиальное решение, — другими словами, существует пара целых чисел x_0 и y_0, x_0, $y_0\neq 0$, которая ему удовлетворяет. Прежде всего, укажем приём, позволяющий разложить в цепную дробь произвольное положительное число. Выше мы пользовались для разложения в цепную дробь специальными свойствами числа $\sqrt{2}$. Пусть α — *любое положительное число*. Тогда всегда существует целое число, которое будет меньше или равно α и больше $\alpha-1$. Такое целое число носит название *целой части* α и обозначается $[\alpha]$. Разность между α и

его целой частью называется *дробной долей числа* α и обозначается $\{\alpha\}$. Из определений целой части и дробной доли числа α непосредственно следует соотношение между ними, именно:

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

или

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

Так как дробная доля числа есть разность между положительным числом и наибольшим целым числом, его не превосходящим, то дробная доля числа всегда меньше единицы и неотрицательна. Например, целая часть $\frac{27}{5}$ есть 5, а дробная его доля есть $\frac{2}{5}$; целая часть $\sqrt{2}$ есть 1, а дробная доля равна $\sqrt{2}-1$; целая часть $\sqrt[3]{52}$ равна 3, а дробная доля равна $\sqrt[3]{52}-3$, и т. д.

Введённое нами определение целой части и дробной доли положительного числа α может быть использовано для разложения этого числа в цепную дробь. Положим:

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

Тогда

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

Так как $\{\alpha\}$ всегда меньше единицы, то α_1 всегда больше единицы. Если бы α было само целым числом, то его дробная доля равнялась бы нулю, α_1 было бы равно бесконечности и мы бы имели равенство $\alpha=q_1$. Отвлекаясь от этого частного случая, который исключается тем, что мы разлагаем в непрерывную дробь иррациональное число, мы можем утверждать, что α_1 — положительное, большее единицы число. С этим числом α_1 мы поступаем так же, как и с α, и пишем равенство

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

Продолжая этот процесс, мы получаем ряд равенств:

$$\left.\begin{aligned}
\alpha &= q_1 + \frac{1}{\alpha_1}, \quad q_1 = [\alpha], \\
\alpha_1 &= q_2 + \frac{1}{\alpha_2}, \quad q_2 = [\alpha_1], \\
\alpha_2 &= q_3 + \frac{1}{\alpha_3}, \quad q_3 = [\alpha_2], \\
&\cdots\cdots\cdots\cdots \\
\alpha_{n-1} &= q_n + \frac{1}{\alpha_n}, \quad q_n = [\alpha_{n-1}], \\
&\cdots\cdots\cdots\cdots
\end{aligned}\right\} \qquad (54)$$

Этот процесс последовательного образования целых чисел $q_1, q_2, q_3, \ldots, q_n, \ldots$ в случае, когда α — рациональное число, — другими словами, когда $\alpha = \frac{a}{b}$, где a и b — целые положительные числа, — как нетрудно заметить, ничем не отличается по своим результатам от получения неполных частных с помощью алгоритма Евклида (см. формулы (6)). Он должен поэтому оборваться при α рациональном. При α иррациональном этот процесс должен быть бесконечным. Действительно, если бы при каком-нибудь n α_n было бы целым числом, то отсюда следовало бы, что α_{n-1} было бы рациональным, что в свою очередь влекло бы за собой рациональность α_{n-2} и т. д. и, наконец, рациональность α_1. Из формул (54), делая последовательные замены, исключая $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$, мы получим цепную дробь

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

которую, так как n можно взять сколь угодно большим, можно записывать и в форме бесконечной цепной дроби

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

Как мы уже говорили выше, в § 4, соотношение (8) между подходящими дробями сохраняется в этом случае, так как оно не зависит от конечности или бесконечности дроби. Из этого соотношения (8), как мы уже видели, следует для чётных подходящих дробей неравенство (25). Это неравенство (25) будет опять лежать в основе доказательства существования решения у уравнения (51), но само доказательство будет сложнее, чем в частном случае, когда $A=2$. За дальнейшими сведениями из теории цепных дробей мы можем отослать читателя к книге проф. А. Я. Хинчина «Цепные дроби».

Теорема III. *При любом целом положительном A и иррациональном $\sqrt{A}$ уравнение* (51)

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

имеет нетривиальное решение $[x_0, y_0]$, $x_0 > 0$, $y_0 > 0$.

Доказательство. Ввиду некоторой сложности доказательства существования решения уравнения (51) мы разобьём это доказательство на ряд шагов. Первый шаг доказательства будет заключаться в том, что мы докажем существование целого положительного числа k, обладающего тем свойством, что уравнение

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

будет иметь бесчисленное множество решений в целых положительных числах x и y. Действительно, рассмотрим двучлен $x^2 - Ay^2$ и будем в него вместо x и y подставлять числители и знаменатели последовательных чётных подходящих дробей к иррациональному числу $\alpha = \sqrt{A}$. Тогда

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

Но из того, что

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

непосредственно следует:

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

Используем эти два последних неравенства для оценки z_{2n}. Заменяя оба множителя в правой части равенства (57) с

помощью этих неравенств бо́льшими величинами, мы получаем для z_{2n} неравенство

$$0 < z_{2n} < \frac{1}{Q_{2n+1}}\left(2aQ_{2n} + \frac{1}{Q_{2n+1}}\right) < 2a + 1, \qquad (58)$$

так как Q_{2n} меньше Q_{2n+1}. При подстановке в двучлен

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

вместо x и y, соответственно, P_{2n} и Q_{2n} z принимает целое положительное значение. Итак, все числа $z_2, z_4, \ldots$ $\ldots, z_{2n}, \ldots$ будут целыми положительными числами, не превышающими одного и того же числа $2a+1$. Но так как $a = \sqrt{A}$ иррационально, то цепная дробь будет бесконечной и, значит, таких пар чисел P_{2n} и Q_{2n} будет бесконечно много. Различных же среди целых положительных чисел $z_2, z_4, \ldots, z_{2n}, \ldots$ будет лишь конечное число, так как между 1 и вполне определённым числом $2a+1$, от n не зависящим, может лежать не более $[2a+1]$ целых чисел. Другими словами, бесконечный ряд чисел $z_2, z_4, \ldots$ $\ldots, z_{2n}, \ldots$ есть не что иное, как последовательность каким-то образом повторяющихся целых чисел $1, 2, 3, \ldots, [2a+1]$, причём не обязательно даже, что все эти числа встречаются в нашей последовательности $z_2, z_4, z_6, \ldots$ Так как последовательность $z_2, z_4, \ldots, z_{2n}, \ldots$ бесконечна, а число различных её членов конечно, то хотя бы одно число k $(1 \leqslant k \leqslant [2a+1])$ в этой последовательности повторяется бесчисленное множество раз. Другими словами, среди пар чисел $[P_2, Q_2], [P_4, Q_4], \ldots, [P_{2n}, Q_{2n}], \ldots$ найдётся бесчисленное множество таких пар, что величина $z = x^2 - Ay^2$ принимает при подстановке этих чисел вместо x и y одно и то же значение k. Итак, мы доказали существование целого положительного числа k, при котором уравнение (56) имеет бесчисленное множество решений в целых числах x и y. Перенумеруем снова эти пары чисел, служащие решениями уравнения (56) при данном k, обозначив их $[u_1, v_1], [u_2, v_2], \ldots, [u_n, v_n], \ldots$ Мы будем тогда иметь, что

$$u_n^2 - Av_n^2 = k. \qquad (59)$$

Заметим, что последовательность пар $[u_1, v_1], [u_2, v_2], \ldots$ $\ldots, [u_n, v_n], \ldots$ будет частью последовательности пар числителей и знаменателей чётных подходящих дробей

числа α. Если бы мы могли утверждать, что $k=1$, то мы бы уже доказали, что уравнение (51) имеет бесчисленное множество решений в целых числах. Так как мы этого утверждать не можем, то допустим, что $k>1$ (в противном случае, когда $k=1$, всё уже доказано), и перейдём ко второму шагу нашего доказательства. Докажем теперь, что среди пар целых чисел $[u_1, v_1]$, ..., $[u_n, v_n]$,... будет бесконечно много пар чисел, дающих одни и те же остатки при делении на число k, — другими словами, что существуют такие два целых неотрицательных числа p и q, меньших k, что для бесчисленного множества пар $[u_1, v_1]$, ..., $[u_n, v_n]$, ... будут иметь место равенства

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

где a_n и b_n — частные от деления u_n и v_n на k, а p и q — остатки. Действительно, если мы разделим u_n и v_n на целое число k, $k>1$, то мы получим соотношения вида (60), где остатки от деления будут, как всегда, находиться между нулём и $k-1$. Так как остатками от деления чисел u_n на k могут быть только числа 0, 1, 2, ..., $k-1$ и, совершенно так же, остатками от деления чисел v_n на k могут быть тоже только эти же числа 0, 1, 2, ..., $k-1$, то число возможных пар остатков при делении чисел u_n и v_n на k будет $k \cdot k = k^2$. Это ясно также из того, что каждой паре $[u_n, v_n]$ соответствует пара остатков $[p_n, q_n]$, причём p_n и q_n, каждый в отдельности, не могут принимать более k различных значений, а число пар поэтому будет не более k^2. Итак, каждой паре целых чисел $[u_n, v_n]$ соответствует пара остатков $[p_n, q_n]$ при делении на k. Но число различных пар остатков конечно, не превышает k^2, а число пар $[u_n, v_n]$ бесконечно. Значит, так как в ряду пар $[p_1, q_1]$, $[p_2, q_2]$, ..., $[p_n, q_n]$, ... имеется лишь конечное число различных пар, то хотя бы одна пара повторяется бесчисленное множество раз. Обозначая эту пару остатков $[p, q]$, мы и получаем, что существует бесчисленное множество пар $[u_n, v_n]$, для которых имеют место равенства (60). Так как не все пары $[u_n, v_n]$ удовлетворяют равенствам (60) при некоторых определённых p и q, существование которых мы сейчас доказали, то мы снова перенумеровываем все те пары $[u_n, v_n]$, которые удовлетворяют равенствам (60), и будем эти пары обозначать $[R_n, S_n]$. Итак, бесконечная последовательность пар $[R_1, S_1]$,

$[R_2, S_2], \ldots, [R_n, S_n], \ldots$ есть часть последовательности пар $[u_n, v_n]$, которая в свою очередь есть часть последовательности пар числителей и знаменателей чётных подходящих дробей числа α. Пары чисел этой последовательности удовлетворяют уравнению (59) и дают одни и те же остатки p и q при делении на k.

Теперь, после того как мы установили существование бесчисленного множества таких пар целых положительных чисел R_n и S_n, мы можем перейти к третьему и последнему шагу нашего доказательства.

Заметим, прежде всего, что пары $[R_n, S_n]$, будучи парами числителей и знаменателей подходящих дробей, должны быть парами взаимно простых чисел, т. е. не иметь общих делителей. Действительно, если в соотношении (24) заменить k на $2k$ и положить $\delta_{2k} = \frac{P_{2k}}{Q_{2k}}$, $\delta_{2k-1} = \frac{R_{2k-1}}{Q_{2k-1}}$, то из равенства

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

умножив обе его части на $Q_{2k}Q_{2k-1}$, мы получаем равенство

$$P_{2k}Q_{2k-1} - Q_{2k}P_{2k-1} = 1. \tag{61}$$

Это соотношение между целыми числами P_{2k}, Q_{2k}, P_{2k-1}, Q_{2k-1} показывает, что если P_{2k} и Q_{2k} имеют общий делитель, больший единицы, то вся левая часть его должна нацело делиться на этот общий делитель. Но справа в равенстве стоит единица, которая не может делиться ни на какое целое число, большее единицы. Таким образом, взаимная простота чисел R_n и S_n, которые могут быть только числителями и знаменателями подходящих дробей, установлена. Из соотношений (7) также непосредственно следует, что

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

Из взаимной простоты чисел R_n и S_n и того обстоятельства, что числа $S_1, S_2, \ldots, S_n, \ldots$, которые взяты из последовательности различных между собой чисел Q_{2n}, также между собой различны, непосредственно следует, что в бесконечном ряду дробей

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

нет одинаковых чисел. Напишем два равенства, следующих из определения чисел R_n и S_n:

$$R_1^2 - AS_1^2 = (R_1 - \alpha S_1)(R_1 + \alpha S_1) = k \tag{62}$$

и

$$R_2^2 - AS_2^2 = (R_2 - \alpha S_2)(R_2 + \alpha S_2) = k, \tag{63}$$

где попрежнему $\alpha = \sqrt{A}$.

Далее имеем:

$$(R_1 - \alpha S_1)(R_2 + \alpha S_2) = R_1R_2 - AS_1S_2 + \alpha(R_1S_2 - S_1R_2), \tag{64}$$

так как $\alpha^2 = A$, и совершенно так же

$$(R_1 + \alpha S_1)(R_2 - \alpha S_2) = R_1R_2 - AS_1S_2 - \alpha(R_1S_2 - S_1R_2). \tag{65}$$

Но R_n и S_n при делении на k дают одни и те же, не зависящие от n остатки. Следовательно, в силу соотношений (60)

$$R_n = c_nk + p, \quad S_n = d_nk + q. \tag{66}$$

Поэтому с помощью лёгких преобразований и замен мы получаем равенства:

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

где x_1 — целое число, так как $R_1^2 - AS_1^2 = k$. Совершенно так же

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

где y_1 — опять целое число. Можно утверждать, что y_1 не равно нулю. Действительно, если $y_1 = 0$, то

$$ky_1 = R_1S_2 - R_2S_1 = 0,$$

откуда

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

Это последнее равенство невозможно, так как мы установили, что все дроби $\frac{P_n}{S_n}$ между собой различны. Равенства (67) и (65) показывают, что

$$(R_1 - aS_1)(R_2 + aS_2) = kx_1 + aky_1 = k(x_1 + ay_1) \qquad (69)$$

и

$$(R_1 + aS_1)(R_2 - aS_2) = kx_1 - aky_1 = k(x_1 - ay_1). \qquad (70)$$

Перемножая теперь почленно равенства (62) и (63) и воспользовавшись равенствами (69) и (70), мы получаем:

$$\begin{aligned} k^2 &= (R_1^2 - AS_1^2)(R_2^2 - AS_2^2) = \\ &= (R_1 - aS_1)(R_2 + aS_2)(R_1 + aS_1)(R_2 - aS_2) = \\ &= k^2(x_1 + ay_1)(x_1 - ay_1) = k^2(x_1^2 - Ay_1^2). \end{aligned} \qquad (71)$$

Сокращая на k^2, окончательно получим:

$$x_1^2 - Ay_1^2 = 1. \qquad (72)$$

Но y_1 не равно нулю, а значит, и x_1 не может быть нулём. В противном случае слева стояло бы отрицательное число, а справа — единица. Итак, даже в предположении, что k не равно единице, мы нашли два целых, не равных нулю числа x_1 и y_1, которые удовлетворяют уравнению (51). Этим полностью завершается теория уравнений типа (51), так как мы знаем, что такие уравнения при A целом, $A > 0$, и $\sqrt{A}$ иррациональном всегда имеют решение, а с помощью наименьшего решения, существование которого тем самым доказано, умеем строить все его решения.

Практически наименьшее решение можно искать путём подбора x_0 и y_0.

Мы полностью рассмотрели, таким образом, случай $A > 0$ и $a = \sqrt{A}$ иррационально в уравнении

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

Если $A > 0$ и $a = \sqrt{A}$ — целое число, то это уравнение может быть записано в форме

$$x^2 - a^2y^2 = (x + ay)(x - ay) = 1,$$

и так как α — целое число, то если x_0 и y_0 — целые числа, ему удовлетворяющие, должны иметь место в отдельности равенства

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

или равенства

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

так как произведение двух целых чисел может быть равно единице тогда и только тогда, когда каждое из этих чисел в отдельности равно $+1$ или -1. Обе эти системы двух уравнений с двумя неизвестными x_0 и y_0 имеют только системы тривиальных решений: $x_0 = 1$, $y_0 = 0$; $x_0 = -1$, $y_0 = 0$. Итак, *уравнение* (51) *при A, равном квадрату целого числа, имеет в целых числах только тривиальные решения* $x_0 = \pm 1$, $y_0 = 0$. *Такие же тривиальные решения имеет в целых числах уравнение* (51) *при A целом и отрицательном* (при $A = -1$ удовлетворяются симметричные тривиальные решения $x_0 = 0$, $y_0 = \pm 1$).

Рассмотрим теперь уравнение более общего вида

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

где $A > 0$ — целое, C — целое число, $\alpha = \sqrt{A}$ — иррациональное число. Мы уже видели, что при $C = 1$ это уравнение всегда имеет бесчисленное множество решений в целых числах x и y. При произвольных C и A такое уравнение может вообще не иметь решений.

Пример. Покажем, что *уравнение*

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

вообще не разрешимо в целых числах x и y. Заметим, прежде всего, что квадрат нечётного числа при делении на 8 всегда даёт в остатке 1. Действительно, так как всякое нечётное число a может быть записано в форме $a = 2N + 1$, где N — целое число, то

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

где M — целое число, в силу того, что или N, или $N+1$ должно быть чётным числом. Далее, если $[x_0, y_0]$ — решение уравнения (74), то x_0 и y_0 не могут быть числами одинаковой чётности. Если бы x_0 и y_0 были одновременно чётными или нечётными, то $x_0^2 - 3y_0^2$ было бы чётным чис-

лом и не могло быть равно 1. Если же x_0 нечётно, а y_0 чётно, то при делении на 4 x_0^2 давало бы в остатке 1, $-3y_0^2$ делилось бы на 4 и $x_0 - 3y_0^2$ при делении на 4 давало бы в остатке 1. Это невозможно, так как при делении на 4 правая часть тривиально даёт в остатке -1 или $3 = 4 - 1$. Наконец, если x_0 чётно, а y_0 нечётно, то x^2 делится на 4, $-3y_0^2$ на основании (75) может быть записано в форме

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

и, значит, при делении на 4 даёт в остатке 1. Поэтому $x_0^2 - 3y_0^2$ при делении на 4 должно опять давать в остатке 1, что, как мы уже видели, невозможно. Поэтому не существует целых чисел x_0 и y_0, которые могли бы удовлетворять уравнению (74).

Не останавливаясь на вопросе, при каких условиях, наложенных на C и A, уравнение (73) будет иметь решение, — вопросе трудном и разрешимом с помощью общей теории квадратических иррациональностей в алгебраической теории чисел, — мы остановимся на случае, когда уравнение (73) имеет нетривиальные решения. Попрежнему нетривиальным решением мы будем называть решение $[x', y']$, если $x', y' \neq 0$. Итак, пусть уравнение (73) имеет нетривиальное решение $[x', y']$; другими словами, пусть

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

Рассмотрим при том же A уравнение

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

Это уравнение имеет бесчисленное множество решений в целых числах при $A > 0$ и иррациональном $\alpha = \sqrt{A}$, и любое такое его решение $[\bar{x}, \bar{y}]$ будет:

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

где x_n и y_n определяются по формулам (50). Так как $[\bar{x}, \bar{y}]$ — решение уравнения (77), то

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

Равенство (76) в свою очередь может быть переписано в форме

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

Перемножая почленно эти два последних равенства, мы получаем:

$$(x'+\alpha y')(\overline{x}+\alpha\overline{y})(x'-\alpha y')(\overline{x}-\alpha\overline{y})=C. \qquad (78)$$

Но

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

и совершенно так же

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

Воспользовавшись этими двумя равенствами, мы можем переписать равенство (78) в форме

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

или в форме

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

Этим мы доказали, что если $[x', y']$ — решение уравнения (73), то этому уравнению будет удовлетворять и пара чисел $[x, y]$:

$$x=x'\overline{x}+Ay'\overline{y}, \quad y=x'\overline{y}+y'\overline{x}, \qquad (79)$$

где $[\overline{x}, \overline{y}]$ — любое решение уравнения (77). Таким образом, мы доказали, что *если уравнение* (73) *имеет хотя бы одно решение, то оно имеет их бесчисленное множество.*

Нельзя, конечно, утверждать, что формулами (79) даются все решения уравнения (73). В теории алгебраических чисел доказывается, что все решения в целых числах уравнения (73) можно получить, взяв некоторое конечное и определённое, зависящее от A и C число решений этого уравнения и размножив их с помощью формул (79). Уравнение (73) при A отрицательном или равном квадрату целого числа может иметь не более конечного числа решений. Это просто доказываемое утверждение мы предоставляем доказать читателю. Решение самых общих уравнений второй степени с двумя неизвестными в целых числах, уравнений вида

$$Ax^2+Bxy+Cy^2+Dx+Ey+F=0, \qquad (80)$$

где числа A, B, C, D, E и F — целые, сводится с помощью замен переменных к решению уравнений вида (73)

с положительным или отрицательным A. Поэтому характер поведения решений, если они существуют, такой же, как и у уравнения типа (73). Подводя итог всему вышеизложенному, мы можем теперь сказать, что *уравнение второй степени с двумя неизвестными типа* (80) *может не иметь решений в целых числах, может иметь их только в конечном числе и, наконец, может иметь бесконечное множество таких решений, причём эти решения берутся тогда из конечного числа обобщённых геометрических прогрессий, даваемых формулами* (79). Сравнивая поведение и характер решений в целых числах уравнений второй степени с двумя неизвестными с поведением решений уравнений первой степени, мы можем установить одно весьма существенное обстоятельство. Именно, если решения уравнения первой степени, когда они существуют, образуют арифметические прогрессии, то решения уравнений второй степени, когда их имеется бесконечно много, берутся из конечного числа обобщённых геометрических прогрессий. Другими словами, в случае второй степени пары целых чисел, которые могут быть решениями уравнения, значительно реже встречаются, чем пары целых чисел, которые могут быть решениями уравнения первой степени. Это обстоятельство не случайно. Оказывается, что уравнения с двумя неизвестными степени выше второй, вообще говоря, могут иметь только конечное число решений. Исключения из этого правила крайне редки.

§ 6. УРАВНЕНИЯ С ДВУМЯ НЕИЗВЕСТНЫМИ СТЕПЕНИ ВЫШЕ ВТОРОЙ

Уравнения с двумя неизвестными степени выше второй почти всегда, за редкими исключениями, могут иметь только конечное число решений в целых числах x и y. Рассмотрим, прежде всего, уравнение

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

где n — целое число, большее двух, и все числа a_0, a_1, a_2, ..., a_n, c — целые числа.

Как доказал в начале нашего столетия А. Туэ, *такое уравнение имеет только конечное число решений в целых числах x и y, за исключением, может быть, случаев,*

когда левая однородная часть этого уравнения есть степень однородного двучлена первой степени или трёхчлена второй степени. В этом последнем случае наше уравнение будет иметь одну из двух форм:

$$(ax+by)^n=c_0, \qquad (ax^2+bxy+cy^2)^n=c_0,$$

и тем самым сводится к уравнениям первой или второй степени, так как для существования у него решений c_0 должно быть n-й степенью целого числа. Мы не можем здесь изложить метод А. Туэ ввиду его сложности и ограничимся некоторыми пояснительными замечаниями, дающими указания на характер доказательства конечности числа решений уравнения (81)*).

Разделим обе части уравнения (81) на y^n. Наше уравнение примет тогда вид

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

Для простоты изложения будем предполагать не только, что все корни уравнения

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

различны и что $a_0a_n\neq 0$, но и что корни этого уравнения не могут быть корнями уравнений с целыми коэффициентами низшей степени. Этот случай является основным в нашем вопросе.

В высшей алгебре доказывается, что всякое алгебраическое уравнение имеет хотя бы один корень, откуда, уже весьма просто, на основании того, что всякий многочлен делится нацело на $z-\alpha$, если α — его корень, следует представление многочлена в виде произведения

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

где $\alpha_1, \alpha_2, \ldots, \alpha_n$ — все n корней данного многочлена. Пользуясь этим выражением многочлена в виде произведения, мы можем переписать уравнение (82) в виде

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

*) Литература по этому вопросу собрана, например, в обзорной статье А. О. Гельфонда «Приближения алгебраических чисел алгебраическими же числами и теория трансцендентных чисел», Успехи матем. наук, вып. 4, 4(32), 1949, стр. 19.

Допустим, что существует бесчисленное множество решений в целых числах $[x_k, y_k]$ уравнения (85). Это значит, что существуют решения со сколь угодно большими по абсолютной величине y_k. Если бы существовало бесчисленное множество пар с ограниченными, меньшими по абсолютной величине какого-то определённого числа, y_k и сколь угодно большими x_k, то для таких x_k левая часть была бы сколь угодно велика, а правая оставалась бы ограниченной, что невозможно. Пусть y_k будет очень велико. Тогда правая часть уравнения (85) будет мала, а значит, должна быть мала и левая часть. Но левая часть уравнения есть произведение n сомножителей, содержащих $\frac{x_k}{y_k}$ и a_0, которое, будучи целым, будет не меньше 1. Значит, малость левой части может обусловливаться только тем, что по абсолютной величине мала какая-то из разностей

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

Ясно, что эта разность может быть мала только в том случае, когда α_m действительно, — другими словами, не имеет места равенство $\alpha_m = a + bi$, $b \neq 0$. В противном случае модуль нашей разности не может быть сколь угодно мал, так как

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

Две разности, два множителя левой части уравнения (85) не могут быть одновременно малы по модулю, так как

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

в силу того, что среди чисел α_m нет одинаковых. Если одна разность меньше по модулю, или абсолютной величине, чем $\frac{1}{2}|\alpha_m - \alpha_s|$, то другая в силу (86) должна быть больше $\frac{1}{2}|\alpha_m - \alpha_s|$. Это есть следствие того, что абсолютная величина суммы не превосходит суммы абсолютных величин. Так как все числа α_m различны между собой,

то наименьшая по абсолютной величине, или модулю, разность $|\alpha_m - \alpha_s|$ будет больше нуля ($m \neq s$). Обозначая её величину через $2d$, мы будем иметь, что если при каком-нибудь достаточно большом y_k, что должно случиться, так как y_k неограниченно растёт,

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

то

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

Тогда, так как абсолютная величина, или модуль, произведения равна произведению абсолютных величин, или модулей, сомножителей, мы будем иметь из уравнения (85), что

$$|a_0|\left|\frac{x_k}{y_k} - \alpha_1\right| \ldots \left|\frac{x_k}{y_k} - \alpha_{m-1}\right|\left|\frac{x_k}{y_k} - \alpha_m\right|\left|\frac{x_k}{y_k} - \alpha_{m+1}\right| \ldots \left|\frac{x_k}{y_k} - \alpha_n\right| = \frac{|c|}{|y_k|^n}. \tag{88}$$

Но если в этом равенстве каждую из разностей $\left|\frac{x_k}{y_k} - \alpha_s\right|$, $s \neq m$, заменить меньшей величиной d, а $|a_0|$ заменить единицей, меньше которой целое число $|a_0|$ быть не может, то левая часть (88) станет меньше правой, и мы получаем неравенство

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

или неравенство

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

где c_1 не зависит от x_n и y_n. Чисел α_m не более n, а пар $[x_k, y_k]$, для которых должно быть при каком-нибудь m справедливо неравенство (89), бесчисленное множество. Поэтому существует какое-то определённое m, такое, что для соответствующего α_m неравенство (89) выполняется бесконечное множество раз. Другими словами, если уравнение (81) имеет бесконечное множество решений в целых числах, то алгебраическое уравнение (83) с целыми коэффициентами имеет такой корень α, для которого при сколь

угодно больших q будет выполняться неравенство

$$\left|\alpha-\frac{p}{q}\right|<\frac{A}{q^n}, \tag{90}$$

где A — постоянное, не зависящее от p и q число, p и q — целые числа, а n — степень уравнения, которому α удовлетворяет. Если бы α было произвольным действительным числом, то можно было бы его так выбрать, что действительно существовало бы бесчисленное множество решений неравенства (90) в целых числах p и q. Но в нашем случае α есть корень алгебраического уравнения с целыми коэффициентами. Такие числа называются *алгебраическими* и обладают особыми свойствами. *Степенью алгебраического числа* называется степень того алгебраического уравнения с целыми коэффициентами наименьшей степени, которому это число удовлетворяет.

А. Туэ доказал, что для алгебраического числа α степени n неравенство

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

может иметь только конечное число решений в целых числах p и q. Но если $n\geqslant 3$, правая часть неравенства (90) при достаточно большом q станет меньше правой части неравенства (91), так как $n>\frac{n}{2}+1$. Поэтому если неравенство (91) может иметь только конечное число решений в целых числах p и q, то неравенство (90) и подавно имеет только конечное число решений. Значит, уравнение (81) может иметь только конечное число решений в целых числах, когда все корни уравнения (83) не могут быть корнями уравнения с целыми коэффициентами низшей, чем n, степени. При $n=2$, как легко можно установить, неравенство (90) действительно может иметь бесчисленное множество решений в целых p и q при некотором A. Теорема А. Туэ была в дальнейшем значительно усилена. Следует только отметить, что метод доказательства его теоремы принципиально не даёт возможности найти верхнюю границу для величины решений, — другими словами, границу возможных величин $|x|$ и $|y|$ по его коэффициентам $a_0, a_1, \ldots, a_n$ и c. Этот

вопрос и сегодня остаётся открытым. Не давая возможности найти границу величины решений, метод А. Туэ даёт зато возможность найти границу для числа решений уравнения (83), правда, достаточно грубую. Для отдельных классов уравнений типа (83) эта граница может быть значительно уточнена. Например, советский математик Б. Н. Делоне *) показал, что уравнение

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

при a целом может иметь, кроме тривиального $x=0$, $y=1$, не более одного решения в целых числах x и y. Кроме того, он показал, что уравнение

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

может иметь не более пяти решений в целых x и y при целых a, b, c и d.

Пусть $P(x, y)$ будет произвольный многочлен с целыми коэффициентами относительно x и y, — другими словами,

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

где A_{ks} — целые числа. Мы будем говорить, что этот *многочлен неприводим*, если его нельзя представить в виде произведения двух других многочленов с целыми коэффициентами, каждый из которых не есть просто число.

Особым и весьма сложным методом К. Зигель доказал, что уравнение

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

где $P(x, y)$ — неприводимый многочлен выше чем второй степени относительно x и y (другими словами, если в него входит член вида $A_{ks}x^ky^s$, где $k+s>2$), может иметь бесконечное множество решений в целых x и y только тогда, когда существуют числа a_n, a_{n-1}, ..., a_0, a_{-1}, ..., a_{-n} и b_n, b_{n-1}, ..., b_0, b_{-1}, ..., b_{-n} такие, что при подстановке вместо x и y в наше уравнение

$$x=a_nt^n+a_{n-1}t^{n-1}+\ \dots\ +a_0+\frac{a_{-1}}{t}+\dots+\frac{a_{-n}}{t^n},$$

$$y=b_nt^n+b_{n-1}t^{n-1}+\ \dots\ +b_0+\frac{b_{-1}}{t}+\dots+\frac{b_{-n}}{t^n}$$

мы получим тождество

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

относительно t. Здесь n — некоторое целое число.

*) Литературу по этому вопросу см. в статье А. О. Гельфонда «Теория чисел» в сборнике «Математика в СССР за тридцать лет», ГТТИ, 1948.

§ 7. АЛГЕБРАИЧЕСКИЕ УРАВНЕНИЯ СТЕПЕНИ ВЫШЕ ВТОРОЙ С ТРЕМЯ НЕИЗВЕСТНЫМИ И НЕКОТОРЫЕ ПОКАЗАТЕЛЬНЫЕ УРАВНЕНИЯ

Если для уравнений с двумя неизвестными мы можем дать ответ на вопрос о существовании конечного или бесконечного числа решений в целых числах, то для уравнений с более чем двумя неизвестными степени выше второй дать ответ на этот вопрос мы можем только для весьма частных классов уравнений. Тем менее в этом последнем случае поддаётся разрешению и более трудный вопрос об определении всех решений уравнения в целых числах. В качестве примера остановимся на так называемой великой теореме Ферма.

Замечательный французский математик Пьер Ферма высказал утверждение, что уравнение

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

при целом $n \geqslant 3$ не имеет решений в целых положительных числах x, y, z (случай $xyz = 0$ исключается положительностью x, y, z). Несмотря на то, что П. Ферма утверждал, что он имеет доказательство (повидимому, методом спуска, о котором речь будет ниже) этого утверждения, его доказательство впоследствии не было найдено. Более того, когда математик Куммер попытался его найти и даже думал одно время, что он его нашёл, он обнаружил, что одно положение, верное в области обычных целых чисел, оказывается неверным для более сложных числовых образований, с которыми естественно приходится сталкиваться при исследовании проблемы Ферма. Это обстоятельство заключается в том, что так называемые *целые алгебраические числа*, — другими словами, корни алгебраических уравнений с целыми рациональными коэффициентами и с коэффициентом при старшей степени, равным 1, — могут не единственным способом быть разложены на простые, неразложимые в свою очередь, целые сомножители той же алгебраической природы. Обычные же целые числа разлагаются на простые множители единственным образом. Например, $6 = 2 \cdot 3$ и никаких других разложений не допускает внутри совокупности обычных целых чисел. Рассмотрим совокупность

всех целых алгебраических чисел вида $m+n\sqrt{-5}$, где m и n — обычные целые числа. Легко видеть, что сумма и произведение двух таких чисел опять будут числом той же совокупности. Совокупность чисел, обладающая тем свойством,что она содержит любые суммы и произведения чисел, в неё входящих, называется кольцом. По определению, в нашем кольце содержатся числа 2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$. Каждое из этих чисел в этом кольце, как легко можно установить, будет простым, т. е. не будет представляться в виде произведения двух не равных единице целых чисел нашего кольца. Но

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

другими словами, число 6 не единственным образом разлагается на простые сомножители в нашем кольце. То же обстоятельство, неединственность разложения на простые сомножители, может иметь место и в других, более сложных, кольцах алгебраически целых чисел. Обнаружив это обстоятельство, Куммер убедился, что его доказательство общей великой теоремы Ферма неверно. Для преодоления трудностей, связанных с неединственностью разложения на множители, Куммером была построена теория идеалов, которая играет в настоящее время исключительно большую роль в алгебре и теории чисел. Но даже с помощью этой новой теории полностью доказать великую теорему Ферма Куммер не смог и доказал её только для n, делящихся хотя бы на одно из так называемых регулярных простых чисел. Не останавливаясь на расшифровке понятия регулярного простого числа, мы можем указать только, что до настоящего времени не известно, существует ли только конечное число таких простых чисел или их бесконечное множество.

В настоящее время великая теорема Ферма доказана для многих n, в частности для любого n, делящегося на простое число, меньшее 100. Великая теорема Ферма сыграла большую роль в развитии математики благодаря связанному с попытками её доказательства открытию теорий идеалов. Но при этом следует отметить, что совсем другим путём и по другому поводу эта теория была

построена замечательным русским математиком Е. И. Золотарёвым, умершим в расцвете своей научной деятельности. В настоящее время доказательство великой теоремы Ферма, особенно доказательство, построенное на соображениях теории делимости чисел, может иметь только спортивный интерес. Конечно, если это доказательство будет получено новым и плодотворным методом, то значение его, связанное со значением самого метода, может быть и очень большим. Следует отметить, что попытки, делающиеся любителями математики и в наше время, доказать теорему Ферма совсем элементарными средствами обречены на неудачу. Элементарные соображения, опирающиеся на теорию делимости чисел, были использованы ещё Куммером и дальнейшая их разработка самыми выдающимися математиками пока ничего существенного не дала.

Мы приведём здесь доказательство теоремы Ферма для случая $n=4$, так как *метод спуска*, на котором это доказательство построено, очень интересен.

Теорема IV. *Уравнение Ферма*

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

не имеет решений в целых числах x, y и z, $xyz\neq 0$.

Доказательство. Мы докажем даже более сильную теорему, именно, что уравнение

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

не имеет решений в целых числах x, y, z, $xyz\neq 0$. Из этой теоремы уже следует непосредственно отсутствие решений у уравнения (93). Если уравнение (94) имеет решение в целых, отличных от нуля числах x, y, z, то можно предполагать, что эти числа попарно взаимно просты. Действительно, если есть решение, в котором числа x и y имеют общий наибольший делитель $d>1$, то

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

где $(x_1, y_1)=1$. Разделив обе части уравнения (94) на d^4, мы будем иметь, что

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

Но x_1 и y_1 — целые числа, значит, $z_1=\frac{z}{d^2}$ — тоже целое число. Если бы у z_1 и y_1 был общий делитель $k>1$, то x_1^2 в силу (95) должно было бы делиться на k, а значит, x_1 и k не могли бы быть взаимно просты. Итак, мы доказали, что если существует решение уравнения (94) в целых, отличных от нуля числах, то существует также решение в целых, отличных от нуля и взаимно простых числах. Поэтому нам достаточно доказать, что уравнение (94) не имеет решений в целых, отличных от нуля и попарно взаимно простых числах. В дальнейшем ходе доказательства мы, говоря, что уравнение (94) имеет решение, будем предполагать, что оно имеет решение в целых, положительных и попарно взаимно простых числах.

В § 3 мы доказали, что все решения уравнения (12)

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

в целых положительных, попарно взаимно простых числах определяются по формуле (18) и имеют вид

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

где u и v — два любых нечётных, взаимно простых положительных числа.

Придадим несколько другой вид формулам (97), определяющим все решения уравнения (96). Так как u и v — нечётные числа, то, положив

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

мы определим числа u и v равенствами

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

где a и b — целые числа разной чётности. Равенства (98) и (99) показывают, что любой паре нечётных взаимно простых чисел u и v соответствует пара взаимно простых чисел a и b разной чётности и что любой паре взаимно простых чисел a и b разной чётности соответствует пара взаимно простых нечётных чисел u и v.

Поэтому, сделав в формулах (97) замену u и v на a и b, мы получим, что все тройки целых положительных и попарно взаимно простых чисел x, y, z (x — нечётное), являющиеся решениями уравнения (96), определяются по формулам

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

где a и b — два любых взаимно простых числа разной чётности при условии, что $x>0$. Эти формулы показывают, что x и y разной чётности. Если уравнение (94) имеет решение $[x_0, y_0, z_0]$, то это значит, что

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

другими словами, что тройка чисел (x_0^2, y_0^2, z_0) является решением уравнения (96). Но тогда должны существовать два числа a и b, $a>b$, взаимно простых и разной чётности, таких, что

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

Мы допускаем при этом, для определённости, что x_0 нечётно, а y_0 чётно. Противоположное допущение ничего не изменило бы, так как было бы достаточно x_0 заменить на y_0 и наоборот. Но мы уже знаем (см. равенство (75)), что квадрат нечётного числа даёт в остатке 1 при делении на 4. Поэтому из равенства

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

следует, что a нечётно, а b чётно. В противном случае левая часть этого равенства при делении на 4 давала бы в остатке 1, а правая, так как мы предположили a чётным, а b нечётным, —1. Так как a нечётно и $(a, b)=1$, то и $(a, 2b)=1$. Но тогда из равенства

$$y_0^2=2ba$$

следует, что

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

где t и s — какие-то целые числа. Но из соотношения (102) следует, что $[x_0, b, a]$ есть решение уравнения (96). Значит,

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

где m и n — некоторые взаимно простые числа разной чётности. Из (103) имеем:

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

откуда в силу взаимной простоты m и n следует, что

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

где p и q — отличные от нуля целые числа. Так как $a=t^2$ и $a=m^2+n^2$, то

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

Но

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

Поэтому

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

Положив $q=x_1$, $p=y_1$ и $t=z_1$, мы видим, что если существует решение $[x_0, y_0, z_0]$, то должно существовать и другое решение $[x_1, y_1, z_1]$, причём $0<z_1<z_0$. Этот процесс получения решений уравнения (94) можно продолжить неограниченно, и мы получим последовательность решений

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

причём целые положительные числа $z_0, z_1, z_2, \ldots, z_n, \ldots$ будут монотонно убывать; другими словами, будут верны для них неравенства

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

Но целые положительные числа не могут образовать бесконечную монотонно убывающую последовательность, так как в такой последовательности не может быть больше z_0 членов. Мы пришли, таким образом, к противоречию, предположив, что уравнение (94) имеет хотя бы одно решение в целых x, y, z, $xyz\neq 0$. Этим доказано, что уравнение (94) не имеет решений. Следовательно, и уравнение (93) не имеет решений в целых положительных числах $[x, y, z]$, так как в противном случае, если $[x, y, z]$ — решение (93), то $[x, y, z^2]$ — решение (94).

Метод доказательства, которым мы пользовались, заключавшийся в построении с помощью одного решения

бесчисленной последовательности решений с неограниченно убывающими положительными z, называется методом спуска. Как мы уже говорили выше, осуществить этот метод в общем случае теоремы Ферма мешает пока неединственность разложения целых чисел алгебраических колец на простые сомножители из того же кольца *).

Заметим, что мы доказали отсутствие целых решений не только у уравнения (94), но и у уравнения

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

Любопытно отметить, что уравнение

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

имеет бесчисленное множество решений в целых положительных числах, например $x=2$, $y=3$, $z=5$. Найти вид всех решений этого уравнения в целых положительных x, y, z мы предоставляем читателю.

Приведём ещё один пример на метод спуска, несколько изменив ход рассуждений.

Пример. *Докажем, что уравнение*

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

не имеет решений в целых, отличных от нуля числах x, y, z. Допустим, что уравнение (107) имеет решение в целых положительных числах $[x_0, y_0, z_0]$. Эти числа мы сразу можем предполагать взаимно простыми, так как если бы они имели общим наибольшим делителем $d>1$, то числа $\frac{x_0}{d}$, $\frac{y_0}{d}$, $\frac{z_0}{d^2}$ также были бы решением уравнения (107). Наличие же общего делителя у двух из них влекло бы за собой существование общего делителя у всех трёх. Кроме того, предположим, что z_0 — наименьшее из всех возможных z в решениях (107) в целых положительных числах. Так как $[x_0, y_0, z_0]$ — решение уравнения (107), то $[x_0^2, y_0^2, z]$ будут решением уравнения

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

*) За дальнейшими сведениями относительно великой теоремы Ферма мы отсылаем к книге А. Я. Хинчина «Великая теорема Ферма».

Пользуясь формулами (19′) § 3, дающими все целые положительные решения (108), мы видим, что существуют такие целые положительные a и b, $(a, b)=1$, a нечётно, которые удовлетворяют равенствам

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

Из равенства $y_0^2=2ab$ следует, что b само должно быть чётно, так как y_0 чётно, y_0^2 делится на 4, а a нечётно. Так как $\frac{b}{2}$ и a взаимно просты, то из равенства

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

непосредственно следует, что

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

где m и n — целые положительные и $(m, 2n)=1$. Но из (109) следует

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

где x_0 и a нечётны. Мы уже видели, что квадрат нечётного числа при делении на 4 даёт в остатке 1. Поэтому левая часть (110) при делении на 4 даёт в остатке 1, а $a^2-8\left(\frac{b}{2}\right)^2$ тоже даёт в остатке 1 при делении на 4. Значит, в равенстве (110) скобка в правой части может входить только с плюсом. Теперь равенство (110) можно записать уже в форме

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

или в форме

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

где x_0, n и m — целые положительные и взаимно простые числа. Значит, числа x_0, $2n^2$, m^2 образуют решение уравнения (108), причём x_0, $2n^2$ и m^2 взаимно просты. Поэтому опять в силу формул (19′) § 3 найдутся такие целые числа p и q, p нечётно, $(p, q)=1$, что

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

Но так как $(p, q)=1$ и $n^2=pq$, то

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

где s и r — целые взаимно простые числа. Отсюда окончательно следует соотношение

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

которое показывает, что числа s, r, m образуют решение уравнения (107). Но из вышеполученных равенств

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

следует, что $z_0 > m$. Итак, имея решение $[x_0, y_0, z_0]$, мы нашли другое решение $[s, r, m]$, причём $0 < m < z_0$. Это же противоречит предположению, которое мы сделали, что решение $[x_0, y_0, z_0]$ имеет z_0 наименьшим из возможных. Таким образом, мы пришли к противоречию, допустив существование решения у уравнения (107), и доказали, что это уравнение неразрешимо в целых, отличных от нуля числах.

Мы предоставляем теперь читателям доказать, что уравнения

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

неразрешимы в целых положительных числах.

В заключение сделаем несколько замечаний о показательных уравнениях. *Уравнение*

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

где a, b и c — целые, не равные степени двойки и нулю, может иметь не более чем конечное число решений в целых числах x, y, z. Это же утверждение с небольшим дополнительным условием остаётся в силе, когда a, b и c будут произвольными алгебраическими числами. Более того, уравнение

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

где A, B, C, $ABC \neq 0$, — целые, $\alpha_1, \dots, \alpha_n$, $\beta_1, \dots, \beta_n$, $\gamma_1, \dots, \gamma_n$ — целые и числа α, β, γ,

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

взаимно просты, может иметь только конечное число решений в целых числах $x_1, \dots, x_n, y_1, \dots, y_m, z_1, \dots, z_p$. Это утверждение также обобщается на случай A, B, C

и α_i, β_k, γ_s алгебраических *). Уравнения типа (115) и их обобщения представляют большой интерес, так как в теории алгебраических чисел доказывается, что каждому алгебраическому уравнению типа (81) соответствует некоторое показательное уравнение типа (115), причём каждому решению уравнения (81) соответствует решение уравнения (115) в целых числах. Такое соответствие распространяется и на уравнения более общего типа, чем (81) и (115).

*) См. обзорную статью А. О. Гельфонда, цитировавшуюся на стр. 48.

ОГЛАВЛЕНИЕ