Библиотека
«Математическое просвещение»
Выпуск 8

В. В. Острик, М. А. Цфасман

АЛГЕБРАИЧЕСКАЯ ГЕОМЕТРИЯ И ТЕОРИЯ ЧИСЕЛ:

РАЦИОНАЛЬНЫЕ И ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

Третье издание,
стереотипное

Издательство Московского центра
непрерывного математического образования
Москва • 2011

УДК 511.5 + 512.75
ББК 22.147
О-76

Острик В. В., Цфасман М. А.
О-76 Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые / В. В. Острик, М. А. Цфасман : 3-е изд., стер. — М. : изд-во МЦНМО, 2011. — 48 с. : ил.
ISBN 978-5-94057-789-8

Многие естественные вопросы из теории чисел красиво решаются геометрическими методами, точнее говоря, методами алгебраической геометрии — области математики, изучающей кривые, поверхности и т. д., задаваемые системами полиномиальных уравнений. В книжке это показано на примере нескольких красивых задач теории чисел, связанных с теоремой Пифагора.

Текст книжки представляет собой значительно пополненную обработку записей лекций, прочитанных В. В. Остриком 18 марта 2000 года на Малом мехмате для школьников 9—11 классов и М. А. Цфасманом 19 марта 2000 года на торжественном закрытии LXIII Московской математической олимпиады школьников (запись Е. Н. Осьмовой, М. Ю. Панова).

Рассчитана на широкий круг читателей, интересующихся математикой: школьников старших классов, студентов младших курсов, учителей.

1-е изд. — 2001 год; 2-е изд., испр. и доп. — 2005 год.

УДК 511.5 + 512.75
ББК 22.147

Серия «Библиотека „Математическое просвещение“»
Серия основана в 1999 году

Выпуск 8

Острик Виктор Валентинович, Цфасман Михаил Анатольевич
АЛГЕБРАИЧЕСКАЯ ГЕОМЕТРИЯ И ТЕОРИЯ ЧИСЕЛ:
рациональные и эллиптические кривые

3-е изд., стер.

Редактор *М. Г. Быкова* Тех. редактор *Д. Е. Юрьев*

Подписано в печать 5/IX 2011 года. Формат 60×84 $^1/_{16}$. Бумага офсетная № 1. Печать офсетная. Объём 3,0 печ. л. Тираж 2000 экз. Заказ .

Издательство Московского центра непрерывного математического образования.
119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241 74 83.

Отпечатано с готовых диапозитивов в ППП «Типография „Наука“».
121099, Москва, Шубинский пер., 6.

ISBN 978-5-94057-789-8

ПИФАГОРОВЫ ТРОЙКИ

Для прямоугольного треугольника с катетами X и Y и гипотенузой Z выполняется теорема Пифагора: сумма квадратов катетов равна квадрату гипотенузы, т. е. верно равенство

$$X^2 + Y^2 = Z^2. \qquad (1)$$

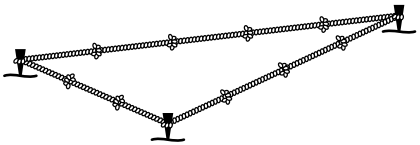


Рис. 1

Ещё в глубокой древности был известен пример целых чисел X, Y, Z, удовлетворяющих этому уравнению: $X = 3$, $Y = 4$, $Z = 5$. Соответствующий треугольник называется египетским. Его можно строить так: верёвочное кольцо с узелками, делящими его на 12 равных частей, растягиваем на трёх колышках, воткнутых в землю, так, чтобы образовался треугольник со сторонами 3, 4 и 5 (рис. 1). Это — способ строить на земле прямой угол.

Опишем все *пифагоровы тройки*, т. е. тройки целых чисел (X, Y, Z), для которых выполняется соотношение $X^2 + Y^2 = Z^2$. Прежде всего заметим, что если найдена такая тройка, то, умножив все три числа на некоторое целое число, вновь получим пифагорову тройку. Поэтому достаточно найти лишь тройки взаимно простых чисел. Более того, достаточно найти тройки попарно взаимно простых чисел: если какие-то два из чисел X, Y, Z делятся на некоторое простое число p, то и третье число обязательно делится на p.

Заметим, что единственное решение с $Z = 0$ есть $X = Y = Z = 0$, и в дальнейшем рассматривать его не будем. Для всех остальных решений уравнения $X^2 + Y^2 = Z^2$ число Z отлично от нуля. Разделив на его квадрат, получим новое уравнение

$$x^2 + y^2 = 1, \qquad (2)$$

где $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ — рациональные числа.

Уравнение (2) задаёт окружность S радиуса 1 с центром в начале координат (рис. 2). Исходная задача свелась к следующей: перечислить все рациональные точки[1]) этой окружности. Оказывается, что их в некотором смысле столько же, сколько рациональных точек

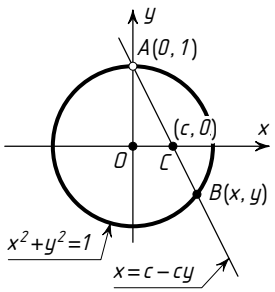


Рис. 2

[1]) Рациональная точка — точка с рациональными координатами.

на числовой прямой. Некоторые из рациональных точек легко найти: $(\pm 1, 0)$, $(0, \pm 1)$. Выберем одну из них, скажем, $A = (0, 1)$. Проведём через точку A всевозможные прямые (кроме горизонтальной). Каждая такая прямая l пересечёт окружность ещё в одной точке $B = (x, y)$ и ось абсцисс в некоторой точке $C = (c, 0)$.

1. Проверьте, что, сопоставляя точке B точку C, мы получаем взаимно однозначное соответствие между точками окружности S (кроме A) и точками прямой $y = 0$ [1]).

Такова геометрия. А как же с арифметикой? Оказывается, что это соответствие сохраняет рациональность точки.

Докажем, что точка B имеет рациональные координаты тогда и только тогда, когда рационально число c. Прямая, проходящая через точки A и C, определяется уравнением $x = c - cy$. Подставим его в уравнение окружности. Получим, что

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

откуда $y = 1$ (что соответствует точке A) или $y = \dfrac{c^2 - 1}{c^2 + 1}$, при этом $x = c - cy = \dfrac{2c}{c^2 + 1}$. Если число c рационально, то x и y тоже рациональны.

Обратное сразу вытекает из следующих двух утверждений (которыми мы будем пользоваться постоянно).

2. Если координаты двух точек рациональны, то уравнение соединяющей их прямой можно записать так, чтобы оно имело рациональные коэффициенты.

Если две прямые задаются уравнениями с рациональными коэффициентами, то точка их пересечения (если она существует) имеет рациональные координаты.

Таким образом, каждое рациональное решение уравнения (2), кроме $x = 0$, $y = 1$, получается, если в формулы

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

подставить вместо c некоторое рациональное число.

Представим число c в виде несократимой дроби m/n (m и n — целые числа). Тогда

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

(заметим, что при $n = 0$, $m \neq 0$ мы получаем «потерянное» было решение $x = 0$, $y = 1$).

[1]) Двумя чертами слева выделены тексты задач для самостоятельного решения. Задачи повышенной сложности отмечены знаком *.

Напомним, что нам требуется найти все целые решения уравнения (1). Имеем:

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

(где $m^2+n^2\neq 0$). Дроби, стоящие в левых частях этих равенств, несократимы, поскольку числа X, Y, Z попарно взаимно просты. Если бы мы знали, что дроби, стоящие в правых частях равенств, тоже несократимы, мы могли бы положить $X=2mn$, $Y=m^2-n^2$, $Z=m^2+n^2$, но, например, при $m=5$, $n=3$ обе эти дроби сократимы. Однако они могут быть сократимы только на 2. Действительно, рассмотрим первую дробь: пусть простое число p ($p\neq 2$) делит $2mn$; если p делит m, то число n не может делиться на p, поскольку дробь m/n несократима. Следовательно, m^2+n^2 не делится на p. Поэтому дробь $\frac{2mn}{m^2+n^2}$ может быть сокращена только на 2, в случае если m и n нечётны. Рассмотрим теперь вторую дробь: если простое число p делит и m^2-n^2, и m^2+n^2, то p делит $2m^2$ и $2n^2$. У m и n общих делителей нет, значит, $p=2$, а m и n нечётны.

Итак, взаимно простые натуральные решения (1) суть

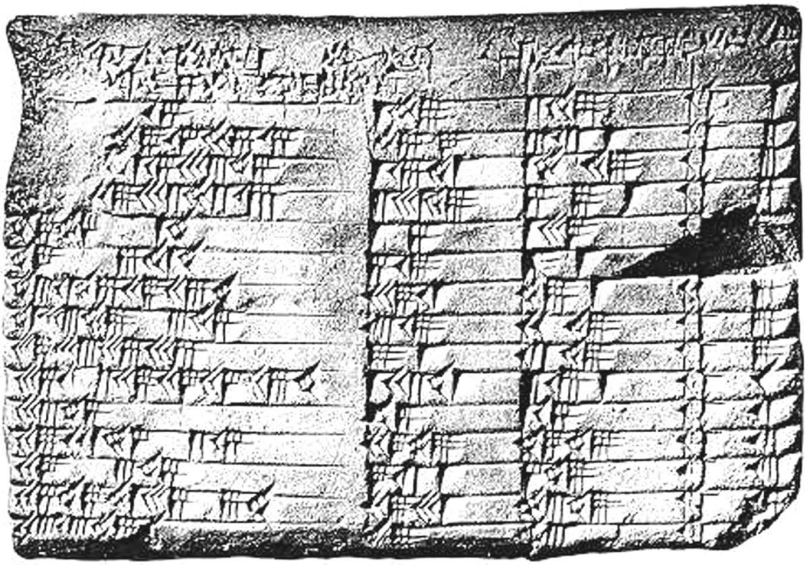
$$X=mn, \quad Y=\frac{m^2-n^2}{2}, \quad Z=\frac{m^2+n^2}{2} \tag{3}$$

при взаимно простых нечётных m и n, $m>n>0$, а также

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

при взаимно простых m и n, $m>n>0$, одно из которых чётно. (Нетрудно проверить, что любая такая тройка (X, Y, Z) действительно является решением.) Любые целые положительные решения получаются умножением (3) или (4) на натуральное число.

Заметим, что формулы (3) и (4) на самом деле совпадают. Если $X=pq$, $Y=\frac{p^2-q^2}{2}$, $Z=\frac{p^2+q^2}{2}$ — решение, вычисленное по формулам (3) (числа p и q оба нечётны и взаимно просты), то это же решение получается по формулам (4) при $m=\frac{p+q}{2}$, $n=\frac{p-q}{2}$ (проверьте, что m и n взаимно просты и ровно одно из этих чисел чётно), правда X и Y при этом меняются местами. Аналогично, любое решение вида (4) можно записать в виде (3). Можно сказать, что все натуральные решения (1) описываются формулами (4) с точностью до перестановки X и Y и умножения X, Y и Z на некоторое натуральное число.



Глиняная табличка Plimpton 322 из Плимптоновской библиотеки Колумбийского университета в Нью-Йорке — древневавилонский клинописный текст (XIX—XVII вв. до н. э.). Найдена в 1920-х годах Дж. Плимптоном.

В табличке перечислено несколько прямоугольных треугольников с целыми сторонами X, Y и Z. Слева несколько столбцов отломано. Первый сохранившийся столбец (I) содержит отношения $\frac{Z^2}{X^2}$, которые плавно убывают от 2 до величины, чуть большей 4/3. Два следующих столбца (II и III) дают «ширину» Y и «диагональ» Z. Последний столбец (IV) содержит только ряд следующих друг за другом чисел от 1 до 15.

Ширина Y и диагональ Z удовлетворяют уравнению

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

в котором «высота» X — целое число, причём простые делители X — только 2, 3 и 5. В 11-й и 15-й строчках числа X, Y и Z имеют общий делитель, больший 1. Во всех остальных случаях эти числа взаимно просты.

Расшифровка таблички Plimpton 322 приведена на стр. 7 (сначала числа записаны в шестидесятеричной системе счисления, принятой в Вавилоне, например, наша запись 1,22;5,14 обозначает число

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

затем числа записаны в десятичной системе).

Следует отметить, что запись чисел в Вавилоне была неоднозначной. Например, записи 1,22;5,14, 1,22,5;14 и 1,22,5,14 (соответствующие разным числам) никак не различались, и понять, какое именно из этих чисел подразумевалось, можно было только из контекста, не различались и, например, записи 5,14;1 и 5,0,14;1, в связи с отсутствием знака для нуля. Приводимая расшифровка сделана в предположении, что все числа, записанные в колонках II и III таблички, являются целыми (точнее, из возможных значений выбиралось наименьшее натуральное).

Z^2/X^2	X	Y	Z	Номер
1;59,0,15	2,0	1,59	2,49	1
1;56,56,58,14,50,6,15	57,36	56,7	1,20,25[1])	2
1;55,7,41,15,33,45	1,20,0	1,16,41	1,50,49	3
1;53,10,29,32,52,16	3,45,0	3,31,49	5,9,1	4
1;48,54,1,40	1,12	1,5	1,37	5
1;47,6,41,40	6,0	5,19	8,1	6
1;43,11,56,28,26,40	45,0	38,11	59,1	7
1;41,33,45,14,3,45	16,0	13,19	20,49	8
1;38,33,36,36	10,0	8,1[2])	12,49	9
1;35,10,2,28,27,24,26	1,48,0	1,22,41	2,16,1	10
1;33,45	1,0	45	1,15	11
1;29,21,54,2,15	40,0	27,59	48,49	12
1;27,0,3,45	4,0	2,41[3])	4,49	13
1;25,48,51,35,6,40	45,0	29,31	53,49	14
1;23,13,46,40	1,30	56	1,46[4])	15
I		II	III	IV

примерно	1,98340	120	119	169	1
»	1,94916	3456	3367	4825	2
»	1,91880	4800	4601	6649	3
»	1,88625	13500	12709	18541	4
»	1,81501	72	65	97	5
»	1,78519	360	319	481	6
»	1,71998	2700	2291	3541	7
»	1,69271	960	799	1249	8
»	1,64267	600	481	769	9
»	1,58612	6480	4961	8161	10
	1,5625	60	45	75	11
примерно	1,48942	2400	1679	2929	12
»	1,45002	240	161	289	13
»	1,43024	2700	1771	3229	14
»	1,38716	90	56	106	15

При расшифровке таблички сделаны следующие четыре исправления:
[1]) число 3,12,1 (записанное в табличке Plimpton 322) заменено на 1,20,25;
[2]) число 9,1 заменено на 8,1;
[3]) число 7,12,1 заменено на 2,41;
[4]) число 53 заменено на 1,46.

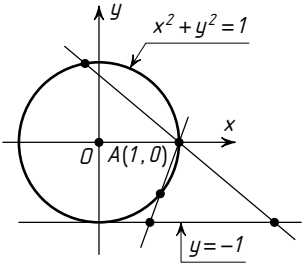


Рис. 3

Вот ещё один способ записать все решения уравнения (1):

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

где m и n — произвольные целые числа, а r — подходящее рациональное число, т. е. такое, что X, Y, Z — целые.

Проверьте, что известные нам решения (3, 4, 5) и (4, 3, 5) получаются, соответственно, из формул (3) при $m=3$, $n=1$ и из формул (4) при $m=2$, $n=1$. Эти решения можно также получить из (3′—4′) при $m=3$, $n=1$, $r=\frac{1}{2}$ и при $m=2$, $n=1$, $r=1$.

3. Выпишите все пифагоровы тройки (a, b, c), такие что $0<a<b<c<100$.

4. Что получится, если в качестве точки A взять $(1, 0)$ и рассматривать точки пересечения прямых, проходящих через A, не с осью абсцисс, а с прямой $y=-1$ (рис. 3)?

Немного истории

Древние греки узнали про треугольник со сторонами 3, 4, 5 от египтян и назвали его египетским. Мы называем прямоугольные треугольники с целыми сторонами пифагоровыми. Но ни египтяне, ни Пифагор не были первыми. Уже в архитектуре древнемесопотамских надгробий (примерно 5000 лет тому назад) встречается равнобедренный треугольник, составленный из двух прямоугольных со сторонами 9, 12 и 15 локтей. А пирамиды фараона Снофру (XXVII в. до н. э.) построены с использованием прямоугольного треугольника со сторонами 20, 21 и 29 десятков египетских локтей и другого прямоугольного треугольника со сторонами 18, 24 и 30 десятков египетских локтей. В глиняной табличке Plimpton 322 (XIX—XVII вв. до н. э.) имеется 15 строк, содержащих значения Y, Z и $\frac{Z^2}{X^2}$ (стр. 6—7). Обратите внимание на то, что приводимые там числа довольно велики. Естественно предположить, что вавилоняне знали общий метод поиска решений.

Греческий математик Диофант (III в. н. э.) умел решать в целых числах не только уравнение (1), но и другие квадратные уравнения, некоторые системы из двух квадратных уравнений от трёх переменных, а также некоторые кубические уравнения от двух переменных (см. приложение 4).

Скорее всего, он опирался на работы многих своих предшественников. Теория чисел нового времени началась с заметок Ферма на полях книги Диофанта. Основы нашего геометрического подхода к уравнениям в целых числах заложил Ньютон, понявший, что сложные замены переменных, используемые Диофантом, зачастую сводятся к проведению секущих и касательных.

РАЦИОНАЛЬНЫЕ КРИВЫЕ

Разобранный приём с проведением секущих является весьма общим. Решим с его помощью следующую задачу: описать такие тройки целых чисел, что квадрат одного плюс удвоенный квадрат другого равен утроенному квадрату третьего, т. е. решим в целых числах уравнение

$$X^2 + 2Y^2 = 3Z^2. \qquad (5)$$

Как и раньше, заметим, что единственным решением с $Z = 0$ является решение $X = Y = Z = 0$, которое далее рассматривать не будем. Разделим обе части равенства на Z^2, получим новое уравнение

$$x^2 + 2y^2 = 3, \qquad (6)$$

где $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ — рациональные числа.

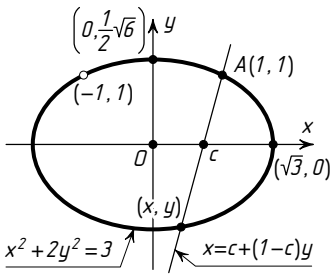


Рис. 4

Уравнение (6) описывает эллипс с полуосями $\sqrt{3}$ и $\frac{1}{2}\sqrt{6}$ и центром в начале координат (рис. 4). Нетрудно найти рациональную точку на этом эллипсе: таковой, например, является точка $A(1, 1)$. Так же как в задаче о пифагоровых тройках, установим взаимно однозначное соответствие между точками эллипса (кроме $(-1, 1)$) и точками прямой $y = 0$. (Рациональных точек на эллипсе опять столько же, сколько на прямой.) Уравнение прямой, проходящей через точки $A(1, 1)$ и $(c, 0)$, можно записать в виде $x = c + (1 - c)y$. Ордината второй точки пересечения прямой с эллипсом удовлетворяет уравнению

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

Один корень этого квадратного уравнения нам известен, он равен 1. Теперь, используя теорему Виета, несложно найти второй

его корень: $y = \frac{c^2-3}{c^2-2c+3}$. Тогда $x = c + (1-c)y = \frac{-c^2+6c-3}{c^2-2c+3}$. (Заметим, что при $c=3$ получаем $x=1$, $y=1$, т. е. это не вторая точка пересечения, а точка касания. В то же время точка $(-1, 1)$ нам не встретится.)

Пользуясь утверждениями задачи 2, мы получаем, что все рациональные решения уравнения (6) описываются формулами

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

где c — рациональное число (кроме решения $x=-1$, $y=1$, которое соответствует горизонтальной прямой), а целые решения уравнения (5) — формулами

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

где m и n — целые числа, r — подходящее рациональное[1]).

5. Опишите все целые решения уравнений
а) $X^2-15Y^2=Z^2$, б) $X^2-YZ=9Z^2$, в) $X^2+3Y^2=5Z^2$.

* * *

Пусть теперь кривая задаётся уравнением $f(x, y)=0$, причём многочлен $f(x, y)$ не разлагается в произведение многочленов степени выше нулевой, даже если допускать комплексные коэффициенты (такие кривые называются *абсолютно неприводимыми*)[2]). Если, как в разобранных нами примерах, существуют многочлены $F(c)$, $G(c)$ и $H(c)$ с рациональными коэффициентами, такие что хотя бы одна из функций $\frac{F(c)}{H(c)}$ и $\frac{G(c)}{H(c)}$ непостоянна и при подстановке $x=\frac{F(c)}{H(c)}$, $y=\frac{G(c)}{H(c)}$ в $f(x, y)$ мы получаем тождественный нуль, то наша кривая называется *рациональной* (поскольку отношение двух многочленов называется рациональной функцией).

6. Пусть $f(x, y)$ — многочлен второй степени с рациональными коэффициентами, причём кривая $f(x, y) = 0$ абсолютно неприводима. Докажите, что если на этой кривой найдётся хотя бы одна рациональная точка, то эта кривая рациональна.

---

[1]) Заметим, что при другом выборе точки A на эллипсе окончательные формулы могут оказаться другими, но, разумеется, описываемое ими множество решений останется прежним (ср. с задачей 4).

[2]) Внимание: кривая $x^2+y^2=0$ абсолютно неприводимой не является, так как $x^2+y^2=(x+\sqrt{-1}y)(x-\sqrt{-1}y)$.

Теорема Лежандра

Рассмотрим такую задачу. Пусть a, b, c — натуральные числа. Как искать решения в рациональных числах уравнения

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

Вы, наверное, догадались: надо поступать так же, как и раньше, но сперва надо найти хотя бы одну рациональную точку на кривой, заданной уравнением $ax^2 + by^2 = c$.

Таким образом, возникает вопрос: когда уравнение $ax^2 + by^2 = c$ имеет рациональное решение? Ответить на него не так просто, как может показаться. Например, при $a = b = 1$ возникает такая задача:

7*. Когда натуральное число c является суммой квадратов двух рациональных чисел?

Эта задача очень сложная. Советуем вам повременить с её решением и ознакомиться сначала с понятием *квадратичного вычета*.

Рассмотрим теперь общий случай. Мы можем считать, что числа a, b, c взаимно просты (иначе разделим их на общий делитель) и *свободны от квадратов*, т. е. не делятся на квадраты целых чисел (если, скажем, a делится на m^2, сделаем замену переменных $x' = mx$).

8*. Пусть a, b, c — взаимно простые целые числа, свободные от квадратов. Если уравнение $ax^2 + by^2 = c$ имеет решение в рациональных числах, то существуют целые числа m, n, k, такие что $m^2 + ab$ делится на c, $n^2 - ac$ делится на b и $k^2 - bc$ делится на a.

Итак, остатки от деления чисел $(-ab)$ на c, ac на b, bc на a не могут быть произвольными.

* * *

К в а д р а т и ч н ы е в ы ч е т ы. Остатки, которые получаются при делении квадратов целых чисел на некоторое число M, называются *квадратичными вычетами по модулю M*, а остальные остатки называются *квадратичными невычетами по модулю M*. Например, 2 является квадратичным вычетом по модулю 7, а 3 является квадратичным невычетом по модулю 7 (докажите это!). Также говорят, что целое число N является квадратичным вычетом (невычетом) по модулю M, если остаток от деления N на M является соответственно квадратичным вычетом (невычетом) по модулю M. Например, 8 — квадратичный вычет по модулю 7, а 10 — невычет по модулю 7.

9. Найдите все квадратичные вычеты и невычеты по модулям а) 7, б) 17, в) 24, г) 30.

10. Пусть p — нечётное простое число. Докажите, что из p возможных остатков при делении на p ровно $(p+1)/2$ являются квадратичными вычетами и ровно $(p-1)/2$ являются квадратичными невычетами.

11*. Пусть $M = p_1 \cdot \ldots \cdot p_n$ — произведение различных простых сомножителей. Найдите число квадратичных вычетов и невычетов по модулю M.

12*. Пусть p — нечётное простое число. Остаток $p-1$ является квадратичным вычетом по модулю p тогда и только тогда, когда p при делении на 4 даёт остаток 1.

* * *

Итак, для того чтобы уравнение $ax^2 + by^2 = c$, где a, b, c — взаимно простые натуральные числа, свободные от квадратов, имело рациональное решение, необходимо, чтобы число $(-ab)$ было квадратичным вычетом по модулю c, число ac было квадратичным вычетом по модулю b и число bc было квадратичным вычетом по модулю a. Оказывается, что перечисленные условия достаточны:

Теорема Лежандра. Уравнение $ax^2 + by^2 = c$, где a, b, c — натуральные числа, имеет рациональное решение тогда и только тогда, когда число $(-ab)$ является квадратичным вычетом по модулю c, число ac — квадратичным вычетом по модулю b, а число bc — квадратичным вычетом по модулю a.

13. Разрешимы ли в рациональных числах уравнения
а) $3x^2 + 5y^2 = 7$; б) $5x^2 + 7y^2 = 3$?

14. Давайте докажем теорему Лежандра. Пусть a, b, c удовлетворяют условиям этой теоремы.

а) Покажите, что в формулировке теоремы Лежандра достаточно предполагать, что числа a, b, c попарно взаимно просты.

б) Пусть p — простое число, делящее abc. Покажите, что существуют линейные функции с целыми коэффициентами $L_p = \lambda_1(p)x + \lambda_2(p)y + \lambda_3(p)z$ и $M_p = \mu_1(p)x + \mu_2(p)y + \mu_3(p)z$ такие, что $ax^2 + by^2 - cz^2 \equiv L_p M_p \pmod{p}$.

в) Покажите, что существуют линейные функции с целыми коэффициентами $L = \lambda_1 x + \lambda_2 y + \lambda_3 z$ и $M = \mu_1 x + \mu_2 y + \mu_3 z$ такие, что $ax^2 + by^2 - cz^2 \equiv LM \pmod{abc}$.

г) Докажите, что существует ненулевое решение сравнения $ax^2 + by^2 - cz^2 \equiv 0 \pmod{abc}$ такое, что $-\sqrt{bc} < x < \sqrt{bc}$, $-\sqrt{ac} < y < \sqrt{ac}$, $-\sqrt{ab} < z < \sqrt{ab}$.

д) Пусть (x_0, y_0, z_0) — решение сравнения из п. г). Докажите, что либо $ax_0^2 + by_0^2 - cz_0^2 = 0$, либо $ax_0^2 + by_0^2 - cz_0^2 = abc$.

е) Пусть $ax_0^2 + by_0^2 - cz_0^2 = abc$. Докажите, что тогда

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0.$$

ж) Докажите теорему Лежандра.

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

Рассмотрим следующие задачи:

А. Найти все пары натуральных чисел m и n, такие что сумма первых m натуральных чисел равна сумме квадратов первых n натуральных чисел:

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

Б. При каких n сумма квадратов первых n натуральных чисел является квадратом некоторого натурального числа?

В. Какие натуральные числа являются одновременно произведением двух последовательных натуральных чисел и произведением трёх последовательных натуральных чисел?

Г (великая теорема Ферма для показателя 3). Доказать, что уравнение $X^3 + Y^3 = Z^3$ не имеет решений в натуральных числах.

Д. Когда сумма квадрата рационального числа и куба того же самого числа является кубом рационального числа?

Е. Когда сумма квадрата рационального числа и куба того же самого числа является квадратом рационального числа?

Все эти задачи объединяет то, что они сводятся к изучению решений в целых или рациональных числах *кубических* уравнений с двумя переменными.

15. Докажите, что

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

А. Эта задача эквивалентна решению в натуральных числах уравнения $\frac{m(m+1)}{2} = \frac{n(n+1)(2n+1)}{6}$.

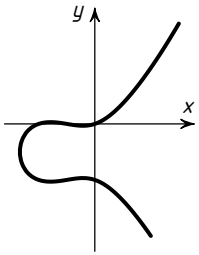
Б. А эта задача эквивалентна решению в натуральных числах уравнения $\frac{n(n+1)(2n+1)}{6} = m^2$.

В. Здесь нужно решить в натуральных числах уравнение $m(m+1) = (n-1)n(n+1)$.

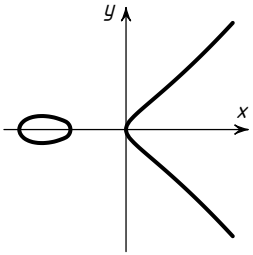
Г. Заменой переменных $x = X/Z$ и $y = Y/Z$ задача сводится к решению в положительных р а ц и о н а л ь н ы х числах уравнения $x^3 + y^3 = 1$.

Д. В этой задаче требуется решить в рациональных числах уравнение $x^2 + x^3 = y^3$.

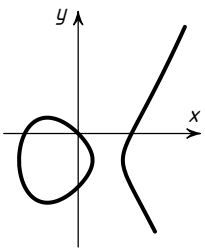
Е. А в этой — уравнение $x^2 + x^3 = y^2$.



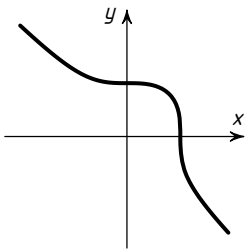
А. $\dfrac{y(y+1)}{2} = \dfrac{x(x+1)(2x+1)}{6}$



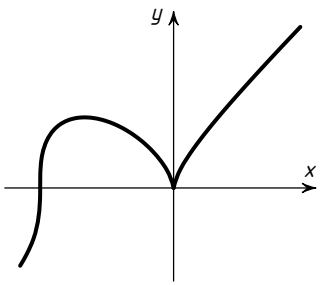
Б. $y^2 = \dfrac{x(x+1)(2x+1)}{6}$



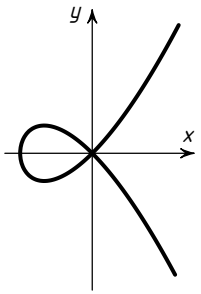
В. $y(y+1) = (x-1)x(x+1)$



Г. $x^3 + y^3 = 1$



Д. $x^2 + x^3 = y^3$



Е. $x^2 + x^3 = y^2$

Рис. 5

Уравнение от двух переменных задаёт некоторую кривую на плоскости. Так как наши кривые задаются уравнениями третьей степени, они являются примерами *кривых третьего порядка* или *кубических кривых* (рис. 5).

Видно, что кривые из задач **Д** и **Е** существенно отличаются от остальных кривых: у первой из них имеется *точка возврата*, а у второй — *точка самопересечения*. Эти точки являются примерами *особых точек*[1]) кривой; кривые, имеющие хотя бы одну особую точку, тоже называются *особыми*. Кривые, не имеющие особых точек, называются *неособыми* или *гладкими* — таковы кривые из задач **А**—**Г**.

16. Какое наибольшее конечное число особых точек может иметь кривая второго порядка? третьего порядка? четвёртого порядка?

17. Может ли кривая четвёртого порядка иметь ровно пять особых точек?

Попробуем применить к нашим кривым метод секущих из предыдущих параграфов. На каждой из наших кривых очень легко найти точки с целыми координатами. Но, к сожалению, проведение секущих в этом случае ничего не даёт: типичная прямая пересекает нашу кривую в трёх точках (а не в двух, как раньше) и рассуждения для кривых второго порядка перестают работать. Тем не менее, всё можно спасти в случае особых кривых.

18. Докажите, что прямая, проходящая через особую точку, может пересекать кривую ещё не более чем в одной точке:
а) для кривых примеров **Д** и **Е**;
б) для произвольной абсолютно неприводимой особой кубической кривой.

Тем самым, проводя секущие через особую точку и применяя те же рассуждения, что и в случае кривых второго порядка, можно решить в рациональных числах кубическое уравнение с рациональными коэффициентами, задающее особую кривую. Заметим, что здесь имеется тонкий момент: для метода секущих необходимо, чтобы начальная точка (в нашем случае — особая точка) имела рациональные координаты.

19. Пусть на абсолютно неприводимой особой кубической кривой, заданной уравнением с рациональными коэффици-

[1]) Дадим точное определение: точка (x_0, y_0) на кривой $F(x, y) = 0$ называется *неособой*, если через неё проходит хотя бы одна прямая

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

такая что $t = 0$ — корень уравнения $F(x_0 + at, y_0 + bt) = 0$ кратности 1, а не больше. В противном случае точка (x_0, y_0) называется *особой*.

ентами, имеется хотя бы одна рациональная точка. Тогда координаты особой точки тоже рациональны.

20*. Приведите пример кубического уравнения с рациональными коэффициентами, задающего особую кривую, все особые точки которой имеют иррациональные координаты.

21. Решите задачи **Д** и **Е**. Докажите, что соответствующие кривые рациональны.

К сожалению, неособая кубическая кривая никогда не является рациональной. Как же поступать с такими кривыми? Первое, что можно сделать, — привести их к более простому виду. Для этого будем использовать *проективные замены координат*, т. е. замены вида

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

Такие замены очень удобны, но у них есть недостаток: они не всюду определены (чему, например, равны x' и y' для точек прямой $\gamma_1 x + \gamma_2 y + \gamma_3 = 0$?). Заметим, однако, что прямая $\gamma_1 x + \gamma_2 y + \gamma_3 = 0$ пересекается с кубической кривой не более чем в трёх точках; если нашей целью является решение кубического уравнения в рациональных (целых, натуральных) числах, мы можем сначала рассмотреть все точки пересечения с этой прямой, а затем делать проективную замену координат.

22. а) При каком условии на коэффициенты α_i, β_i, γ_i, $i = 1, 2, 3$, проективная замена обратима, т. е. переводит разные точки (x, y) в разные точки (x', y')?

б) Пусть проективная замена координат обратима. Тогда обратная замена (т. е. замена, выражающая x и y через x' и y') тоже является проективной заменой координат.

в) Последовательное применение двух обратимых проективных замен эквивалентно некоторой одной такой замене.

В дальнейшем мы будем рассматривать лишь обратимые проективные замены координат.

Кубическая кривая на плоскости (x, y) называется *кривой в форме Вейерштрасса*, если она задаётся уравнением вида $y^2 = x^3 + ax + b$.

23. Кривая в форме Вейерштрасса является особой тогда и только тогда, когда $4a^3 + 27b^2 = 0$.

Число $\Delta = 4a^3 + 27b^2$ называется *дискриминантом* кубической кривой, а также *дискриминантом* кубического многочлена $x^3 + ax + b$. (Дискриминант многочлена обращается в нуль тогда и только тогда, когда многочлен имеет кратный корень.)

24. Когда является особой кривая, заданная уравнением $y^2 = x^3 + ax^2 + bx + c$?

Теорема Ньютона. Для любой неособой кубической кривой существует проективная замена координат, приводящая её в форму Вейерштрасса. Более того, если коэффициенты уравнения исходной кривой рациональны и на кривой имеется хотя бы одна рациональная точка перегиба[1]), то можно найти проективную замену с рациональными α_i, β_i, γ_i $(i=1,\ 2,\ 3)$, преобразующую исходную кривую в кривую в форме Вейерштрасса с рациональными a и b.

25. Докажите эту теорему.

Проиллюстрируем теорему Ньютона на примере задач **А**—**Г**.

А. После замены $m=\frac{y-9}{18}$, $n=\frac{x-3}{6}$ получаем уравнение

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

Б. Замена $m=\frac{y}{72}$, $n=\frac{x-6}{12}$ приводит уравнение к виду

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

В. Замена $m=y-\frac{1}{2}$, $n=x$ приводит уравнение к виду

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

Г. Кривая Ферма $x^3+y^3=1$ — самый интересный случай (рис. 6). Сделаем сначала замену $x=s-t$, $y=t$: получится уравнение $s^3-3st(s-t)=1$. Теперь заменой $s=\frac{1}{3u}$, $t=\frac{6v+1}{6u}$ уравнение приводится к виду

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

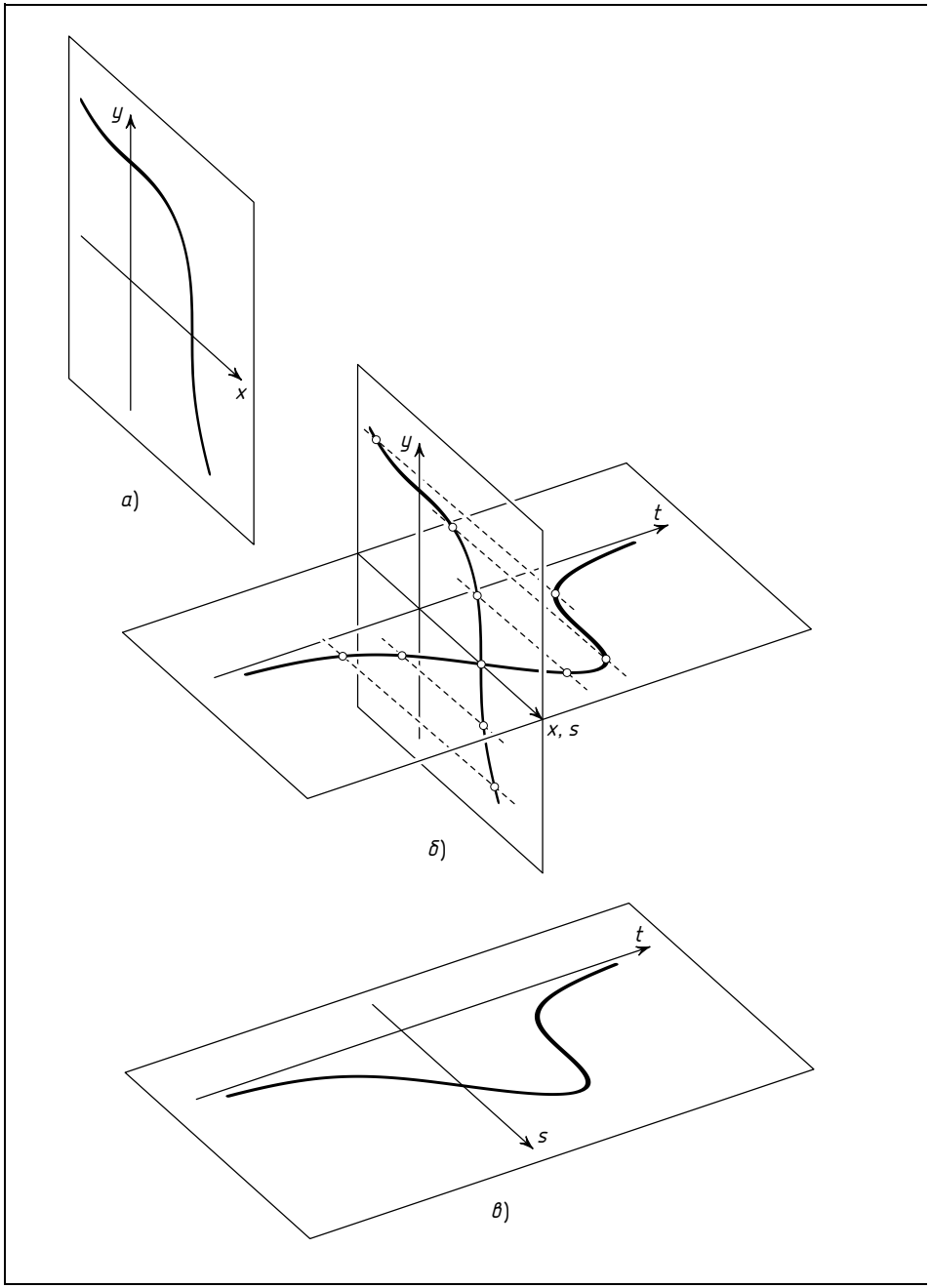
К сожалению, не все кубические кривые, заданные уравнениями с рациональными коэффициентами, имеют рациональную точку перегиба.

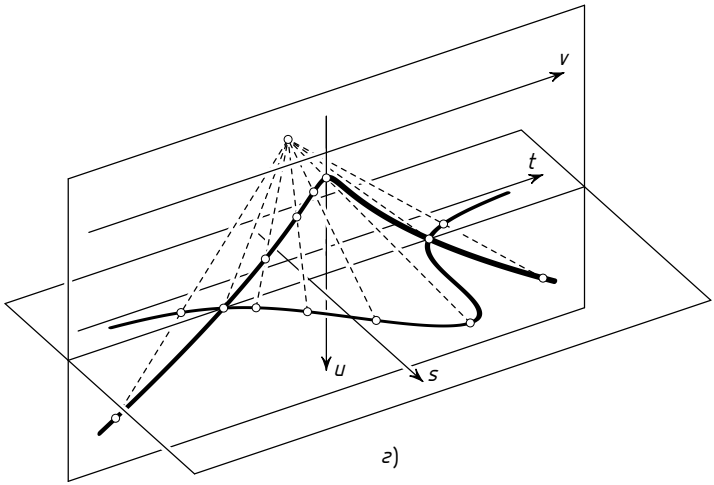
26. Проверьте, что на кривых $x^3+2y^3=4$ и $x^3+2y^3=7$ вообще нет рациональных точек.

Но и при наличии на кривой какой-то рациональной точки все точки перегиба могут быть нерациональны.

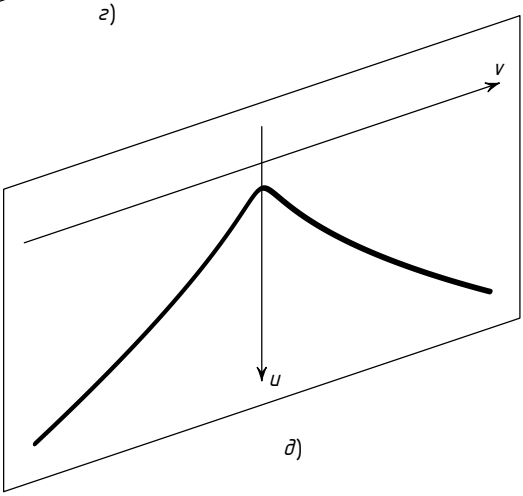
27. Проверьте, что все точки перегиба кривой $x^3+2y^3=3$ нерациональны (заметим, что эта кривая имеет рациональную точку $(1,\ 1)$).

[1]) Напомним, что касательная прямая в точке (x_0, y_0) неособой кривой $F(x, y)=0$ — это прямая $x=x_0+at$, $y=y_0+bt$, такая что $t=0$ является корнем уравнения $F(x_0+at, y_0+bt)=0$, кратность которого не менее 2. Касательная прямая в неособой точке существует и единственна. В случае когда $t=0$ имеет кратность 3 и выше, точка (x_0, y_0) называется *точкой перегиба*.


y
x
а)
y
t
x, s
б)
t
s
в)



г)



д)

Рис. 6. Проективные замены переменных, приводящие кривую $x^3+y^3=1$ к форме Вейерштрасса.

а) Кривая $x^3+y^3=1$. *б*) Замены $x=s-t$, $y=t$ — параллельная проекция плоскости xy на плоскость st. *в*) Кривая $s^3-3s^2t+3st^2=1$. *г*) Замены $s=\dfrac{1}{3u}$, $t=\dfrac{6v+1}{6u}$ — центральная проекция плоскости st на плоскость uv. *д*) Кривая $v^2=u^3-\dfrac{1}{108}$ (в форме Вейерштрасса).

Итак, теорема Ньютона, вообще говоря, недостаточна для приведения кривой к форме Вейерштрасса. На этот случай имеется

Теорема Нагеля. Если на неособой кубической кривой C_1 имеется рациональная точка, то все остальные рациональные точки на этой кривой находятся во взаимно однозначном соответствии с рациональными точками на некоторой кривой C_2 в форме Вейерштрасса, за исключением, быть может, не более трёх рациональных точек на C_2.

Проиллюстрируем эту теорему на примере кривой $x^3+2y^3=3$.

1) Проведём касательную через рациональную точку $(1, 1)$. Она задаётся уравнением $x+2y=3$ и пересекает кривую ещё в одной точке $(-5, 4)$.

2) Введём новые координаты $X=x+2y-3$, $Y=y-4$ (точка $(-5, 4)$ в новых координатах переместилась в начало координат, а касательная стала осью ординат). Теперь введём переменную $u=Y/X$. В новых координатах кривая имеет вид

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

Пусть f_1, f_2, f_3 обозначают коэффициенты при x, x^2, x^3, соответственно (таким образом, f_1, f_2, f_3 — многочлены от переменной u степеней 3, 2 и 1).

3) После сокращения на x и умножения на $4f_3$ уравнение принимает вид

$$4x^2f_3^2+4xf_3f_2+4f_3f_1=0$$

или, после выделения полного квадрата,

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

Простое вычисление показывает, что

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

(заметим, что произошло чудесное сокращение слагаемых, содержащих u^4). Введём теперь переменную $s_1=2xf_3+f_2$. Наше уравнение уже совсем близко к форме Вейерштрасса:

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

После замены переменной $u=u_1+1$ получаем $s_1^2=-3+72u_1^3$. И наконец, замена $9s_1=s$, $18u_1=t$ даёт нам уравнение в форме Вейерштрасса

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

28. Проверьте, что рациональные точки на кривой $x^3+2y^3=3$, за исключением точки $(1, 1)$, соответствуют рациональным точкам на новой кривой $s^2=t^3-243$. Заметим, что при этом точка $(1, 1)$ становится «бесконечно удалённой»

точкой на новой кривой; так как уравнение $f_3 = 0$ не имеет рациональных корней, множество исключительных точек из теоремы Нагеля пусто. Какая точка соответствует точке $(-5, 4)$?

29*. Докажите, что описанный метод позволяет привести к форме Вейерштрасса любую неособую кривую с рациональной точкой, не обязательно являющейся точкой перегиба. (Мы рекомендуем вернуться к этой задаче после прочтения следующего параграфа.)

Неособая кривая третьего порядка называется *эллиптической кривой*. В задачах теории чисел естественно оказывается рассматривать эллиптические кривые, заданные уравнением с рациональными коэффициентами и имеющие рациональную точку, что мы и делаем в дальнейшем (такие кривые обычно называются эллиптическими кривыми над полем рациональных чисел).

Как мы только что объяснили, такую кривую можно некоторой заменой координат с рациональными коэффициентами привести к форме Вейерштрасса.

30. Если дискриминант $\Delta = 4a^3 + 27b^2$ кривой $y^2 = x^3 + ax + b$ равен нулю, то эта кривая рациональна.

Верно и обратное: если $\Delta \neq 0$, то кривая $y^2 = x^3 + ax + b$ не является рациональной, но это уже сложная теорема.

31*. Когда можно перевести кривую с уравнением $y^2 = x^3 + a_1x + b_1$ в кривую с уравнением $y^2 = x^3 + a_2x + b_2$ проективной заменой координат?

Сложение точек эллиптической кривой

Итак, задачи **А**—**В** эквивалентны нахождению всех точек с целыми координатами на эллиптических кривых, в то время как в задаче **Г** требуется найти все точки с *рациональными* координатами на эллиптической кривой.

Оказывается, для произвольной эллиптической кривой задача нахождения рациональных точек в некотором смысле проще, чем задача нахождения целых точек на этой же кривой! Дело в том, что метод секущих позволяет ввести на множестве рациональных точек эллиптической кривой некоторую структуру. А именно, рациональные точки на эллиптической кривой можно «размножать».

Допустим, что мы нашли на эллиптической кривой $y^2 = x^3 + ax + b$ две рациональные точки $P(x_P, y_P)$ и $Q(x_Q, y_Q)$ (рис. 7). Проведём, как и раньше, прямую PQ и вычислим координаты третьей точки пересечения прямой с нашей

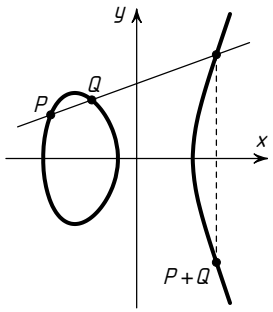


Рис. 7

кривой[1]). Эти координаты удовлетворяют системе уравнений

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

Если $x_P \neq x_Q$ и $y_P \neq y_Q$, то, выразив из второго уравнения x через y, подставим полученное выражение в первое уравнение. В результате мы приходим к кубическому уравнению на y с рациональными коэффициентами. Поскольку два корня этого уравнения рациональны (они равны y_P и y_Q), а сумма всех трёх корней — рациональное число (по теореме Виета), значит, третий корень тоже рационален[2]). Итак, по двум рациональным точкам, лежащим на эллиптической кривой, мы построили третью рациональную точку. Ещё одна рациональная точка получается из построенной точки симметрией относительно оси Ox. Эта симметричная точка называется *суммой* точек P и Q и обозначается $P+Q$ (см. рис. 7).

Замечательно, что введённое нами сложение точек эллиптической кривой обладает свойствами сложения чисел, а именно:

а) коммутативностью (для любых точек P и Q эллиптической кривой выполняется тождество $P+Q=Q+P$);

б) наличием нуля (такой точки $\mathbf{0}$, что $P+\mathbf{0}=P=\mathbf{0}+P$ для любой точки P эллиптической кривой);

в) наличием для любой точки P эллиптической кривой противоположной точки (такой точки $-P$, что $P+(-P)=\mathbf{0}=(-P)+P$);

г) ассоциативностью (для любых точек P, Q и R эллиптической кривой выполняется тождество $(P+Q)+R=P+(Q+R)$).

Проверим эти свойства. К о м м у т а т и в н о с т ь. Для вычисления точки $Q+P$ мы используем ту же самую прямую, что и для вычисления $P+Q$, следовательно, $P+Q=Q+P$.

Н а л и ч и е н у л я и п р о т и в о п о л о ж н о й т о ч к и. Пусть на кривой дана точка P (рис. 8). Мы хотим найти такую точку, что если провести прямую через неё и точку P, пересечь эту прямую с кривой, а потом отразить точку пере-

[1]) Вообще говоря, не всякая прямая пересекает нашу кривую ровно в трёх точках. В некоторых случаях (рис. 12, *а*—*г*) прямая пересекает кривую менее чем в трёх точках. Бороться с этими ситуациями нужно разными способами — но об этом чуть позже.

[2]) Если $y_P=y_Q$, $x_P\neq x_Q$, то уравнение прямой PQ имеет вид $y=y_P$ и, подставив $y=y_P$ в первое уравнение, мы получим кубическое уравнение на x с рациональными коэффициентами. Так что в этом случае тоже всё в порядке.

сечения относительно оси Ox, то вновь получится P. Обозначим через Q точку, симметричную P относительно оси Ox. Из сказанного вытекает, что прямая должна проходить через точки P и Q, т. е. быть вертикальной. Следовательно, точка $\mathbf{0}$ должна лежать и на кривой, и на любой вертикальной прямой, пересекающей кривую.

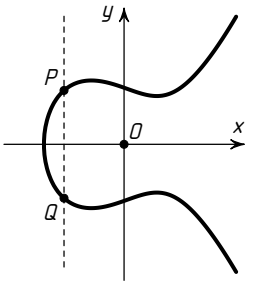


Рис. 8

Такой точки в плоскости нет. Но она нам очень нужна, поэтому мы добавим её к плоскости, назовём *бесконечно удалённой точкой* и обозначим символом ∞. Будем считать, что ∞ есть точка пересечения в с е х вертикалей. Тем самым, хотя точку $\mathbf{0}=\infty$ мы добавили формально, мы знаем, что прямая, проходящая через ∞ и любую точку Q — это вертикальная прямая, проходящая через Q[1]). Правильно считать точку $\mathbf{0}$ рациональной.

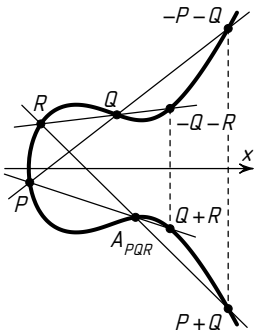


Рис. 9

Вертикальная прямая, проходящая через точку P, проходит и через $\mathbf{0}=\infty$. Поэтому Q, точка пересечения этой прямой с эллиптической кривой, удовлетворяет соотношению $P+Q=\mathbf{0}$, т. е. является противоположной к P. Значит, любая точка P имеет противоположную точку $Q=-P$, симметричную P относительно оси Ox (см. рис. 8). Заметим, что для точек P, лежащих на оси абсцисс, $-P=P$.

А с с о ц и а т и в н о с т ь. Отметим на эллиптической кривой точки P, Q, R (рис. 9). Построим точки $-P-Q$ и $-R-Q$ пересечения прямых PQ и RQ с кривой, а также точки $P+Q$ и $Q+R$. Чтобы доказать равенство $(P+Q)+R=P+(Q+R)$, достаточно показать, что точка пересечения прямой, проходящей через точки $P+Q$ и R, с прямой, проходящей через P и $Q+R$, лежит на кривой.

Возникшая конфигурация шести прямых l_1, l_2, l_3, m_1, m_2, m_3 (проходящих, соответственно, через точки Q и R, $-P-Q$ и $P+Q$, P и $Q+R$, P и Q, $-R-Q$ и $Q+R$, R и $P+Q$) схематично изображена на рис. 10. Каждая из перечисленных прямых проходит через три точки (прямые, проходящие через $-R-Q$ и $Q+R$, $-P-Q$ и $P+Q$, проходят через точку

[1]) Теперь мы уже знаем, как поступать в ситуации, показанной на рис. 12, *а*. Вертикальная прямая имеет с кривой три общие точки: P, Q, ∞.

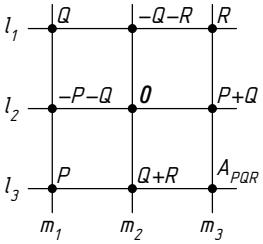


Рис. 10

$\mathbf{0}=\infty$), всего девять точек. Нам известно, что восемь из этих девяти точек лежат на эллиптической кривой E с уравнением $F(x, y)=0$. А доказываем мы, что и девятая точка A_{PQR} лежит на этой кривой. Пусть уравнения прямых l_1, l_2, l_3, m_1, m_2, m_3 суть

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

Покажем, что

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

где α и β — некоторые числа. Рассмотрим разность

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

Эта разность является многочленом от x и y степени не выше третьей. Этот многочлен равен нулю в точках P, $-P-Q$ и Q. Выберем на прямой m_1 ещё одну точку $S=(s_1, s_2)$, отличную от P, $-P-Q$ и Q. Точка S не лежит ни на одной из прямых l_1, l_2, l_3 и, следовательно, $L_1(s_1, s_2)\neq 0$, $L_2(s_1, s_2)\neq 0$, $L_3(s_1, s_2)\neq 0$, а $M_1(s_1, s_2)=0$. Подставим координаты точки S в разность (7) и найдём α из уравнения

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

При таком выборе α разность (7) обращается в нуль в четырёх точках P, Q, $-P-Q$ и S прямой m_1.

32. Пусть многочлен $F_1(x, y)$ степени не выше третьей обращается в нуль в четырёх точках некоторой прямой $M(x, y)=0$. Тогда многочлен F_1 делится на многочлен M.

Итак, мы выбрали параметр α так, что разность (7) делится на M_1. Рассмотрев точки Q, $-Q-R$ и R прямой l_1, аналогично подберём параметр β так, чтобы разность (7) делилась на L_1. Получаем, что разность (7) представляется в виде $L_1(x, y)M_1(x, y)N(x, y)$, где $N(x, y)$ — многочлен степени не выше единицы. Если эта степень равна единице, то уравнение $N(x, y)=0$ задаёт некоторую прямую n.

Итак, $F-(\alpha L_1 L_2 L_3+\beta M_1 M_2 M_3)=L_1 M_1 N$. Подставим в это равенство координаты точки $P+Q$. В левой части получится нуль. Если ни L_1, ни M_1 в нуль не обращаются, то $N=0$, а это означает, что точка $P+Q$ лежит на прямой n. Аналогично заключаем, что точка $Q+R$ лежит на n. Если бы ∞ была обычной точкой, то мы точно так же получили бы, что и она лежит на n.

33. Пусть прямые l_1 и m_1 не являются вертикальными. Докажите, что тогда прямая n вертикальна.

Очевидно, что в общем случае из того, что прямые l_1 и m_1 не вертикальны, не следует, что прямая, проходящая через точки $P+Q$ и $Q+R$, вертикальна. Поэтому многочлен N имеет степень нуль, т. е. является константой. Но многочлен N обращается в нуль в точке $P+Q$, следовательно, он тождественно равен нулю. Таким образом,

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

и точка A_{PQR}, координаты которой определяются из системы уравнений

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

лежит на кривой $F(x, y)=0$.

Тем самым мы доказали ассоциативность сложения точек при некоторых дополнительных предположениях: никакие точки на рис. 10 не совпадают; прямые l_1 и m_1 не проходят через точку $P+Q$; прямая, проходящая через точки $P+Q$ и $Q+R$, а также прямые l_1 и m_1 не вертикальны. Каждый из оставшихся случаев можно рассмотреть отдельно, но можно поступить иначе: заметим, что координаты точек $(P+Q)+R$ и $P+(Q+R)$ зависят от координат точек P, Q, R непрерывно. Мы доказали, что $(P+Q)+R=P+(Q+R)$ для всех достаточно общих наборов точек P, Q, R. Отсюда по непрерывности получаем, что это равенство выполнено всегда (разумеется, чтобы сделать последнее рассуждение строгим, мы должны точно определить все используемые в нём понятия: «непрерывность», «достаточно общие наборы», но мы привели здесь лишь идею доказательства).

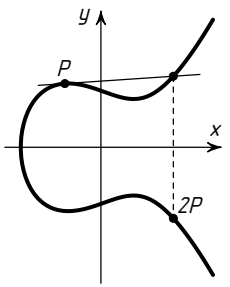


Рис. 11

* * *

Как вычислить точку $P+P=2P$? Когда точки были различны, мы проводили через них прямую и т. д. Раз они слились, понятно, что нужно провести касательную (рис. 11). А что делать, чтобы найти $3P$? Очень просто, берём сумму $2P$ и P. Подобно этому можно вычислить $4P=3P+P$, $5P=4P+P$ и т. д.

34. Пусть $P=(x_0, y_0)$ — точка на кривой $y^2=x^3+ax+b$. Вычислите координаты точки $2P$.

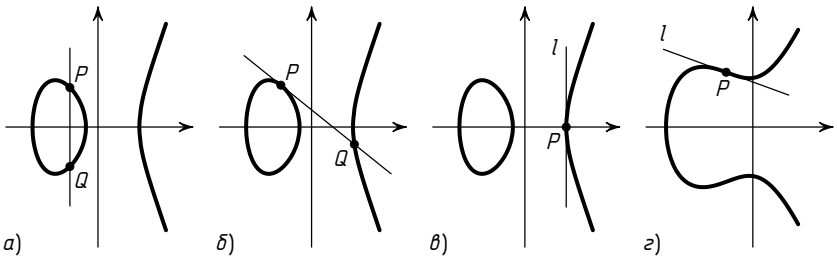


Рис. 12

Настало время объяснить, что делать в ситуациях, показанных на рис. 12, *б*—*г* (см. сноски на стр. 22 и 23). В ситуации *г*, т. е. когда касание происходит в точке перегиба, мы считаем, что прямая l тоже имеет три точки пересечения с кривой, просто эти точки слились. В ситуациях с «простым» касанием (*б*, *в*) точка P учитывается дважды, при этом в ситуации *в* прямая l проходит ещё и через точку ∞.

Тем самым любая прямая, проходящая хотя бы через одну точку эллиптической кривой, не равную ∞, пересекает кривую в трёх точках. Сумма этих трёх точек всегда равна $\mathbf{0}$ (проверьте!).

С учётом этих замечаний определена сумма л ю б ы х двух точек эллиптической кривой. Осталось проверить, что и теперь сложение обладает свойствами а)—г) сложения, см. стр. 22.

Кручение и ранг

Пусть P — некоторая точка на эллиптической кривой. По ней можно построить новые точки . . ., $-3P$, $-2P$, $-P$, P, $2P$, $3P$, ... Если точка P рациональна, то все эти точки тоже являются рациональными. Возможны две «модели поведения» точки P: либо все полученные точки различны, либо среди них есть совпадающие. В последнем случае пусть, например, $mP = nP$, $m > n$. Согласно правилам сложения немедленно получаем, что $(m-n)P = \mathbf{0}$, т. е. существует натуральное число k_1, такое что $k_1 P = \mathbf{0}$. Пусть k — наименьшее такое натуральное число. Число k называется *порядком* точки P, а P называется *точкой кручения* (или *точкой конечного порядка*). Заметим, что согласно этому определению точка $\mathbf{0}$ является точкой кручения порядка 1. В случае первой «модели поведения» говорят, что порядок точки P равен бесконечности.

35. Пусть P — точка порядка k. Докажите, что среди точек . . ., $-3P$, $-2P$, $-P$, $\mathbf{0}$, P, $2P$, $3P$, . . . ровно k различных.

36. Докажите, что сумма двух точек кручения снова является точкой конечного порядка.

37. Пусть P — точка порядка k. Чему равен порядок точки nP, где n — целое число?

38. Найдите все точки порядка 2 на эллиптической кривой $y^2 = x^3 + ax + b$. В каком случае эти точки рациональны? Найдите точки порядка 2 на эллиптических кривых из задач **А**—**Г**.

39. Найдите все точки порядка 3 на эллиптических кривых из задач **А**—**Г**.

40*. Каким геометрическим свойством обладают точки порядка 3 эллиптической кривой? Каким может быть число точек порядка 3 (не обязательно рациональных) на эллиптической кривой?

Замечательно, что любая эллиптическая кривая всегда содержит только конечное число рациональных точек кручения (попробуйте это доказать! — авторам неизвестно простое решение). Более того, как доказал Барри Мазур, для числа t рациональных точек конечного порядка на эллиптической кривой имеются лишь следующие возможности: $1 \leqslant t \leqslant 10$, $t = 12$ или $t = 16$.

Посмотрим теперь, как могут себя вести две точки P и Q бесконечного порядка. Здесь тоже возможны две «модели поведения»: либо все точки $mP + nQ$, m, $n \in \mathbb{Z}$, различны, либо найдутся совпадающие. В первом случае говорят, что точки P и Q *линейно независимы* (а во втором — что они *линейно зависимы*). Это определение можно обобщить: скажем, что точки P_1, P_2, . . ., P_n линейно независимы, если все точки $m_1P_1 + m_2P_2 + \ldots + m_nP_n$ (m_1, m_2, . . ., $m_n \in \mathbb{Z}$) различны. Замечательная теорема Морделла утверждает, что для любой эллиптической кривой существует неотрицательное целое число n, такое что любые $n+1$ рациональных точек этой кривой линейно зависимы. Наименьшее такое число n называется *рангом* эллиптической кривой.

41. Эллиптическая кривая имеет бесконечно много рациональных точек тогда и только тогда, когда её ранг n больше нуля.

Теорема Морделла. Пусть E — эллиптическая кривая. Тогда существует набор рациональных точек P_1, P_2, . . ., P_n, такой что любая рациональная точка кривой E представляется в виде

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

где a_1, . . ., a_n — целые числа, однозначно определённые точкой P, а Q — некоторая рациональная точка кручения.

Иными словами, все рациональные точки на эллиптической кривой получаются из конечного числа таких точек с помощью проведения секущих и касательных.

Ранг кривой E равен наименьшему возможному значению n из теоремы Морделла.

Посмотрим на наши примеры с точки зрения кручения и ранга[1]).

А. Кривая $y^2 = x^3 - 9x + 81$ не имеет кручения (т. е. точка $\mathbf{0}$ — единственная рациональная точка кручения на этой кривой). Её ранг равен 2. В качестве точек P_1, P_2 из теоремы Морделла можно взять точки $(-3, 9)$ и $(0, 9)$.

Б. Кривая $y^2 = x^3 - 36x$ имеет ровно четыре рациональные точки кручения: точку $\mathbf{0}$ и ещё три точки второго порядка. Её ранг равен 1, и в качестве P_1 можно взять точку $(-2, 8)$.

В. Кривая $y^2 = x^3 - x + \frac{1}{4}$ не имеет кручения. Её ранг равен 1, в качестве P_1 можно взять точку $(0, 1/2)$.

Г. Кривая Ферма $y^2 = x^3 - \frac{1}{108}$ имеет ровно три рациональные точки кручения: $\mathbf{0}$ и две точки порядка 3, а её ранг равен 0. Разумеется, это утверждение эквивалентно великой теореме Ферма для показателя 3.

Д. Кривая $s^2 = t^3 - 243$ не имеет кручения. Её ранг равен 1; в качестве P_1 можно взять точку $(10, 7)$.

Чтобы показать читателю, насколько глубоко мы проникли в дебри трудной теории чисел, заметим, что ответа на следующий вопрос человечество ещё не знает.

Проблема ранга. Может ли ранг эллиптической кривой быть сколь угодно велик?

Сейчас известны кривые ранга до 24. Ожидается, что ответ положительный.

Целые точки на эллиптических кривых

Даже предполагая известными результаты предыдущего параграфа, мы всё ещё не можем сказать, что решили наши исходные задачи **А**—**В**. В каждом из этих случаев мы нашли бесконечно много рациональных решений, но в исходных задачах нам нужны были *целые* решения. Как выделить их из бесконечного числа рациональных точек? В той же статье, где была доказана теорема из предыдущего параграфа, Луис Джоэл Морделл доказал, что любая эллиптическая кривая содержит лишь конечное число целых точек. Однако его теорема не помогает *найти* эти точки.

Кривая $y^2 + y = x^3 - x$ из задачи **В** распадается на два куска: овал и бесконечную дугу (рис. 13). Точка $P_1 = (0, 0)$

[1]) Мы должны признать, что нахождение точек кручения и вычисление ранга для наших кривых — задачи трудные и неэлементарные.

лежит на овале. Все целые решения можно найти, решив задачу 42.

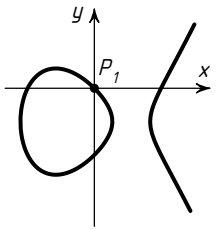


Рис. 13

42. а) Найдите все целые точки, лежащие на овале.

б) Докажите, что точки nP_1 при нечётных n лежат на овале, а при чётных n — на дуге.

в) Проверьте, что если простое число p делит знаменатели обеих координат точки nP_1, то p делит знаменатели координат точки $2nP_1$ (предполагается, что все координаты представлены в виде несократимых дробей).

г) Найдите все целые точки на кривой $y^2 + y = x^3 - x$.

43. Найдите все целые точки на кривой $y^2 = x^3 - 36x$ и решите задачу **Б**.

Как видно, нам очень помогло то обстоятельство, что кривая состоит из двух кусков. Для кривой из задачи **А** это неверно. Тем не менее здесь можно показать, что все целые точки кривой имеют вид $aP_1 + bP_2$, где $|a|$, $|b| \leqslant 13$, и затем решить задачу с помощью конечного перебора (доступного компьютеру, но недоступного авторам). Ответ: целые точки имеют абсциссы -5, -3, 0, 3, 7, 9, 24, 33, 39, 513, 1099, 5112. А отсюда можно найти и все пары (m, n): (1, 1), (10, 5), (13, 6), (645, 85). Первые три из них можно обнаружить, пытаясь решить нашу задачу простым перебором; однако добраться до четвёртой пары без помощи компьютера — вряд ли доступное человеку вычисление.

Ещё более замечательным примером такого рода является кривая $y^2 = x^3 + 24$. Немного поразмышляв, можно придумать «небольшие» решения

$$\begin{aligned} P_1 &= (-2, 4), & 4^2 &= (-2)^3 + 24, \\ P_2 &= (1, 5), & 5^2 &= 1^3 + 24, \\ P_3 &= (10, 32), & 32^2 &= 10^3 + 24. \end{aligned}$$

На первый взгляд, других решений (с $y > 0$) нет. Однако есть ещё четвёртое решение $P_4 = P_1 + 2P_2 = (8158, 736\,844)$.

Заметим, что $P_3 = P_1 - P_2$ и что ранг этой кривой равен 2; более того, любая рациональная точка P кривой $y^2 = x^3 + 24$ может быть представлена в виде $P = aP_1 + bP_2$, где a и b — целые числа.

КОНГРУЭНТНЫЕ ЧИСЛА

Вернёмся к самому первому примеру в книжке. Пусть рациональные числа X, Y, Z — длины сторон прямоугольного треугольника. Несмотря на то, что формулы (3′—4′) были

выведены нами для целых решений уравнения $X^2 + Y^2 = Z^2$, они годятся и для всех рациональных решений, надо только числу r разрешить принимать любые рациональные значения.

Назовём рациональное число s *конгруэнтным*, если существует прямоугольный треугольник площади s с рациональными длинами сторон.

Возникает естественный вопрос: как выяснить, является ли данное число конгруэнтным? Задача описания всех конгруэнтных чисел приводит к глубоким и содержательным теоремам и гипотезам алгебраической геометрии. Мы как бы уже знаем ответ, но ещё не умеем его полностью обосновывать. Однако про некоторые числа известно (и доказано), что они конгруэнтные, а про некоторые — что они не конгруэнтные.

Например, площадь египетского треугольника (со сторонами 3, 4, 5) равна $\frac{1}{2} \cdot 3 \cdot 4 = 6$, так что 6 — конгруэнтное число. Чуть сложнее показать, что число 5 является конгруэнтным. Проверьте, что площадь прямоугольного треугольника со сторонами $3/2$, $20/3$, $41/6$ равна 5.

44* (Эйлер). Докажите, что число 7 тоже является конгруэнтным.

Заметим теперь, что если число s конгруэнтное, то и число sl^2 конгруэнтное при любом рациональном l, поскольку треугольник площади sl^2 получается из треугольника площади s увеличением всех сторон в l раз. Так как $\frac{m}{n} = mn \cdot \frac{1}{n^2}$, в дальнейшем нам достаточно рассматривать целые числа. По той же причине будем рассматривать только числа, свободные от квадратов.

Теорема Ферма. Число 1 не конгруэнтно.

Доказательство. Допустим, что число 1 конгруэнтно. Это означает, что существует прямоугольный треугольник с целыми длинами сторон a, b, x (x — длина гипотенузы), площадь которого равна $\frac{1}{2}ab = y^2$, y — целое число (ясно, что можно выбрать a и b так, чтобы только одно из них было чётным). Преобразуем выражение $x^4 - 16y^4$:

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

Итак, если 1 — конгруэнтное число, то уравнение $x^4 - (2y)^4 = u^2$ имеет решение в натуральных числах (число u нечётно). Выберем среди всех ненулевых решений с нечётным u

такое решение (x_0, y_0, u_0), для которого $|u|$ минимально. Числа x_0, y_0 и u_0 попарно взаимно просты: если бы какие-нибудь два из них имели общий простой делитель p, то и третье число делилось бы на p (причём число u_0 делилось бы даже на p^2), а для решения $\left(\frac{x_0}{p}, \frac{y_0}{p}, \frac{u_0}{p^2}\right)$ значение $|u|$ меньше.

Применяя формулы (4) к равенству $x_0^4 = (2y_0)^4 + u_0^2$, получаем

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

(в нашем случае числа x_0^2, $(2y_0)^2$ и u_0 попарно взаимно просты и $(2y_0)^2$ чётно), где m и n — взаимно простые числа, одно из которых (будем считать, что n) чётно. Из равенства $(2y_0)^2 = 2mn$ следует, что $m = m_1^2$, $n = 2n_1^2$. Из равенства $x_0^2 = m^2 + n^2$ следует, что

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

где m_2 и n_2 — также взаимно простые числа, одно из которых чётно, причём из последнего равенства ясно, что n_2 чётно. Получаем:

$$m_2 = m_3^2, \quad n_2 = n_3^2 \quad \text{и} \quad m_3^4 - n_3^4 = m_1^2.$$

И так как n_3 чётно, $(m_3, n_3/2, m_1)$ — решение уравнения $x^4 - (2y)^4 = u^2$ в целых числах со значением $|u|$ меньшим, чем $|u_0|$:

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

и $|m_1| \leqslant \sqrt{\frac{|u_0|+1}{2}} < |u_0|$ при $|u_0| > 1$. Случай $|u_0| = 1$ тривиален.

Теорема доказана.

Применённый метод доказательства называется *методом бесконечного спуска* и помогает решить многие задачи теории чисел.

45 (великая теорема Ферма для показателя 4). Уравнение $x^4 + y^4 = z^4$ не имеет решений в натуральных числах.

Конгруэнтные числа и эллиптические кривые

Замечательно, что задача о конгруэнтных числах эквивалентна вопросу о ранге некоторых эллиптических кривых. Пусть s — конгруэнтное число, т. е. s — площадь прямоугольного треугольника с рациональными катетами a и b и гипотенузой c, $c^2 = a^2 + b^2$, $s = \frac{1}{2}ab$ (считаем s целым числом, свободным от квадратов). Сопоставим числу s эллиптическую

кривую E_s, заданную уравнением

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

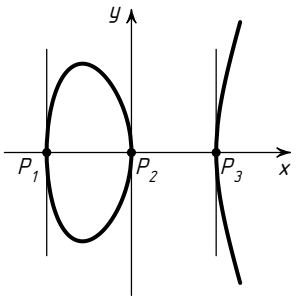


Рис. 14

Подставим в это уравнение $x = \left(\frac{c}{2}\right)^2$:

$$y^2 = \left(\left(\frac{c}{2}\right)^2 - \frac{ab}{2}\right)\left(\frac{c}{2}\right)^2\left(\left(\frac{c}{2}\right)^2 + \frac{ab}{2}\right) =$$

$$= \frac{c^2-2ab}{4}\cdot\left(\frac{c}{2}\right)^2\cdot\frac{c^2+2ab}{4} = \left(\frac{a-b}{2}\right)^2\left(\frac{c}{2}\right)^2\left(\frac{a+b}{2}\right)^2.$$

Таким образом,

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

— рациональная точка.

Также на кривой E_s лежат точки $P_1 = (-s, 0)$, $P_2 = (0, 0)$, $P_3 = (s, 0)$. Эти три точки суть точки порядка 2, так как касательные к кривой E_s в этих точках вертикальны (рис. 14).

Оказывается, верна следующая

Теорема I. На кривой E_s имеется ровно четыре рациональные точки конечного порядка: точка **0** и три точки порядка 2.

Эта теорема весьма сложна. В её доказательстве, приведённом в приложении 1, мы используем арифметику остатков по модулю p и важную теорему Дирихле о простых числах в арифметической прогрессии, которую мы не доказываем.

Заметим, что кривая E_6 совпадает с кривой из задачи **Б**. Так что заодно мы вычислили кручение и на этой кривой.

Из теоремы I следует, что найденная нами точка P имеет бесконечный порядок. Более того, верна

Теорема II. Число s конгруэнтно тогда и только тогда, когда на кривой E_s имеется рациональная точка бесконечного порядка.

Доказательство. Мы уже знаем, что если s конгруэнтно, то кривая E_s содержит рациональную точку P бесконечного порядка. Однако эта точка весьма специальна: её координата x является квадратом рационального числа. Так что для доказательства теоремы II мы должны научится по произвольной точке Q бесконечного порядка строить прямоугольный треугольник с площадью s. Сначала будем действовать «в обратную сторону»: построим по прямоугольному треугольнику с катетами a, b, гипотенузой c и пло-

щадью s ещё одну точку на кривой E_s. Как мы показали ранее, существует рациональное число t, такое что

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

Поскольку $s=\frac{ab}{2}$, то $\frac{s}{c^2}=\frac{ab}{2c^2}=\frac{t(1-t^2)}{(1+t^2)^2}$. Следовательно,

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

и рациональная точка $Q=\left(-st, \frac{s^2(1+t^2)}{c}\right)$ лежит на кривой E_s.

По теореме I эта точка имеет бесконечный порядок, так как её ордината не равна нулю.

Наоборот, пусть $Q=(x, y)$ — рациональная точка бесконечного порядка. Тогда $y\neq 0$ (иначе Q — одна из точек порядка 2), откуда $x\neq 0$, $x\neq -s$. Положим

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

46. Построенные числа a, b, c положительны, рациональны и удовлетворяют уравнениям $a^2+b^2=c^2$, $\frac{1}{2}ab=s$.

Теорема II доказана.

* * *

Интересно выяснить, как связаны точки P и Q. Ответ даёт следующая задача.

47. Докажите, что $2Q=-P$.

Заметим, что из теоремы II и теоремы Ферма, доказанной в предыдущем параграфе, следует, что ранг кривой E_1 (заданной уравнением $y^2=x^3-x$) равен 0.

Конгруэнтные числа: ответ

Задача о конгруэнтных числах была известна ещё древним грекам, однако ответ на неё удалось сформулировать лишь в XX веке. А именно, примерно двадцать лет назад был найден удивительный критерий для выяснения вопроса о конгруэнтности произвольного числа.

Критерий Таннелла. Нечётное натуральное число n, свободное от квадратов, конгруэнтно тогда и только тогда, когда количество решений в целых числах уравнения

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

равно половине количества решений в целых числах уравнения

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

Чётное натуральное число n, свободное от квадратов, конгруэнтно тогда и только тогда, когда количество решений в целых числах уравнения

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

равно половине количества решений в целых числах уравнения

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

Заметим, что для заданного n число решений каждого из этих уравнений находится очень просто, например перебором.

Рассмотрим несколько примеров. При $n = 1$ оба соответствующих уравнения имеют по два решения $(0, -1, 0)$. Следовательно, число 1 не является конгруэнтным. При $n = 2$ оба соответствующих уравнения тоже имеют по два решения, значит, и число 2 не является конгруэнтным. Число $n = 34$ ведёт себя по-другому. Уравнение $17 = 4x^2 + y^2 + 32z^2$ имеет четыре решения $(\pm 2, \pm 1, 0)$, а уравнение $17 = 4x^2 + y^2 + 8z^2$ — восемь решений $(0, \pm 3, \pm 1)$ и $(\pm 2, \pm 1, 0)$. В этом случае критерий Таннелла утверждает, что прямоугольный треугольник с площадью 34 существует. И это действительно верно: длины сторон одного из таких треугольников равны $\frac{136}{15}$, $\frac{15}{2}$ и $\frac{353}{30}$.

К сожалению, критерий Таннелла не доказан полностью. Сегодня мы знаем лишь, что если число n конгруэнтно, то выполнены соответствующие утверждения о количествах решений. Обратное утверждение вытекает из некоторой общей гипотезы об эллиптических кривых — гипотезы Бёрча и Свиннертон-Дайера. Эта гипотеза связывает ранг эллиптической кривой с количеством её точек по модулю p для всевозможных простых чисел p. (Вычисления показывают, что если $n \leqslant 10\,000$ и n удовлетворяет критерию Таннелла, то оно и вправду конгруэнтно.) Чтобы оценить силу гипотезы Бёрча и Свиннертон-Дайера (и следующей из неё недоказанной части критерия Таннелла), рассмотрим пример.

48. Проверьте, что число 157 удовлетворяет критерию Таннелла.

Итак, мы можем предполагать, что число 157 конгруэнтно. Это действительно так, однако длина гипотенузы самого простого прямоугольного треугольника с такой площадью выражается дробью с сорокавосьмизначным числителем (рис. 15)!

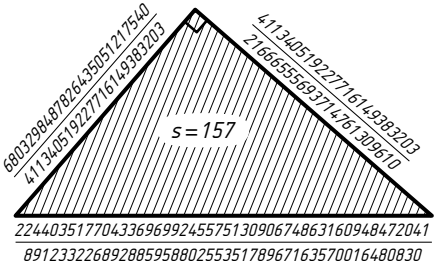


Рис. 15

49. Докажите, что все свободные от квадратов натуральные числа, дающие остатки 5, 6 или 7 при делении на 8, удовлетворяют критерию Таннелла.

Напротив, доказано, что простые числа, дающие остаток 3 при делении на 8, не удовлетворяют критерию Таннелла и, следовательно, конгруэнтными быть не могут.

50*. Разбейте числа от 1 до 100 на не удовлетворяющие критерию Таннелла (и, следовательно, не конгруэнтные) и удовлетворяющие (т. е. гипотетически конгруэнтные). Для последних попробуйте найти соответствующие треугольники.

ПРИЛОЖЕНИЕ 1
ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ I

Допустим, что на кривой E_s имеются другие рациональные точки конечного порядка, кроме $\mathbf{0}$, P_1, P_2, P_3.

51. В этом случае на E_s найдётся либо рациональная точка нечётного простого порядка r, либо рациональная точка порядка 4.

52. Точки порядка 3 и 4 на кривых E_s имеют иррациональные координаты.

Итак, мы можем предполагать, что на кривой E_s имеется точка P нечётного простого порядка $r \neq 3$.

Выберем теперь простое число p, такое что знаменатели координат точки P и число s не делятся на p. Рассмотрим конечное множество $\widetilde{E}_s(p)$ пар (x, y) остатков при делении на p, таких что $y^2 - x^3 + s^2x$ делится на p. Добавим к множеству $\widetilde{E}_s(p)$ точку $\mathbf{0}$ и обозначим $E_s(p) = \widetilde{E}_s(p) \cup \{\mathbf{0}\}$. Решающее наблюдение состоит в том, что на множестве $E_s(p)$ тоже имеется операция сложения. Дело в том, что операция сложения рациональных точек на кривой E_s задаётся некоторыми алгебраическими формулами, выражающими координаты суммы точек через координаты слагаемых. Мы эти формулы не

выписывали, они довольно сложны; для нас сейчас важно лишь то, что эти формулы существуют. Эти же самые формулы имеют смысл и для арифметики остатков по модулю p: в этой арифметике мы тоже умеем складывать, вычитать, умножать и делить! Свойства сложения — коммутативность, ассоциативность — сводятся к некоторым алгебраическим тождествам и поэтому сохраняются и для сложения точек «по модулю p». Итак, на множестве $E_s(p)$ имеется сложение, которое обладает всеми свойствами обычного сложения. Относительно этого сложения все элементы $E_s(p)$ являются точками кручения, так как само множество $E_s(p)$ конечно. Заметим, что эта конструкция не работает в случае, когда s делится на p, по той же причине, по которой нет сложения на особых кривых третьей степени: мешает «особая точка» $(0, 0)$.

Рассмотрим точку P «по модулю p»: заменим числители и знаменатели её координат их остатками по модулю p и выполним деление в арифметике остатков по модулю p. Получим элемент $\overline{P}$ множества $E_s(p)$. Заметим, что $r\overline{P} = \mathbf{0}$. Действительно, тот факт, что $rP = \mathbf{0}$ на кривой E_s, выражается некоторым алгебраическим тождеством, связывающим координаты точки P. Очевидно, то же самое тождество удовлетворяется по модулю p и координатами точки $\overline{P}$. А в силу нашего определения сложения на множестве $E_s(p)$ это и означает, что $r\overline{P} = \mathbf{0}$.

|| **53.** Порядок точки $\overline{P}$ равен r.

Итак, мы построили множество $E_s(p)$ с операцией сложения[1]) и принадлежащую ему точку $\overline{P}$ порядка r. Следующее важное наблюдение состоит в том, что количество элементов множества $E_s(p)$ делится на r. Действительно, разобьём множество $E_s(p)$ на классы эквивалентности следующим образом: скажем, что точки Q_1, $Q_2 \in E_s(p)$ эквивалентны, если $Q_1 - Q_2 = m\overline{P}$ для некоторого целого числа m.

|| **54.** Проверьте, что если Q_1 эквивалентна Q_2, а Q_2 эквивалентна Q_3, то Q_1 эквивалентна Q_3 и Q_2 эквивалентна Q_1.

|| **55.** Каждый класс эквивалентности содержит ровно r элементов $E_s(p)$.

Если q — количество классов эквивалентности, то количество элементов $E_s(p)$ равно qr и, в частности, делится на r. Чтобы прийти к противоречию, желательно научиться вычислять число элементов $E_s(p)$. Оказывается, для «примерно половины» простых чисел это легко сделать.

[1]) Множество $E_s(p)$ с операцией сложения является примером *конечной абелевой группы*. *Абелевой группой* называется множество с операцией сложения, удовлетворяющей свойствам сложения а)—г), см. стр. 22.

56*. Пусть p даёт остаток 3 при делении на 4. Тогда количество элементов в $E_s(p)$ равно $p+1$.

Итак, мы показали, что число r должно делить все числа $p+1$, где p — простое число вида $4k+3$, не делящее s и знаменателей координат точки p. Это уже мало правдоподобно, так как имеется бесконечно много простых чисел вида $4k+3$ и было бы удивительно, если бы все эти числа, кроме конечного числа, после прибавления 1 делились на одно и то же простое число. Однако для того, чтобы дать строгое доказательство невозможности такого явления, нужно использовать замечательную теорему Дирихле.

Теорема Дирихле. Каждая арифметическая прогрессия с целыми взаимно простыми начальным членом и разностью содержит бесконечно много простых чисел.

57. Докажите, что существуют бесконечно много простых чисел вида а) $4k+3$, б) $6k+5$, в)* $4k+1$, г)* $6k+1$.

В частности, поскольку $r \neq 3$, имеется бесконечное число простых чисел вида $p = 4rk+3$, k — целое число. Но $p+1 = 4rk+4$, очевидно, не делится на r. Это противоречие доказывает теорему I.

ПРИЛОЖЕНИЕ 2
ВЕЛИКАЯ ТЕОРЕМА ФЕРМА И ПРОБЛЕМА ЭЙЛЕРА

В начале этой книжки мы описали все натуральные решения уравнения $X^2+Y^2=Z^2$. Эту задачу решили ещё математики глубокой древности. В XVII веке Пьер Ферма предположил, что у уравнения

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

при $n \geqslant 3$ натуральных решений нет[1]). Более того, ему казалось, что он умеет это доказывать. В течение более чем трёх веков многие учёные пытались доказать это утверждение, называемое великой теоремой Ферма. Эти попытки оказались исключительно плодотворными, благодаря им возникла бóльшая часть современной теории чисел. Но теорема Ферма продолжала держать оборону. Крепость пала под дружными ударами многих замечательных математиков всего мира. Совсем недавно великая теорема Ферма была окончательно доказана

[1]) Теорема Ферма для показателя 3 была сформулирована ещё арабским математиком аль-Худжанди в X веке, веком позже Омар Хайям отмечал, что доказать её не удаётся.

Эндрю Уайлсом. Доказательство использует очень-очень глубокую теорию тех же эллиптических кривых.

Начинается оно примерно так: пусть $A^n + B^n = C^n$; построим эллиптическую кривую

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

Далее изучаются свойства этой кривой, и они оказываются столь поразительными, что таких кривых не существует.

Великий математик XVIII века Леонард Эйлер первым доказал отсутствие натуральных решений у уравнения $X^3 + Y^3 = Z^3$ (задача о трёх кубах) и предположил, что уравнения $X^4 + Y^4 + Z^4 = T^4$, $X^5 + Y^5 + Z^5 + U^5 = V^5$ и т. д. также не имеют натуральных решений (задачи о четырёх четвёртых степенях, пяти пятых степенях и т. д.). Эта проблема стойко противостояла усилиям математиков вплоть до появления вычислительных машин. На заре компьютерной техники был найден контрпример для пятых степеней:

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

Задача о четвёртых степенях оказалась много труднее. Победа была одержана с помощью умелой комбинации методов теории рациональных и эллиптических кривых с компьютерными вычислениями. Ноум Элкис нашёл контрпример

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

Вскоре на более мощных компьютерах был найден другой, меньший контрпример:

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

Идея состоит в том, чтобы до рассмотрения поверхности F с уравнением $x^4 + y^4 + z^4 = 1$ рассмотреть более простую поверхность F': $x^4 + y^4 + t^2 = 1$. Если на F имеется рациональная точка (x, y, z), то на F' есть рациональная точка (x, y, t), где $t = z^2$. Поверхность F' удаётся представить в виде объединения рациональных кривых, т. е. плоских кривых второго порядка. Делается это так: рассмотрим поверхность F'', заданную уравнением

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

При фиксированном u получается рациональная кривая F''_u. Замена $x = w + v$, $y = w - v$, $t = u(x^2 + xy + y^2 + x + y) + 1 - (x + y)^2$ переводит поверхность F' в поверхность F''. Теорема Лежандра (в слегка изменённом виде она верна и для любой неособой рациональной кривой второго порядка) даёт нам необходимое и достаточное условие существования рациональной точки на кривой F''_u. Возьмём теперь кривую C', имеющую рацио-

нальную точку. Прообраз C кривой C' на поверхности F оказывается эллиптической кривой. На ней и надо искать точки. Проверяем разрешимость уравнения кривой C в остатках при делении на небольшие простые числа. И только если для всех таких простых чисел решения есть, ищем рациональное решение на компьютере. Это значительно уменьшает перебор.

Интересно, что на самом деле рациональных решений уравнения $x^4+y^4+z^4=1$ очень много: сколь угодно близко к любому вещественному решению имеется какое-то рациональное.

ПРИЛОЖЕНИЕ 3
ПИФАГОРОВ КИРПИЧ

Задачу о пифагоровых треугольниках можно сформулировать чуть иначе. Назовём прямоугольник *пифагоровым*, если длины его сторон X и Y, а также длина его диагонали Z — целые числа (рис. 16).

В такой формулировке задача имеет естественное обобщение. Назовём *пифагоровым кирпичом* прямоугольный параллелепипед, такой что его рёбра X, Y, Z, диагонали граней U, V, W и главная диагональ T — целые числа (рис. 17). Если T не обязательно целое, скажем, что это слабо пифагоров кирпич.

Вот пример слабо пифагорова кирпича: $X=44$, $Y=117$, $Z=240$, при этом получается $U=125$, $V=244$, $W=267$.

Существует ли хотя бы один пифагоров кирпич? Как описать все слабо пифагоровы кирпичи? Ответы человечеству не известны.

58. Сформулируйте эти задачи на языке уравнений. Какой геометрический объект соответствует этим уравнениям?

59. Опишите все параллелепипеды с целыми X, Y, Z и T.

60 (Эйлер). Проверьте, что для любого натурального $n\geqslant 2$ кирпич со сторонами

$$X=n^6-15n^4+15n^2-1,\quad Y=6n^5-20n^3+6n,\quad Z=8n^5-8n$$

слабо пифагоров.

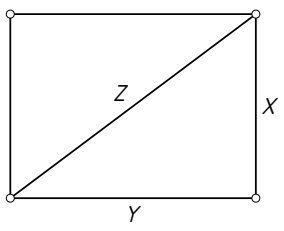


Рис. 16

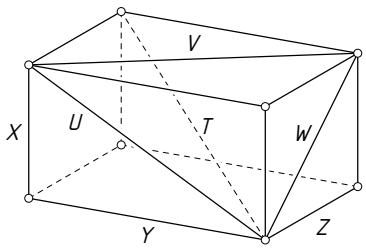


Рис. 17

ПРИЛОЖЕНИЕ 4
КАК ДИОФАНТ РЕШАЛ АРИФМЕТИЧЕСКИЕ ЗАДАЧИ

Мы привыкли решать задачи, используя уравнения, в которых переменные обозначены буквами, а арифметические операции — знаками. Надо, однако, помнить, что современные обозначения появились не так давно, в XVI—XVII веках. Древние же математики использовали только слова. Вот как Диофант описывает решение уравнения $x^3 + ax^2 = y^2$ (в правой колонке сказано то же самое с использованием чисел и букв):

«Найти кубическое число, такое что если к нему прибавить сколько-то раз взятый квадрат с его стороной, то получится некоторое квадратное число.

Найти (целые) решения уравнения

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

Предположим, что куб имеет стороной одну вещь, т. е. имеется некоторый один куб; предположим, что число раз есть десять, и прибавим к этому кубу десять раз квадрат стороны куба, что есть некоторый квадрат, т. е. имеется куб плюс десять квадратов, равный квадрату. Предположим, что этот квадрат имеет стороной вещь, квадрат которой больше десяти квадратов, чтобы сделать уменьшение возможным. Предположим, что его сторона есть четыре вещи, квадрат есть шестнадцать квадратов. Куб прибавить десять квадратов равно тогда шестнадцати квадратам. Отнимем десять общих квадратов, останется шесть квадратов, которые равны кубу. Поделим это на квадрат, получим одну вещь, равную шести единицам. Куб есть двести шестнадцать, квадрат его стороны есть тридцать шесть; десять раз это последнее есть триста шестьдесят. Добавляя их к кубу, получаем пятьсот семьдесят шесть, квадрат, сторона которого равна двадцати четырём.

Возьмём, к примеру $a = 10$.

Чтобы $x^3 > 0$, необходимо $y^2 > 10x^2$.

Возьмём $y = 4x$, тогда $y^2 = 16x^2$.

Получим $6x^2 = x^3$.

Находим $x = 6$.

Действительно,

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

Таким образом, мы нашли кубическое число, такое что если к нему добавить десять раз квадрат его стороны, то получится в результате сложения квадратное число; это есть двести шестнадцать, т. е. сторона его есть шесть. Что и требовалось найти».

Теперь попробуем восстановить общий метод, которым пользуется Диофант и которому он пытается обучить читателя.

Положим $y = tx$, где t — целое число. Уравнение перепишется так: $x^3 + ax^2 = t^2x^2$, т. е. $x + a = t^2$, $x = t^2 - a$, $y = t^3 - at$ для любого t (Диофант потребовал бы ещё $x > 0$, $y > 0$, т. е. $t^2 > a$).

Насколько мы знаем, Диофант не понимал, что уравнение задаёт кривую, на которой нужно найти целые точки. Для этого требуется понятие координат, появившееся впервые у Декарта в XVII веке. Однако мы сразу узнаём проведение прямых через особую точку $(0, 0)$ кривой $y^2 = x^3 + ax^2$.

ОТВЕТЫ, УКАЗАНИЯ, РЕШЕНИЯ

3. Ответ:

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

5. Ответ: а) $X = (15m^2 + n^2)r$, $Y = 2mnr$, $Z = (15m^2 - n^2)r$; б) $X = 9mnr$, $Y = 9(9n^2 - m^2)r$, $Z = m^2r$, в пунктах а) и б) m и n — целые числа, r — подходящее рациональное (эти формулы — только один из возможных способов записать все решения).

в) Единственным решением с $Z = 0$ является $X = Y = Z = 0$. Пусть теперь $Z \neq 0$. Предположим, что (X, Y, Z) — решение уравнения $X^2 + 3Y^2 = 5Z^2$, причём числа X, Y, Z не имеют общих простых делителей. Рассмотрим уравнение «по модулю 5»: число X^2 при делении на 5 может давать остатки 0, 1 или 4, а число $3Y^2$ — остатки 0, 2 или 3. Следовательно, поскольку $X^2 + 3Y^2$ делится на 5, и X, и Y делятся на 5, откуда Z тоже делится на 5. Получаем противоречие с предположением, что числа X, Y, Z не имеют общих простых делителей.

6. Пусть (x_0, y_0) — рациональная точка на кривой $ax^2 + bxy + cy^2 + dx + ey + f = 0$. Проведём через эту точку прямую с угловым коэффициентом t: $y = tx + (y_0 - tx_0)$. Подставим y в уравнение кривой. Получится уравнение не более чем второй степени $A(t)\,x^2 + B(t)x + C(t) = 0$, коэффициенты которого, как нетрудно видеть, — многочлены от переменной t с рациональными коэффициентами (поскольку x_0, y_0, a, b, c, d, e, f — рациональные числа). Заметим, что ни при каком t_0 числа $A(t)$, $B(t)$ и $C(t)$ не равны нулю одновременно, поскольку это означало бы, что при подстановке $y = t_0x + (y_0 - t_0x_0)$ многочлен $ax^2 + bxy + cy^2 + dx + ey + f$ становится тождественным нулём. Введём новую систему координат, в которой прямая $y = t_0x + (y_0 - t_0x_0)$ задаётся уравнением $y' = 0$. В этой системе уравнение нашей кривой имеет вид $F(x', y') = 0$, F — многочлен степени не выше второй; при этом $F(x', 0) \equiv 0$,

следовательно, $F(x', y')$ делится на y', т. е. $F(x', y') = y'\,G(x', y')$, где $G(x', y')$ — некоторый многочлен. Возвращаясь в прежнюю систему координат, получаем, что многочлен $ax^2 + bxy + cy^2 + dx + ey + f$ делится на многочлен $y - tx - (y_0 - tx_0)$, что противоречит абсолютной неприводимости нашей кривой.

Если $A(t) = a + bt + ct^2 = 0$, то уравнение $A(t)\,x^2 + B(t)\,x + C(t) = 0$ имеет степень 1, но таких значений t не более двух. При прочих t уравнение квадратное. Один корень этого уравнения равен x_0, по теореме Виета другой корень равен $-\dfrac{B(t)}{A(t)} - x_0$. Итак,

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

— искомые рациональные функции с рациональными коэффициентами. Осталось проверить, что хотя бы одна из них непостоянна.

Предположим, что они обе тождественно постоянны,

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

Значит, $t(h_1 - 2x_0) \equiv h_2$, откуда $h_1 = 2x_0$, $-\dfrac{B(t)}{A(t)} = 2x_0$ и $A(t)x^2 + B(t)x + C(t) = A(t)x^2 - 2x_0A(t)x + C(t)$. Число x_0 — всегда корень этого многочлена, значит, $C(t) = x_0^2A(t)$. Пусть t_0 — корень уравнения $A(t) = 0$ (возможно, комплексный). Тогда $A(t_0) = B(t_0) = C(t_0) = 0$, чего, как показано ранее, быть не может. Противоречие.

7. Ответ: тогда и только тогда, когда все нечётные простые числа, входящие в разложение числа c на простые множители в нечётных степенях, дают остаток 1 при делении на 4.

В решении этой задачи используются результаты задач 8 и 10—12.

Можно считать, что c свободно от квадратов. Если $c = x^2 + y^2$, то (см. задачу 8) число -1 должно быть квадратичным вычетом по модулю c. Следовательно, все простые делители c должны иметь вид $4k+1$ (см. задачу 12).

Обратно, пусть все простые делители бесквадратного числа c имеют вид $p = 4k+1$ или $p = 2$ (случай $c = 1$ тривиален). Поскольку из равенств $c_1 = x_1^2 + y_1^2$ и $c_2 = x_2^2 + y_2^2$ следует $c_1c_2 = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2$, достаточно доказать, что любое простое число $p = 4k+1$ представимо в виде суммы двух квадратов рациональных чисел (для $p = 2$ имеем $2 = 1^2 + 1^2$).

Доказательство проведём по индукции. Наше утверждение верно для $p = 5$: имеем $5 = 2^2 + 1^2$; допустим, оно верно для всех простых $p' = 4k' + 1$, $p' < p$. Докажем его для p. Согласно задаче 12 найдётся такое натуральное число m, что $m^2 + 1$ делится на p, т. е. $m^2 + 1 = np$. Если $n = 1$, то всё доказано. В противном случае мы можем считать, что $|m| \leqslant p/2$ (для этого сначала заменим m его остатком от деления на p, а затем, если понадобится, на $p - m$); разумеется, $1 \leqslant p/2$. Тогда $n \leqslant p/2 < p$. Все простые делители np вида $4k+3$ входят в np (а значит, и в n) в чётных степенях. Пусть $n = n_{\text{бескв}} \cdot \tilde{n}^2$, где $n_{\text{бескв}}$ — бесквадратное число. Тогда $n_{\text{бескв}} \leqslant n < p$; все нечётные простые делители p' числа $n_{\text{бескв}}$ меньше p и имеют вид $4k' + 1$. По предположению индукции, они представимы в виде суммы двух квадратов рациональных чисел, следовательно, $n_{\text{бескв}}$ и n тоже представимы. Пусть $n = a^2 + b^2$. Следующее тождество завершает доказательство:

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

Несколько более тонкие рассуждения показывают, что в этом случае c является суммой квадратов двух целых чисел.

10. Пусть x — целое число. Остаток от деления x^2 на p зависит лишь от остатка от деления x на p. Поэтому, чтобы найти все квадратичные вычеты, достаточно найти остатки от деления на p чисел x^2, где $x=0, 1, \ldots, p-1$. Заметим, что числа x^2 и $(p-x)^2$ дают один и тот же остаток при делении на p. Среди чисел $0, 1, \ldots, p-1$ можно выделить $\frac{p-1}{2}$ пар $(x, p-x)$, при этом остаётся число 0. Следовательно, число квадратичных вычетов не больше $\frac{p+1}{2}$. С другой стороны, если x^2 и y^2 дают один и тот же остаток при делении на p, то $x^2-y^2=(x-y)(x+y)$ делится на p, т. е. $x-y$ или $x+y$ делится на p. Это значит, что либо x и y, либо x и $p-y$ дают одинаковые остатки при делении на p. Следовательно, число квадратичных вычетов равно $\frac{p+1}{2}$.

11. Решение этой задачи основывается на следующем утверждении.

Китайская теорема об остатках. Пусть M и N — взаимно простые числа. Для любых чисел x и y существует число z такое, что x и z дают одинаковые остатки при делении на M, а y и z дают одинаковые остатки при делении на N.

Пусть $\tau(N)$ — число остатков по модулю N, являющихся квадратичными вычетами по модулю N. Докажем, что если N_1 и N_2 — взаимно простые числа, то $\tau(N_1N_2)=\tau(N_1)\tau(N_2)$. Для этого построим взаимно однозначное отображение, которое паре

(квадратичный вычет по модулю N_1, квадратичный вычет по модулю N_2)

сопоставляет квадратичный вычет по модулю N_1N_2 (мы сейчас рассматриваем только остатки по каждому из модулей). Пусть $a\equiv u^2 \pmod{N_1}$, $0\leqslant a<N_1$, $b\equiv v^2 \pmod{N_2}$, $0\leqslant b<N_2$. Тогда, по китайской теореме об остатках, найдётся такое целое число z, что $z\equiv a \pmod{N_1}$, $z\equiv b \pmod{N_2}$. Сопоставим паре (a, b) остаток c от деления z на N_1N_2. Этот остаток не зависит от выбора z, так как любые два числа z и z', такие что $z\equiv z'\equiv a \pmod{N_1}$ и $z\equiv z'\equiv b \pmod{N_2}$, отличаются на число, кратное N_1N_2. Это легко следует из взаимной простоты N_1 и N_2. Докажем, что остаток c является квадратичным вычетом по модулю N_1N_2. Действительно, по китайской теореме об остатках, найдётся такое число w, что $w\equiv u \pmod{N_1}$, $w\equiv v \pmod{N_2}$. Тогда $c\equiv w^2 \pmod{N_1}$, $c\equiv w^2 \pmod{N_2}$, а отсюда, в силу взаимной простоты N_1 и N_2, нетрудно получить, что $c\equiv w^2 \pmod{N_1N_2}$. Покажем, что построенное нами отображение является взаимно однозначным.

Действительно, так как по построению $c\equiv a \pmod{N_1}$, $c\equiv b \pmod{N_2}$, разным парам вычетов (a, b) будут соответствовать разные вычеты c. Если же c — квадратичный вычет по модулю N_1N_2, то паре (a, b), где a — остаток от деления c на N_1, b — остаток от деления c на N_2, как раз и будет соответствовать остаток c.

Итак, $\tau(N_1N_2)=\tau(N_1)\tau(N_2)$. Отсюда следует, что $\tau(M)=\tau(p_1)\cdot\ldots\cdot\tau(p_n)$. Мы знаем (см. задачу 10), что для нечётных простых p выполнено $\tau(p)=\frac{p+1}{2}=\left[\frac{p}{2}\right]+1$. Для числа 2 верно такое же равенство $\tau(2)=2=\left[\frac{2}{2}\right]+1$, которое легко проверить. Осталось выписать окончательный ответ: количество квадратичных вычетов по модулю M равно

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

остальные $M-\tau(M)$ остатков являются квадратичными невычетами.

Попробуйте решить эту задачу для произвольного целого числа M.

12. Для решения этой задачи нам потребуется

Малая теорема Ферма. Пусть p — простое число, a — произвольное целое число, не делящееся на p. Тогда $a^{p-1}-1$ делится на p.

Пусть p — нечётное простое число. Из малой теоремы Ферма следует, что тогда либо $a^{(p-1)/2}-1$, либо $a^{(p-1)/2}+1$ делится на p.

Если a — ненулевой квадратичный вычет по модулю p, т. е. остаток от деления a на p равен остатку от деления x^2 на p, то остаток от деления $a^{(p-1)/2}$ на p равен остатку от деления $(x^2)^{(p-1)/2}=x^{p-1}$ на p, т. е. равен 1. Значит, $a^{(p-1)/2}-1$ делится на p. Другими словами, ненулевые квадратичные вычеты являются корнями «уравнения по модулю p» $x^{(p-1)/2}-1=0$. Так как число ненулевых квадратичных вычетов равно $\dfrac{p-1}{2}$, никаких других корней у этого уравнения нет. Следовательно, если a — квадратичный невычет по модулю p, то $a^{(p-1)/2}+1$ делится на p.

Пусть теперь $a=p-1$. Тогда

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

13. Ответ: а) нет; б) да, например, $(1/2,\,1/2)$ — решение.

14. Указания. а) Если a и b делятся на q, то $ax^2+by^2-cz^2=0$ тогда и только тогда, когда $\dfrac{a}{q}(qx)^2+\dfrac{b}{q}(qy)^2-qcz^2=0$.

б) Например, пусть p делит b. Если $n^2\equiv ac \pmod p$ (напомним, что ac является квадратичным вычетом по модулю b, следовательно и по модулю p), то $ax^2-cy^2\equiv a\left(x-\dfrac{n}{a}y\right)\left(x+\dfrac{n}{a}y\right) \pmod p$.

в) Примените китайскую теорему об остатках.

г) Рассмотрим все тройки целых чисел x, y, z такие, что $0\leqslant x<\sqrt{bc}$, $0\leqslant y<\sqrt{ac}$, $0\leqslant z<\sqrt{ab}$. Количество таких троек строго больше, чем abc (за исключением случая $a=b=c=1$). Поэтому найдутся две разные тройки x', y', z' и x'', y'', z'', такие что $L(x',y',z')=L(x'',y'',z'')$. Тогда $(x'-x'',y'-y'',z'-z'')$ будет ненулевым решением сравнения $ax^2+by^2-cz^2\equiv 0 \pmod{abc}$, удовлетворяющим указанным неравенствам.

д) Из неравенств легко находим $-abc<ax^2+by^2-cz^2<2abc$.

16. Пусть прямая пересекает кривую второго порядка в особой точке и ещё в одной точке. Докажем, что тогда уравнение кривой делится на уравнение прямой.

Пусть, к примеру, прямая задаётся уравнением $y=0$, а кривая — уравнением $F(x,y)=0$. Многочлен $F(x,0)$ от переменной x имеет корень кратности 2 в особой точке кривой и ещё один корень. Но это многочлен степени не выше второй. Следовательно, $F(x,0)=0$ при всех x и $F(x,y)$ делится на y.

Из доказанного вспомогательного утверждения получаем, что если кривая $F(x,y)=0$ второго порядка имеет особую точку, то $F(x,y)=l_1(x,y)\times l_2(x,y)$, где l_1 и l_2 — линейные функции.

Итак, кривая второго порядка с особой точкой является объединением двух прямых, а особая точка — это точка пересечения этих прямых. Похожие рассуждения применимы к кривым третьего и четвёртого порядков.

Ответ: на кривой второго порядка не больше одной особой точки, на кривой третьего порядка — не больше трёх, на кривой четвёртого порядка — не больше шести (в последнем случае можно воспользоваться таким фактом: через любые пять точек плоскости проходит кривая второго порядка). Во всех случаях кривая с наибольшим числом особых точек — объединение нескольких прямых.

17. Ответ: да, может. Например, объединение четырёх прямых, две из которых параллельны.

20. Ответ: например, $y^3+3xy^2-x^3-3x^2-3xy-3y^2+3=0$. Проверьте, что это уравнение задаёт объединение трёх прямых, проходящих через точки (x_1, x_2), (x_2, x_3) и (x_3, x_1), где x_1, x_2, x_3 — корни многочлена $x^3-3x+1=0$ (они иррациональны). Особыми точками этой «кривой» являются (x_1, x_2), (x_2, x_3) и (x_3, x_1).

22. а) Ответ: при

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

25. Указание: в качестве γ_i следует взять коэффициенты касательной прямой в точке перегиба.

23. Пусть (x_0, y_0) — особая точка. Для вертикальной прямой $x=x_0$, $y=t$ кратность корня $t=y_0$ уравнения $t^2-x_0^3-ax_0-b=0$ может равняться 2, только если $y_0=0$. В этом случае x_0 — корень уравнения $x^3+ax+b=0$. Рассмотрим теперь прямую $x=x_0+t$, $y=0$. Уравнение $(x_0+t)^3+a(x_0+t)+b=0$ с учётом $x_0^3+ax_0+b=0$ переписывается в виде $t^3+3x_0t^2+(3x_0^2+a)t=0$. Кратность корня $t=0$ должна быть больше 1, поэтому $a=-3x_0^2$. Подставляя $x=x_0$ в уравнение $x^3-3x_0^2x+b=0$, получаем $b=2x_0^3$. Следовательно, $\Delta=4a^3+27b^2=0$.

Обратно, пусть $\Delta=0$. Тогда (это можно доказать, используя теорему Виета) уравнение $x^3+ax+b=0$ имеет кратный корень x_0. Подставим $x=x_0+t$ в это уравнение; $t=0$ является кратным корнем, поэтому $a=-3x_0^2$, тогда $b=2x_0^3$. Покажем, что $(x_0, 0)$ — особая точка кривой $y^2=x^3-3x_0^2x+2x_0^3$. Подставляя в уравнение кривой $x=x_0+ut$, $y=vt$, получаем $v^2t^2=3x_0u^2t^2+u^3t^3$, т. е. $t=0$ — корень кратности не менее 2.

24. Ответ: при $4\left(b-\dfrac{a^2}{3}\right)^3+27\left(c-\dfrac{ab}{3}+\dfrac{2a^3}{27}\right)^2=0$.

31. Ответ: тогда и только тогда, когда $\dfrac{4a_1^3}{4a_1^3+27b_1^2}=\dfrac{4a_2^3}{4a_2^3+27b_2^2}$.

32. Введём новую систему координат, в которой прямая $M(x, y)=0$ будет осью абсцисс и, следовательно, будет задаваться уравнением $y'=0$. В новых переменных многочлен $F_1(x, y)$ примет вид $G(x', y')$ (степень многочлена G, очевидно, тоже не выше третьей). Многочлен $G(x', 0)$ степени не выше третьей имеет четыре различных корня и, значит, тождественно равен нулю. Другими словами, $G(x', y')$ делится на y'. Возвращаясь в старую систему координат, получаем утверждение задачи.

33. Указание: относительно переменной y разность (7) имеет степень не выше второй.

40. Условие $3P=\mathbf{0}$ равносильно $2P=-P$. По определению точки $2P$ это означает, что третья точка пересечения кривой с касательной, проведённой в точке P, совпадает с самой точкой P (см. рис. 12, *г*). Такие точки называются *точками перегиба*. Точки перегиба кривой $y^2=x^3+ax+b$ — это в точности те точки, где обращается в нуль вторая производная функции $y(x)=\sqrt{x^3+ax+b}$.

Эллиптическая кривая в форме Вейерштрасса всегда содержит восемь точек перегиба с комплексными координатами, но только две из них могут иметь вещественные координаты.

41. Пусть ранг кривой больше нуля. Тогда на ней имеется рациональная точка P бесконечного порядка (линейно независимая сама с собой) и, следовательно, имеется бесконечно много рациональных точек $\ldots, -3P, -2P, -P, P, 2P, 3P, \ldots$. Пусть ранг кривой равен нулю. Это означает, что

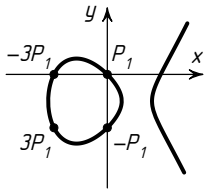


Рис. 18

любая рациональная точка не является линейно независимой, т. е. является точкой конечного порядка. Однако на эллиптической кривой имеется лишь конечное число рациональных точек кручения.

42. а) Ответ: $P_1 = (0, 0)$, $-P_1 = (0, -1)$, $3P_1 = (-1, -1)$, $-3P_1 = (-1, 0)$, рис. 18.

49. Указание: оба уравнения из критерия Таннелла не имеют решений.

50. В табл. 1 возле каждого из чисел от 1 до 100, являющегося бесквадратным, записаны через тире количества решений уравнений из критерия Таннелла, возле чисел, не являющихся бесквадратными, приведены их бесквадратные части. Числа, удовлетворяющие критерию Таннелла (гипотетически конгруэнтные), выделены рубленым шрифтом. В табл. 2 приведены длины сторон соответствующих треугольников.

52. Найдём точки перегиба на кривой $y^2 = x^3 - s^2x$ (эти точки и являются точками порядка 3, см. задачу 40). Для этого продифференцируем два раза её уравнение:

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

Если $y'' = 0$, то $(y')^2 = 3x$. Имеем:

$$\begin{aligned}
4y^2(y')^2 &= (3x^2 - s^2)^2 && \text{(возводим } 2yy' = 3x^2 - s^2 \text{ в квадрат)},\\
4(x^3 - s^2x)\cdot 3x &= (3x^2 - s^2)^2 && \text{(подставляем } y^2 = x^3 - s^2x,\ (y')^2 = 3x),\\
12x^4 - 12s^2x^2 &= 9x^4 - 6x^2s^2 + s^4,\\
3x^4 - 6x^2s^2 - s^4 &= 0.
\end{aligned}$$

Дискриминант этого биквадратного уравнения равен $36s^4 + 12s^4 = 48s^4 = 3(4s^2)^2$. Следовательно, x^2 является иррациональным числом.

Рассмотрим теперь точки порядка 4. Предположим, что $s \neq 1$. Нам понадобится формула для удвоения точки на кривой E_s. А именно, если положить $Q = (x_0, y_0)$ и $2Q = (x_1, y_1)$, то $x_1 = \left(\dfrac{x_0^2 + s^2}{2x_0y_0}\right)^2$. Если R — точка четвёртого порядка, то $2R$ является точкой порядка 2. Следовательно, её абсцисса x_1 равна 0, s или $-s$, а поскольку x_1 положительна, $x_1 = s$. И мы немедленно получаем противоречие с рациональностью точки (x_0, y_0). Случай $s = 1$ читателю предлагается разобрать самостоятельно.

53. Указание: докажите сначала, что порядок точки $\overline{P}$ делит число r.

56. Указание: -1 является квадратичным невычетом по модулю p.

58. Ответ: для пифагорова кирпича

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

для слабо пифагорова кирпича

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

Разделив все переменные на одну из них, например на U, получим систему из четырёх уравнений с шестью переменными (соответственно, из трёх уравнений с пятью переменными). Соответствующие геометрические объекты являются *алгебраическими поверхностями*. Эти поверхности лежат в многомерных пространствах и имеют конечное число особых точек (посчитайте, сколько).

Таблица 1

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

Таблица 2

5	$\frac{3}{2}, \frac{20}{3}, \frac{41}{6}$	37	$\frac{777923}{6090}, \frac{450660}{777923}, \frac{605170417321}{4737551070}$	65	$12, \frac{65}{6}, \frac{97}{6}$
6	3, 4, 5			69	$\frac{437}{104}, \frac{624}{19}, \frac{65425}{1976}$
7	$\frac{24}{5}, \frac{35}{12}, \frac{337}{60}$	38	$\frac{5301}{425}, \frac{1700}{279}, \frac{1646021}{118575}$	70	$15, \frac{28}{3}, \frac{53}{3}$
13	$\frac{780}{323}, \frac{323}{30}, \frac{106921}{9690}$	39	$\frac{312}{10}, \frac{5}{2}, \frac{313}{10}$	71	$\frac{30317}{660}, \frac{1320}{427}, \frac{12974641}{281820}$
14	$\frac{21}{2}, \frac{8}{3}, \frac{65}{6}$	41	$\frac{40}{3}, \frac{123}{20}, \frac{881}{60}$	77	$\frac{525}{848}, \frac{18656}{75}, \frac{15820337}{63600}$
15	$\frac{15}{2}, 4, \frac{17}{2}$	46	$\frac{253}{42}, \frac{168}{11}, \frac{7585}{462}$	78	$45, \frac{52}{15}, \frac{677}{15}$
21	$12, \frac{7}{2}, \frac{25}{2}$	47	$\frac{11547216}{2097655}, \frac{98589785}{5773608}, \frac{21728794487529 7}{12111037689240}$	79	$\frac{335946000}{2950969}, \frac{233126551}{167973000}, \frac{56434050774922081}{495683115837000}$
22	$\frac{140}{3}, \frac{33}{35}, \frac{4901}{105}$				
23	$\frac{41496}{3485}, \frac{80155}{20748}, \frac{905141617}{72306780}$	53	$\frac{1472112483}{202332130}, \frac{21447205780}{1472112483}, \frac{4850493897329785961}{297855654284978790}$	85	$\frac{77}{6}, \frac{1020}{77}, \frac{8521}{462}$
				86	$\frac{2193}{91}, \frac{364}{51}, \frac{116645}{4641}$
29	$\frac{52780}{99}, \frac{99}{910}, \frac{48029801}{90090}$	55	$\frac{117}{10}, \frac{1100}{117}, \frac{17561}{1170}$	87	$\frac{3484}{1925}, \frac{167475}{1742}, \frac{322446497}{3353350}$
30	12, 5, 13	61	$\frac{6428003}{1423110}, \frac{173619420}{6428003}, \frac{250510625883241}{9147755349330}$	93	$\frac{56203}{1330}, \frac{7980}{1813}, \frac{2090761}{49210}$
31	$\frac{8897}{360}, \frac{720}{287}, \frac{2566561}{103320}$			94	$\frac{7728}{2057}, \frac{96679}{1932}, \frac{199428385}{3974124}$
34	$\frac{136}{15}, \frac{15}{2}, \frac{353}{30}$	62	$\frac{84560}{5727}, \frac{177537}{21140}, \frac{2056525601}{121068780}$	95	$\frac{1443}{34}, \frac{6460}{1443}, \frac{2093801}{49062}$

59. Описать все параллелепипеды с целыми X, Y, Z и T — значит описать все целые решения уравнения $X^2 + Y^2 + Z^2 = T^2$. Единственным решением этого уравнения с $T = 0$ является $X = Y = Z = T = 0$. Для всех остальных решений $T \neq 0$ и уравнение можно разделить на T^2. Таким образом, задача сводится к описанию всех рациональных решений уравнения

$$x^2 + y^2 + z^2 = 1,$$

где $x = \frac{X}{T}$, $y = \frac{Y}{T}$, $z = \frac{Z}{T}$. Это уравнение задаёт сферу в трёхмерном пространстве $Oxyz$ (рис. 19). Выберем на ней некоторую рациональную точку, например, $A(0, 0, 1)$. Легко проверить, что любая прямая AB, где $B(x, y, z)$ — ещё одна рациональная точка на сфере, пересекает плоскость Oxy в рациональной точке $C(a, b, 0)$ и, обратно, любая прямая AC пересекает сферу в рациональной точке B. Таким образом, на сфере «столько же» рациональных точек, сколько на плоскости. Числа x, y и z выражаются через a и b так:

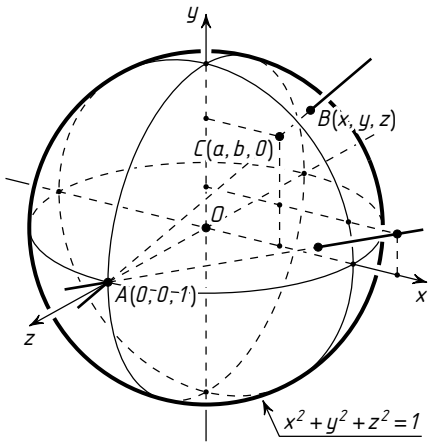


Рис. 19

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

$$z = \frac{a^2 + b^2 - 1}{a^2 + b^2 + 1}.$$

Отсюда, полагая $a = \frac{k}{l}$, $b = \frac{m}{n}$, получаем окончательный ответ:

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

Здесь k, l, m, n — целые числа, r — подходящее рациональное число, т. е. такое, что числа X, Y, Z, T являются целыми.

60. Покажем, что многочлены $X^2 + Y^2$, $Y^2 + Z^2$, $Z^2 + X^2$ являются точными квадратами многочленов с целыми коэффициентами. Тем самым при любом целом значении n числа U, V, W тоже будут целыми. Итак,

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

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

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

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