РАЦИОНАЛЬНЫЕ ТОЧКИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Ю. П. СОЛОВЬЕВ

Московский государственный университет им. М.В. Ломоносова

RATIONAL POINTS ON ELLIPTIC CURVES

Yu. P. SOLOV'EV

The article is devoted to some basic concepts of elliptic curves theory. A tremendous purely mathematical activity is observed in this area with applications varying from cryptography to physics.

Статья посвящена некоторым понятиям теории эллиптических кривых – бурно развивающейся области современной математики с широчайшим диапазоном приложений – от криптографии до математической физики.

Древний мир оставил нам в наследство несколько великих математических сочинений. Пожалуй, самое загадочное из них – это "Арифметика" Диофанта Александрийского в 13 книгах, созданная в середине III века н. э. Удивительна судьба "Арифметики" Диофанта. После пожара Александрийской библиотеки "Арифметика" исчезла более чем на тысячелетие и считалась полностью утраченной. Лишь в 1464 году немецкий ученый Регионтан случайно обнаружил 6 из 13 книг "Арифметики". В первый раз она была напечатана в латинском переводе в 1575 году. После издания 1621 года, подготовленного Баше де Мезириаком, книга стала настольной для многих математиков, например П. Ферма (1601–1665) и Р. Декарта (1596–1650).

За тысячелетие книга совсем не устарела – она сильно опережала уровень лучших алгебраических исследований XVI века. Посудите сами: в отличие от европейских алгебраистов того времени Диофант свободно оперировал отрицательными и рациональными числами, владел буквенной нотацией для уравнений, а самое главное – умел находить решения в целых и рациональных числах линейных, квадратных, кубических уравнений и систем с двумя и более неизвестными с целыми коэффициентами. Решение таких уравнений – они называются *диофантовыми* – с тех пор находится в центре внимания математиков.

В статье речь пойдет о решении некоторых диофантовых уравнений, наиболее красивых и, кроме того, связанных живыми нитями с многими областями математики. Нам придется не только бросить пристальный взгляд на сочинения Диофанта, но и коснуться самых последних событий современной математической жизни.

МЕТОД СЕКУЩИХ ДИОФАНТА

Проиллюстрируем этот метод на конкретном примере – частном случае одного из тех уравнений, которые Диофант разбирает в своей "Арифметике". Пусть дано уравнение

$$x^2 - y^2 = 1 \qquad (1)$$

и требуется найти все его рациональные решения, то есть все пары

$$(x; y) = (a/b; c/d), \qquad a, b, c, d \in \mathbf{Z},$$

обращающие уравнение (1) в числовое тождество.

Уравнение (1), как и любое уравнение от переменных x, y, можно рассматривать как кривую на плоскости Oxy. В данном случае это гипербола (рис. 1). Сразу бросается в глаза решение (1, 0) – точка пересечения P кривой с осью Ox. Проведем через эту точку секущую

$$y = k(x - 1) \qquad (2)$$

и найдем ее вторую точку пересечения с кривой (1). Для этого подставим выражение (2) для y в уравнение (1) и решим получившееся квадратное уравнение относительно x. Получим

$$x_{1,2} = \frac{-k^2 \pm 1}{1 - k^2}.$$

Корень $x_1 = 1$ нам и так известен (он относится к точке (1, 0)), а второй корень $x_2 = (k^2 + 1)/(k^2 - 1)$ дает искомую вторую точку

$$(x_2; y_2) = \left(\frac{k^2 + 1}{k^2 - 1}, \quad \frac{2k}{k^2 - 1}\right). \qquad (3)$$

Для любого рационального k ($k \neq \pm 1$) эта формула определяет точку на нашей кривой, а значит, и рациональное решение данного уравнения. (При $k = \pm 1$ секущая пересекает кривую только в точке P (см. рис. 1).) Обратно, для любого рационального решения, то есть рациональной точки M на кривой, секущая PM задается уравнением (2) с рациональным k (ибо тогда катеты прямоугольного треугольника PMH рациональны).

Таким образом, *формула* (3) *при всевозможных рациональных* $k \neq \pm 1$ *дает все решения в рациональных числах уравнения* (1).

Сам Диофант, конечно, не вводил в рассмотрение систему координат Oxy, не рассматривал кривую данного уравнения – метод координат появился лишь в работах Декарта в XVII веке. Диофант делал подстановку (2) чисто алгебраически и получил, разумеется в другой записи, формулу (3). Более того, он понимал, что продемонстрированный метод с успехом применим не только к многочлену $x^2 - y^2 - 1$, но и вообще к многочлену второй степени от двух переменных общего вида

$$p(x, y) = ax^2 + bxy + cy^2 + dx + ey + f,$$

где $a, b, \ldots, f$ – целые (или рациональные) числа при условии, что у многочлена удалось найти хотя бы один рациональный корень.

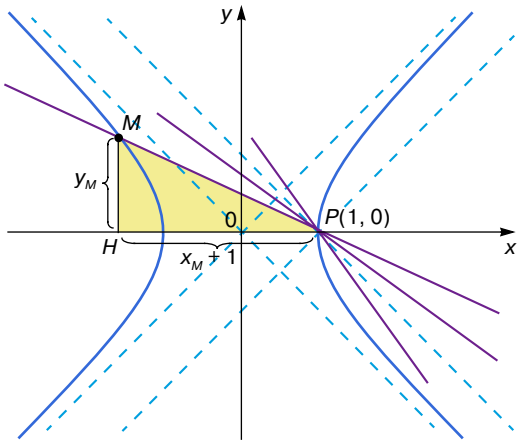

Рис. 1

Не на всякой кривой второй степени имеются рациональные точки, например их нет на окружности $x^2 + y^2 = 3$ или на эллипсе $x^2 + 82y^2 = 3$ [1]. Задача о существовании хотя бы одной рациональной точки на кривой второй степени оказалась очень трудной. Первые нетривиальные продвижения в ее решении получили индийские математики Брахмагупта (VII век) и Бхаскара (XII век), а окончательный ответ был найден лишь в 1768 году французским математиком Ж.-Л. Лагранжем (1736–1813).

Диофант не ограничился уравнениями второй степени. Он с успехом берется и за третью степень, демонстрируя общий прием на одной конкретной задаче.

ОДНА ЗАДАЧА ИЗ “АРИФМЕТИКИ” ДИОФАНТА. КАСАТЕЛЬНАЯ

В этой задаче требуется найти рациональное решение уравнения

$$y(6 - y) = x^3 - x. \qquad (4)$$

Короткое решение, содержащее в зародыше замечательную идею, Диофант излагает с незаурядным мастерством. Попробуем, пишет он, замену $x = 2y - 1$ (разумеется, обозначения у него совсем другие). Тогда получим

$$6y - y^2 = 8y^3 - 12y^2 + 4y.$$

Если бы 6 равнялось 4, как хорошо бы сократились члены с y в первой степени! Но число 4 появилось из двойки при замене $x = 2y - 1$. Так заменим его тройкой, то есть возьмем $x = 3y - 1$. Тогда линейные члены сокращаются и остается

$$y^2(27y - 26) = 0, \qquad (5)$$

откуда $y = 26/27$ и $x = 17/9$. Получено рациональное решение (17/9, 26/27) кубического уравнения (4).

На первый взгляд здесь нет ничего особенного – просто удачная замена $x = 3y - 1$ позволила найти решение. В чем же глубокая идея? Чтобы ответить на этот вопрос, вновь воспользуемся методом координат и построим график кривой (4) [2] (рис. 2). На этом рисунке красным показана прямая $x - 3y + 1 = 0$.

[1] Рациональные точки $(a/b, b/c)$ имеются, однако, на окружности $x^2 + y^2 = 1$. Для таких точек тройка целых чисел (a, b, c) называется пифагоровой – она удовлетворяет соотношению $a^2 + b^2 = c^2$. Все пифагоровы тройки могут быть найдены методом секущих.

[2] О том, как строить графики подобных кривых, мы подробно расскажем ниже.

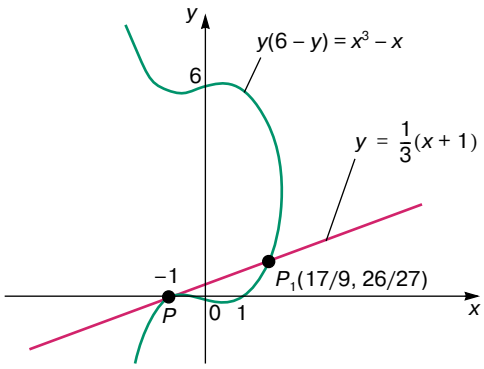

Рис. 2

Она касается нашей кривой в точке $P = (-1, 0)$ (действительно, уравнение (5) имеет кроме корня $y = 26/27$ еще и "два слившихся корня" $y^2 = 0$).

По этому пути можно было бы пойти дальше: через полученную рациональную точку (17/9, 26/27) провести еще одну касательную к кривой (4) до пересечения с ней в третьей рациональной точке и т. д. Но Диофант не сделал этого шага. И потребовалось более 1500 лет, прежде чем математики сумели до конца воспользоваться идеями Диофанта.

КРИВЫЕ ТРЕТЬЕЙ СТЕПЕНИ

Оставаясь верными геометрическому подходу, рассмотренному выше, сосредоточим внимание не на решении уравнений третьей степени, а на следующем эквивалентном вопросе: найти рациональные точки кривой на плоскости, задаваемой уравнением третьей степени

$$f(x, y) = ax^3 + bx^2y + \ldots + hx + iy + j = 0$$

с целыми коэффициентами.

Все такие кривые можно разбить на два больших класса. К первому классу отнесем те кривые, у которых имеются точки заострения (как точка (0, 0) кривой $y^2 = x^3$) или точки самопересечения (рис. 3, *а*), а также кривые, для которых $f(x, y)$ представляется в виде

$$f(x, y) = f_1(x, y) \cdot f_2(x, y),$$

где $f_1(x, y)$, $f_2(x, y)$ – многочлены меньших степеней (рис. 3, *б*). Назовем такие кривые *вырожденными*. Второй класс образуют невырожденные кривые третьей степени с целыми коэффициентами – такие кривые называются *эллиптическими*. Именно этот (наиболее общий) класс и будет нас интересовать. Мы будем рассматривать эллиптические кривые, заданные в *канонической форме*, то есть уравнением

$$y^2 = x^3 + ax^2 + bx + c \qquad (6)$$

с целыми коэффициентами a, b и c, в котором многочлен $P(x) = x^3 + ax^2 + bx + c$ не имеет кратных корней.

Это не нарушает общности: любую неособую кривую $f(u, \upsilon) = 0$ третьей степени можно преобразованием вида $x = r(u, \upsilon)$, $y = s(u, \upsilon)$, где $r(u, \upsilon)$ и $s(u, \upsilon)$ – рациональные функции, привести к виду (6). При этом если коэффициенты многочлена $f(x, y)$ целые, то задачу отыскания рациональных точек на кривой $f(x, y) = 0$ можно свести к аналогичной задаче для кривой (6) с целыми a, b и c.

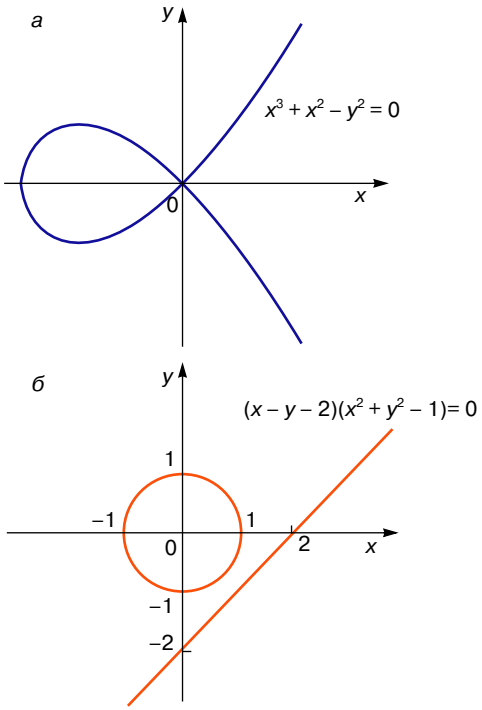

Рис. 3

ГРАФИЧЕСКОЕ ИЗОБРАЖЕНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Выясним, как выглядит кривая (6). Чтобы получить ее графическое изображение, нужно нарисовать график функции $y = \sqrt{x^3 + ax^2 + bx + c}$ и симметрично отразить его относительно оси Ox. Для построения графика $y = \sqrt{x^3 + ax^2 + bx + c}$ построим вначале график функции $y = x^3 + ax^2 + bx + c$. Известно, что у многочлена третьей степени (без кратных корней) может быть либо один, либо три вещественных корня. По предположению, все эти корни различны. Поэтому график $y = x^3 + ax^2 + bx + c$ выглядит так, как показано на рис. 4, *а* и *б*. А теперь уже нетрудно получить график функции $y = \sqrt{x^3 + ax^2 + bx + c}$ (рис. 5, *а*) и тем самым вид эллиптической кривой $y^2 = x^3 + ax^2 + bx + c$ (рис. 5, *б*) для случая кривой, изображенной на рис. 4, *а*. Кривая, изображенная на рис. 4, *б*, исследуется аналогично; результирующая кривая состоит из двух кусков (см. рис. 7, *б*).

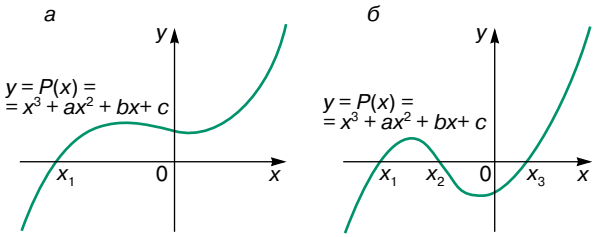

Рис. 4

Отметим следующее обстоятельство. Графики функций $y = \sqrt{P(x)}$ и $y = -\sqrt{P(x)}$ склеиваются в точках x_1, x_2, x_3 гладко, то есть без углов. Это происходит потому, что касательные к графику $y = \sqrt{P(x)}$ в точках x_1, x_2, x_3 вертикальные. Другими словами, их угловой коэффициент обращается в бесконечность. Это легко доказать подсчетом производной функции $y = \sqrt{P(x)}$.

СЛОЖЕНИЕ ТОЧЕК НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Метод секущих, примененный к эллиптической кривой C, приводит к неожиданному результату: оказывается, точки на ней можно складывать. Определим операцию сложения точек на C отправляясь от ее графического изображения (рис. 6). Возьмем на C две точки P и Q и проведем через них прямую. Эта прямая имеет третью точку пересечения с кривой C. Отразим эту точку от оси Ox и назовем получившуюся точку *суммой* точек P и Q (обозначение: $P + Q$, рис. 6). Не всегда прямая, проходящая через две точки, пересекает кривую C в третьей, например с вертикальной прямой этого не происходит. Далее мы более подробно рассмотрим эту ситуацию.

Исследуем свойства операции сложения точек на эллиптической кривой. За образец примем свойства операции сложения чисел. Эта операция *коммутативна,* то есть $a + b = b + a$, и *ассоциативна,* то есть $(a + b) + c = a + (b + c)$. Кроме того, у этой операции существует *нуль*, то есть такое число 0, что $a + 0 = a$ для любого a, и, наконец, для каждого числа a имеется *противоположное* ему, то есть такое число $-a$, что $a + (-a) = 0$.

А как обстоит дело на эллиптической кривой? Прежде всего *операция сложения точек коммутативна.* В самом деле, для вычисления $Q + P$ мы используем ту же самую прямую, что и для $P + Q$, следовательно, $P + Q = Q + P$.

Ассоциативность для сложения точек на эллиптической кривой также выполняется, но геометрически доказать этот факт достаточно трудно. Проще всего ассоциативность можно получить с помощью приводимых ниже формул (8) и (9).

Займемся теперь существованием нуля. Нуль – это такая точка E на кривой, что $P + E = P$. Как ее найти? Посмотрим на рис. 7, *а*. Пусть на кривой дана точка P. Мы хотим найти нечто такое, что если провести прямую через P и это нечто, пересечь получившуюся прямую с кривой, а потом отразить точку пересечения от оси Ox, то вновь получится P. Обозначим буквой R точку, симметричную P относительно оси Ox. Из сказанного вытекает, что прямая должна проходить через точки P и R, то есть должна быть вертикальной. Следовательно, если имеется точка E, для которой $P + E = P$, то эта точка не может находиться в плоскости, поскольку она должна лежать и на кривой, и на любой вертикальной прямой.

Раз точки E в плоскости нет, а она очень нужна, то добавим ее к плоскости (и, разумеется, к кривой) и назовем *бесконечно удаленной точкой*. Каким требованиям она должна удовлетворять? Любая вертикальная прямая стремится к бесконечности сверху и снизу. Потребуем, чтобы все эти точки в

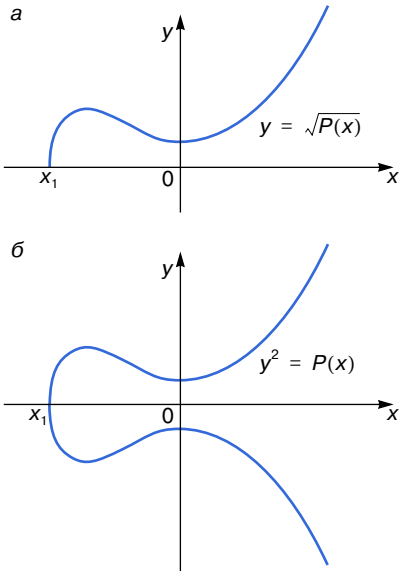

Рис. 5

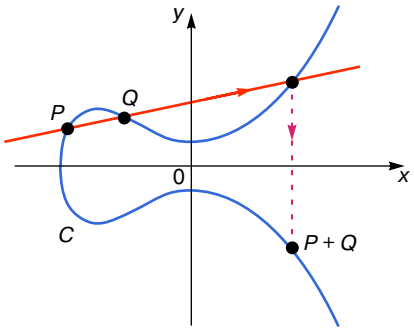

Рис. 6

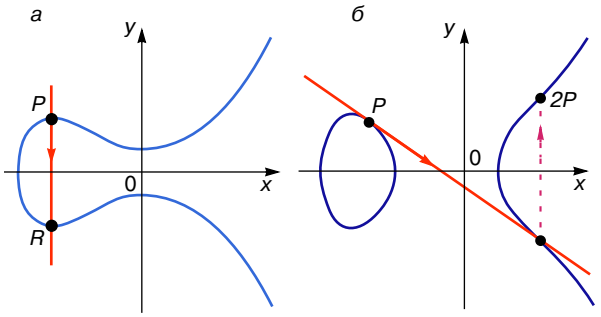

Рис. 7

бесконечности были одной и той же точкой E, то есть будем считать, что *E есть точка пересечения всех вертикалей*. Это требование корректно определяет точку E – нулевую точку относительно нашей операции сложения. В силу нашего соглашения вертикальная прямая, проходящая через точку P, проходит через P и E. Поэтому точка R пересечения этой прямой с эллиптической кривой удовлетворяет соотношению $P + R = E$, то есть является противоположной к P. В то же время R – это точка, симметричная к P относительно оси Ox. Значит, любая точка P имеет противоположную $-P = R$. Тем самым мы убедились, что *сложение точек на эллиптической кривой обладает теми же свойствами, что и сложение чисел*.

Как вычислить точку $P + P$? Когда точки были различны, мы проводили секущую. Раз они слились, понятно, что нужно провести касательную (рис. 7, *б*). А что делать, чтобы найти $3P$? Очень просто, берем сумму $2P$ и P. Подобно этому, $4P = 3P + P$, $5P = 4P + P$ и т. д.

ПОИСК РАЦИОНАЛЬНЫХ ТОЧЕК

Вооружившись операцией сложения, займемся теперь рациональными точками. Пусть $P = (x_1; y_1)$, $Q = (x_2; y_2)$ – две рациональные точки на эллиптической кривой $y^2 = x^3 + ax^2 + bx + c$, где a, b, c – целые числа, и прямая, проходящая через P и Q, пересекает эту кривую еще в одной точке $R = (x_3; y_3)$. Тогда R также является рациональной точкой.

Доказывается это утверждение довольно просто. Если

$$y = kx + d \qquad (7)$$

есть уравнение прямой, проходящей через точки P и Q, то k и d – рациональные числа, поскольку их можно выразить через координаты $(x_1; y_1)$ и $(x_2; y_2)$ точек P и Q по формулам

$$k = \frac{y_1 - y_2}{x_1 - x_2}, \qquad d = y_1 - kx_1 = \frac{x_1y_2 - x_2y_1}{x_1 - x_2}.$$

Подставив (7) в уравнение эллиптической кривой, получим для x уравнение третьей степени с рациональными коэффициентами

$$(kx + d)^2 = x^3 + ax^2 + bx + c,$$

то есть

$$x_3 + (a - k^2)x^2 + (b - 2kd)x + c - d^2 = 0.$$

По теореме Виета

$$x_1 + x_2 + x_3 = k^2 - a.$$

Так как x_1 и x_2 рациональны, то рациональным будет x_3, а значит, и $y_3 = kx_3 + d$.

Из этого доказательства сразу же следует формула для вычисления координат точки $P + Q$. По определению, $P + Q$ получается из R отражением от оси Ox, значит, координаты (u, υ) точки $P + Q$ можно найти по формулам

$$u = k^2 - a - x_1 - x_2, \quad \upsilon = -ku - d = -[k(u - x_1) + y_1].$$

Подставив сюда значение k, получим

$$u = \frac{(y_1 - y_2)^2}{(x_1 - x_2)^2} - (a + x_1 + x_2),$$

$$\upsilon = \frac{y_1 - y_2}{x_1 - x_2}(x_1 - u) - y_1. \qquad (8)$$

Ясно, что, если $x_1 = x_2$, эти формулы не имеют смысла. В этом случае уравнение секущей (7) нужно заменить уравнением касательной и действовать по прежней схеме. В результате получим

$$u = -2x_1 - a + \left(\frac{3x_1^2 + 2ax_1 + b}{2y_1}\right)^2,$$

$$\upsilon = -y_1 - \frac{3x_1^2 + 2ax_1 + b}{2y_1}(u - x_1). \qquad (9)$$

Таким образом, зная хотя бы одну рациональную точку P на эллиптической кривой, мы можем найти по указанным формулам точки $2P$, $3P$ и т.д. Рассмотрим пример. Пусть кривая задана уравнением $y^2 = x^3 - 2$ и $P = (3, 5)$. Тогда $2P = (129/100, -383/1000)$ – новая рациональная точка. Теперь можно вычислить $3P$, $4P$ и т. д. Заметим, что объем вычислений с каждым шагом стремительно растет. Если обозначить через u_n первую координату точки nP, то

$$u_1 = 3, \qquad u_2 = \frac{129}{100}, \qquad u_3 = \frac{164\,323}{29\,241},$$

$$u_4 = \frac{2\,340\,922\,881}{58\,675\,600}, \qquad u_5 = \frac{307\,326\,105\,747\,363}{160\,280\,942\,564\,521}.$$

Далее нарастание происходит еще быстрее. Например, у u_{11} в числителе 71 знак.

В настоящее время неизвестно никакой общей процедуры для нахождения всех рациональных решений уравнения $y^2 = x^3 + ax^2 + bx + c$. В разобранном примере $y^2 = x^3 - 2$ одно решение $(3, 5)$ мы просто подобрали; в общем же случае неизвестно никакого метода, который позволил бы найти это первое решение. Нахождение рационального решения эллиптического уравнения с помощью эффективной

процедуры является одной из крупнейших проблем теории чисел. Однако, если одно решение есть, можно найти другие по формулам (8) и (9).

ПОРЯДОК ТОЧЕК НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

При получении точек nP из данной точки P возможны два случая. В первом случае на шаге n получается нуль, то есть существует такое число n, что $nP = E$. Если $mP \neq E$ для всех $m < n$, то говорят, что точка P имеет *конечный порядок n*. Например, на кривой $y^2 = x^3 + 4$ точка $P = (0, 2)$ имеет порядок 3, на кривой $y^2 = x^3 + 1$ точка $P = (2, 3)$ имеет порядок 6, на кривой $y^2 = x^3 - 43x + 166$ точка $P = (3, 8)$ имеет порядок 7. Можно поставить вопрос: сколько существует рациональных точек конечного порядка и каковы эти порядки?

В 1976 году американский математик Б. Мазур получил выдающийся результат, показав, что *если P – рациональная точка порядка n, то $n \leq 10$ или $n = 12$; к тому же на эллиптической кривой существует самое большее* 16 *рациональных точек конечного порядка*.

Второй случай – это когда все точки $2P$, $3P$, $4P$ и т.д. различны. В 1901 году французский математик А. Пуанкаре (1854–1912) высказал гипотезу о том, что *всегда можно найти такое конечное число рациональных точек P_1, ..., P_r бесконечного порядка, что всякая рациональная точка P выражается через них, то есть представляется в виде*

$$P = n_1P_1 + ... + n_rP_r + Q,$$

где n_1, ..., n_r – целые числа, однозначно определяемые точкой P, а Q – точка конечного порядка. Сами же точки P_1, ..., P_r не выражаются друг через друга. Число r называется *рангом кривой*.

Гипотезу Пуанкаре в 1922 году доказал английский математик Л. Морделл, но его доказательство не дает никакого способа для вычисления ранга. Лишь в 1995 году было показано, что ранг эллиптической кривой может быть найден с помощью весьма сложной аналитической конструкции.

В явном виде найдены лишь кривые, ранг которых не превосходит 21, при этом возникают гигантские числа. Например, кривая

$$y^2 + xy = x^3 - 431\,092\,980\,766\,333\,677\,958\,362\,095\,891\,166x + \\ + 5\,156\,283\,555\,366\,643\,659\,035\,652\,799\,871\,176\,909\,391\,533\,088\,196$$

имеет ранг 20.

КОДЫ С ОТКРЫТЫМ КЛЮЧОМ

Около десяти лет назад эллиптические кривые получили неожиданное применение в теории кодирования – в так называемом кодировании с открытым ключом. Сущность его заключается в следующем. Прежде всего выбираются два больших простых числа, скажем p и q, каждое примерно длиной в 100–200 знаков. Затем составляется их произведение $N = pq$. Для того чтобы прочитать сообщение, ваш корреспондент должен знать лишь значение числа N. Однако, для того чтобы расшифровать сообщение, нужно найти множители p и q. Поэтому любые сообщения, переданные таким образом, будут расшифрованы лишь тогда, когда противник сможет разложить число N на множители. Насколько быстро это можно сделать? Ясно, что наименьший множитель числа N должен быть меньше $\sqrt{N}$. Поэтому можно использовать такую процедуру: сначала проверяется, делится ли число N на 2, затем на 3, на 5 и на все последующие простые числа, не превосходящие $\sqrt{N}$. Если число N невелико, эта процедура удобна, но для больших N она абсолютно неэффективна. Например, если число N имеет около 100 знаков и если каждую секунду проверять 1 000 000 возможных делителей, то понадобится $3{,}2 \cdot 10^{37}$ лет для его разложения на множители. Поэтому нужна более эффективная процедура. В 1987 году голландский математик Х. Ленстра предложил быстрый алгоритм для разложения больших чисел на простые множители. Мы не имеем возможности привести его здесь, отметим лишь, что сердцевиной его является операция сложения точек на эллиптической кривой.

КРИВЫЕ ВЫСШИХ СТЕПЕНЕЙ

Мы ограничились здесь кривыми (а значит, диофантовыми уравнениями) степеней 2 и 3. А как обстоит дело со степенями $n \geq 4$? В этом случае также естественно выделить класс невырожденных кривых степени n (типичный представитель – кривая $x^n + y^n = 1$). При $n > 3$ картина разительно меняется. Еще в 1931 году Л. Морделл выдвинул гипотезу: на таких кривых *число рациональных точек всегда конечно*. Гипотеза Морделла более полувека была в центре внимания ведущих математиков всего мира. В 1983 году ее доказал немецкий математик Г. Фальтингс. Эффективных алгоритмов для нахождения этих точек пока неизвестно.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

1. *Коблиц Н.* Введение в эллиптические кривые и модулярные формы. М.: Мир, 1988.

2. *Прасолов В. В., Соловьев Ю. П.* Эллиптические функции и алгебраические уравнения. М.: Факториал, 1997.

3. *Степанов С. А.* Арифметика алгебраических кривых. М.: Наука, 1991.

4. *Успенский В.А.* Как теория чисел помогает в шифровальном деле // Соросовский Образовательный Журнал. 1996. № 6. С. 122–127.

* * *

Юрий Петрович Соловьев, доктор физико-математических наук, профессор Московского государственного университета им. М.В. Ломоносова. Специалист в области дифференциальной геометрии, алгебраической и дифференциальной топологии, математической физики. Автор 60 научных статей, десяти монографий и учебников.