И. Г. БАШМАКОВА

ДИОФАНТ И ДИОФАНТОВЫ УРАВНЕНИЯ

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1972

512
Б 33
УДК 512

2-2-2
75-72

ПРЕДИСЛОВИЕ

В наши дни каждый, кто занимался математикой как профессионал или как любитель, слышал о диофантовых уравнениях и даже о диофантовом анализе. За последние 15–20 лет эта область сделалась «модной» благодаря своей близости к алгебраической геометрии — властительнице дум современных математиков. Между тем, о том, кто дал имя неопределённому анализу, о самом Диофанте, одном из наиболее интересных учёных античности, почти ничего не написано. О его работах даже историки науки имеют самое превратное представление. Большинство из них считает, что Диофант занимался решением отдельных задач, равносильных неопределённым уравнениям, применяя для этого хитроумные, но частные методы. Подробнее об этих оценках Диофанта мы скажем в § 4.

Между тем простой разбор задач Диофанта показывает, что он не только поставил проблему решения неопределённых уравнений в рациональных числах, но и дал некоторые общие методы их решения. Надо при этом иметь в виду, что в античной математике общие методы никогда не излагались «в чистом виде», отдельно от решаемых задач. Так, например, поступал Архимед: определяя площади эллипса, сегмента параболы, поверхности шара, объёмы шара и других тел, он применял метод интегральных сумм и метод предельного перехода, однако нигде не дал общего абстрактного описания этих методов. Учёным XVI–XVII веков приходилось тщательно изучать и перелагать по-новому его сочинения, чтобы выделить оттуда методы Архимеда. Аналогично обстоит дело и с Диофантом. Его методы были поняты и применены для решения новых задач Виетом и Ферма, т. е. в то же время, когда был разгадан и Архимед. В своих исследованиях мы пойдём вслед за Виетом и Ферма, т. е. будем анализировать решение конкретных задач, чтобы понять применённые там общие методы.

Заметим ещё, что если история интеграционных методов Архимеда в основном завершается созданием интегрального и дифференциального исчисления Ньютоном и Лейбницем, то история методов Диофанта растягивается ещё на несколько сотен лет, переплетаясь с развитием теории алгебраических функций и алгебраической геометрии. Развитие идей Диофанта можно проследить вплоть до работ Анри Пуанкаре и Андре Вейля. Поэтому-то история диофантова анализа особенно интересна.

Настоящая книга будет посвящена в основном методам Диофанта для решения неопределённых уравнений второго и третьего порядка в рациональных числах и их истории. Попутно мы рассмотрим вопрос и о числовой системе, которую применял Диофант, и о его буквенной символике. В этом гораздо более простом вопросе также до сих пор нет ясности: большинство историков науки считает, что Диофант ограничивался областью положительных рациональных чисел и не знал отрицательных чисел. Мы постараемся показать, что это не так, что именно в «Арифметике» Диофанта область чисел была расширена до п о л я р а ц и о н а л ь н ы х ч и с е л $\mathbb{Q}$.

Я надеюсь, что эта книга познакомит читателя с новой стороной античной математики. Ведь большинство из нас составляет о ней впечатление по «Началам» Евклида, сочинениям Архимеда и Аполлония. Диофант открывает нам мир арифметики и алгебры, не менее богатый и красочный.

Разумеется, мы не сможем рассказать здесь о всём творчестве Диофанта, ещё того менее, — о всём диофантовом анализе и его истории. Как мы уже говорили, мы будем следить в основном за той областью, которая получила название арифметики алгебраических кривых и которая состоит в нахождении рациональных точек алгебраической кривой (или рациональных решений одного алгебраического уравнения от двух переменных) и в изучении структуры этого множества. Поэтому читатель не найдёт здесь истории проблемы решения неопределённых уравнений в ц е л ы х числах, которой занимались Ферма, Эйлер, Лагранж, Лежандр и которой продолжают заниматься и теперь. Мы не будем также касаться трудного и тонкого вопроса о существовании рационального

(или целого) решения у неопределённого уравнения с целыми рациональными коэффициентами, поскольку этот вопрос выходит за пределы круга проблем, непосредственно идущих от Диофанта. Наконец, мы не будем касаться и истории десятой проблемы Гильберта, в которой требуется найти общий метод (или доказать, что такового не существует), «следуя которому можно было бы в конечное число шагов узнать, имеет данное уравнение решение в целых рациональных числах или нет» [1]). Настоящая книга рассчитана на широкий круг читателей: её смогут прочесть преподаватели математики высших учебных заведений и школ, студенты физико-математических факультетов университетов и пединститутов, инженеры и школьники старших классов специализированных школ (с математическим уклоном). Строго говоря, для понимания книги достаточно знания аналитической геометрии и элементов дифференциального и интегрального исчисления, поэтому школьникам не все разделы будут доступны в равной степени. Чтобы облегчить пользование книгой, мы даём здесь «указатель», в котором расскажем, как книга построена и какие параграфы можно опустить без ущерба для понимания целого. В § 1 рассказывается о самом Диофанте, в § 2 — о системе чисел и символов, которые он вводит, в § 3 приводятся сведения из диофантовых уравнений и алгебраической геометрии, необходимые для понимания дальнейшего. Следующий, § 4, посвящён оценкам методов Диофанта историками математики. В § 5 и § 6 излагаются задачи Диофанта и исследуется, какими методами он решал неопределённые уравнения второго и третьего порядков. Здесь же рассказывается об однородных или проективных координатах. В § 7 приводятся некоторые задачи Диофанта, которые потребовали теоретико-числового исследования. Эти задачи позволяют судить об объёме знаний античных математиков по теории чисел. Всё дальнейшее, т. е. §§ 8–13, посвящено истории методов Диофанта от исследований Виета и Ферма до двадцатых годов XX века. В § 10 рассказывается о теореме сложения эллиптических интегралов Эйлера и о её применении для отыскания рациональных

[1]) См. книгу «Проблемы Гильберта», «Наука», 1969.

точек кривой третьего порядка у Якоби. Чтобы понять этот параграф, читатель должен быть знаком с понятием несобственного интеграла. Это место школьники могут пропустить. Чтение § 11 они тогда должны начинать со слов «Теперь мы можем придать операции сложения точек...». В §§ 12–13, где говорится о работах А. Пуанкаре и некоторых последующих результатах, многие вопросы изложены схематично, другие, требующие введения новых сложных понятий, опущены. Всё же я надеюсь, что читатель получит некоторое представление о творчестве Диофанта и об истории арифметики алгебраических кривых, а может быть, и заинтересуется этой прекрасной областью математики.

В заключение я приношу глубокую благодарность А. И. Лапину и И. Р. Шафаревичу, которым я обязана многими ценными замечаниями и указаниями.

Многие усовершенствования и поправки были внесены в рукопись редактором Н. Н. Гендрихсоном, которому я также приношу глубокую благодарность.

В конце книги помещён список наиболее доступных изданий «Арифметики» Диофанта и сочинений о ней.

§ 1. ДИОФАНТ

Диофант представляет одну из наиболее трудных загадок в истории науки. Нам не известны ни время, когда он жил, ни предшественники его, которые работали бы в той же области. Труды его подобны сверкающему огню среди полной непроницаемой тьмы.

Промежуток времени, когда мог жить Диофант, составляет полтысячелетия! Нижняя грань этого промежутка определяется без труда: в своей книге о многоугольных числах Диофант неоднократно упоминает математика Гипсикла Александрийского, который жил в середине II века до н. э. С другой стороны, в комментариях Теона Александрийского к «Альмагесту» знаменитого астронома Птолемея помещён отрывок из сочинения Диофанта. Теон жил в середине IV века н. э. Этим определяется верхняя грань этого промежутка. Итак, 500 лет!

Французский историк науки Поль Таннери, издатель наиболее полного текста Диофанта, попытался су́зить этот промежуток. В библиотеке Эскуриала он нашёл отрывки из письма Михаила Пселла, византийского учёного XI века, где говорится, что «учёнейший Анатолий, после того как собрал наиболее существенные части этой науки (речь идёт о введении степеней неизвестного и об их обозначениях), посвятил их своему другу Диофанту». Анатолий Александрийский действительно составил «Введение в арифметику», отрывки из которой приводят в дошедших до нас сочинениях Ямблих и Евсевий. Но Анатолий жил в Александрии в середине III века н. э. и даже более точно — до 270 года, когда он стал епископом Лаодакийским. Значит, его дружба с Диофантом, которого все называют Александрийским, должна была иметь место до этого. Итак, если знаменитый александрийский математик и друг Анатолия по имени Диофант составляют одно лицо, то время жизни Диофанта — середина III века н. э.

Сама же «Арифметика» Диофанта посвящена «достопочтенному Дионисию», который, как видно из текста «Введения», интересовался арифметикой и её преподаванием. Хотя имя Дионисий было в то время довольно распространённым, Таннери предположил, что «достопочтенного» Дионисия следует искать среди известных людей эпохи, занимавших видные посты. И вот оказалось, что в 247 году епископом Александрии стал некий Дионисий, который с 231 года руководил христианской гимназией города! Поэтому Таннери отождествил этого Дионисия с тем, которому посвятил свой труд Диофант, и пришёл к выводу, что Диофант жил в середине III века н. э. Мы можем, за неимением лучшего, принять эту дату.

Зато место жительства Диофанта хорошо известно — это знаменитая Александрия, центр научной мысли эллинистического мира.

После распада огромной империи Александра Македонского Египет в конце IV века до н. э. достался его полководцу Птолемею Лагу, который перенёс столицу в новый город — Александрию. Вскоре этот многоязыкий торговый город сделался одним из прекраснейших городов древности. Размерами его превзошёл впоследствии Рим, но долгое время ему не было равного. И вот именно этот город стал на многие века научным и культурным центром древнего мира. Это было связано с тем, что Птолемей Лаг основал Музейон, храм Муз, нечто вроде первой Академии наук, куда приглашались наиболее крупные учёные, причём им назначалось содержание, так что основным делом их были размышления и беседы с учениками. При Музейоне была построена знаменитая библиотека, которая в лучшие свои дни насчитывала более 700 000 рукописей. Неудивительно, что учёные и жаждущие знаний юноши со всего мира устремились в Александрию, чтобы послушать знаменитых философов, поучиться астрономии и математике, иметь возможность в прохладных залах библиотеки углубиться в изучение уникальных рукописей.

Музейон пережил династию Птолемеев. В первые века до н. э. он пришёл во временный упадок, связанный с общим упадком дома Птолемеев в связи с римскими завоеваниями

(Александрия была окончательно завоевана в 31 году до н. э.), но затем в первые века н. э. он снова возродился, поддерживаемый уже римскими императорами. Александрия продолжала оставаться научным центром мира. Рим никогда не был в этом отношении её соперником: римской науки (мы имеем в виду естественные науки) просто не существовало, и римляне оставались верными заветам Вергилия, писавшего:

> Тоньше другие ковать будут жизнью дышащую бронзу, —
> Верю тому, — создадут из мрамора лики живые,
> Красноречивее будут в судах, движения неба
> Тростью начертят своей и вычислят звёзд восхожденья,
> Ты же, римлянин, знай, как надо народами править [1]).

И если в III–II веках до н. э. Музейон блистал именами Евклида, Аполлония, Эратосфена, Гиппарха, то в I–III веках н. э. здесь работали такие учёные как Герон, Птолемей и Диофант.

Чтобы исчерпать всё известное о личности Диофанта, приведём дошедшее до нас стихотворение-загадку:

> Прах Диофанта гробница покоит; дивись ей — и камень
> Мудрым искусством его скажет усопшего век.
> Волей богов шестую часть жизни он прожил ребёнком
> И половину шестой встретил с пушком на щеках.
> Только минула седьмая, с подругою он обручился.
> С нею пять лет проведя сына дождался мудрец;
> Только полжизни отцовской возлюбленный сын его прожил.
> Отнят он был у отца ранней могилой своей.
> Дважды два года родитель оплакивал тяжкое горе,
> Тут и увидел предел жизни печальной своей [2]).

Отсюда нетрудно подсчитать, что Диофант прожил 84 года. Однако для этого вовсе не нужно владеть искусством Диофанта! Достаточно уметь решать уравнение 1-й степени с одним неизвестным, а это умели делать египетские писцы ещё за 2 тысячи лет до н. э.

Но наиболее загадочным представляется творчество Диофанта. До нас дошло шесть книг из 13, которые были объединены в «Арифметику». Стиль и содержание этих книг резко отличаются от классических античных сочинений по теории чисел и алгебре, образцы которых мы знаем по «Началам»

[1]) Перевод Ф. А. Петровского.
[2]) Перевод С. П. Боброва.

Евклида, его «Данным», леммам из сочинений Архимеда и Аполлония. «Арифметика», несомненно, явилась результатом многочисленных исследований, которые остались нам совершенно не известны. Мы можем только гадать о её корнях и изумляться богатству и красоте её методов и результатов.

«Арифметика» Диофанта — это сборник задач (их всего 189), каждая из которых снабжена решением (или несколькими способами решения) и необходимыми пояснениями. Поэтому с первого взгляда кажется, что она не является теоретическим произведением. Однако при внимательном чтении видно, что задачи тщательно подобраны и служат для иллюстрации вполне определённых, строго продуманных методов. Как это было принято в древности, методы не формулируются в общем виде, а повторяются для решения однотипных задач.

Всё же первой книге предпослано «общее введение» автора, на котором мы остановимся более подробно.

§ 2. ЧИСЛА И СИМВОЛЫ

Диофант начинает с основных определений и описания буквенных символов, которые он будет применять.

В классической греческой математике, которая нашла своё завершение в «Началах» Евклида, под числом (ἀριθμός — «*аритмос*» или «*арифмос*»; отсюда название «арифметика» для науки о числах) понималось множество единиц, т. е. целое число. Ни дроби, ни иррациональности числами не назывались. Строго говоря, никаких дробей в «Началах» нет. Единица считается неделимой и вместо долей единицы рассматриваются отношения целых чисел; иррациональности появляются как отношения несоизмеримых отрезков, например, число, которое мы теперь обозначаем $\sqrt{2}$, для греков классической эпохи было отношением диагонали квадрата к его стороне. Об отрицательных числах не было и речи. Для них не существовало даже никаких эквивалентов. Совершенно иную картину мы находим у Диофанта.

Диофант приводит традиционное определение числа как множества единиц, однако в дальнейшем ищет для своих за-

дач *положительные рациональные* решения, причём называет каждое такое решение числом (ἀριθμός — «аритмос»).

Но этим дело не ограничивается. Диофант вводит отрицательные числа: он называет их специальным термином λεῖψις — «лейпсис» — производное от глагола λεῖπω — «лейпо», что означает недоставать, нехватать, так что сам термин можно было бы перевести словом «недостаток». Кстати, так поступает известный русский историк науки И. Тимченко [1]). Положительное число Диофант называет словом ὑπαρξις — «ипарксис», что означает существование, бытие, а во множественном числе это слово может означать имущество или достояние. Таким образом, терминология Диофанта для относительных чисел близка к той, которую употребляли в Средние века на Востоке и в Европе. Скорее всего, это было просто переводом с греческого на арабский, санскрит, латынь, а затем на различные языки Европы.

Заметим, что термин λεῖψις — «лейпсис» — нельзя переводить как «вычитаемое», как это делают многие переводчики Диофанта, потому что для операции вычитания Диофант применяет совершенно иные термины, а именно ἀφελεῖν — «*афелейн*» или ἀφαιρεῖν — «*афайрейн*», которые являются производными от глагола ἀφαιρεω — «*афайрео*» — отнимать. Сам Диофант при преобразовании уравнений часто употребляет стандартное выражение «прибавим к обеим сторонам λεῖψις».

Мы так подробно остановились на филологическом анализе текста Диофанта, чтобы убедить читателя, что мы не отступим от истины, если будем переводить термины Диофанта как «положительное» и «отрицательное».

Диофант формулирует для относительных чисел правило знаков:

> «отрицательное, умноженное на отрицательное, даёт положительное, тогда как отрицательное на положительное даёт отрицательное, и отличительный знак для отрицательного есть Д перевёрнутая и укороченная (буква) ψ».

Далее он пишет:

[1]) И. Тимченко, Основания теории аналитических функций, ч. I, Исторические сведения, Одесса, 1899.

> «После того как я тебе объяснил умножение, становится ясным и деление предложенных членов; теперь будет хорошо приступить к упражнениям над сложением, вычитанием и умножением таких членов. И положительные и отрицательные члены с различными коэффициентами прибавлять к другим членам, которые либо положительны, либо, равным образом, и положительны и отрицательны, и от положительных членов и других отрицательных отнимать другие положительные и, равным образом, положительные и отрицательные».

Заметим, что хотя Диофант ищет только рациональные положительные решения, в промежуточных выкладках он охотно пользуется отрицательными числами.

Мы можем, таким образом, отметить, что Диофант расширил числовую область до поля рациональных чисел, в котором можно беспрепятственно производить все четыре действия арифметики.

В «Арифметике» мы встречаем впервые и буквенную символику. Диофант ввёл следующие обозначения для первых шести степеней x, $x^2, \ldots, x^6$ неизвестного x:

первая степень — ς;

вторая степень — $\Delta^{\tilde{\upsilon}}$ от **Δύναμις** — «*дюнамис*», что означает сила, степень;

третья степень — $\mathrm{K}^{\tilde{\upsilon}}$ от **Κύβος** — «*кубос*», т. е. куб;

четвёртая степень — $\Delta^{\tilde{\upsilon}}\Delta$ от **Δύναμοδύναμις** — «*дюнамодюнамис*», т. е. квадратоквадрат;

пятая степень — $\Delta\mathrm{K}^{\tilde{\upsilon}}$ от **Δύναμοκύβος** — «*дюнамокубос*», т. е. квадратокуб;

шестая степень — $\mathrm{K}^{\tilde{\upsilon}}\mathrm{K}$ от **Κύβοκύβος** — «*кубокубос*», т. е. кубокуб.

Свободный член, или x^0, Диофант обозначал символом $\overset{\circ}{\mathrm{M}}$, т. е. первыми двумя буквами слова **μονάς** — «*монас*», что значит единица.

Он ввёл специальный знак для отрицательного показателя степени X и, таким образом, получил возможность обозначать первые шесть отрицательных степеней неизвестного. Например, x^{-2}, x^{-3} он обозначал соответственно $\Delta^{\tilde{\upsilon}}X$, $\mathrm{K}^{\tilde{\upsilon}}X$.

Итак, у Диофанта была символика для обозначения о д н о г о неизвестного и его положительных и отрицательных

степеней вплоть до шестой. Обозначения для второго неизвестного он не ввёл, что сильно затрудняло решение задач. Иногда на протяжении одной задачи символ ς мог обозначать то одно, то другое неизвестное число. Кроме этих символов, Диофант употреблял знак □ для неопределённого квадрата. Например, если по условию задачи произведение двух чисел в сумме с одним из них должно было равняться квадрату, то этот последний квадрат записывался с помощью □.

Далее, Диофант излагает правила умножения x^m на x^n для положительных и отрицательных m и n ($|m| \leqslant 6$, $|n| \leqslant 6$).

Для равенства Диофант применял знак ίσ — первые две буквы слова ίσος — «*исос*», т. е. равный. Всё это даёт ему возможность получить буквенную запись уравнения. Например, уравнение

$$202x^2 + 13 - 10x = 13$$

он записывает так:

$$\Delta^{\tilde{\upsilon}}\overline{\sigma\beta}\,\overset{\circ}{\mathrm{M}}\,\overline{\iota\gamma} \wedge \varsigma\bar{\imath}\acute{\imath}\sigma\,\overset{\circ}{\mathrm{M}}\,\overline{\iota\gamma} \quad {}^{1}).$$

Далее, во «введении» формулируются правила преобразования уравнений: прибавление равных членов к обеим частям уравнения и приведение подобных членов. Оба эти правила получили впоследствии широкую известность под арабизированными названиями «алджебр» и «альмукабала».

Мы видим, что хотя при наименовании и обозначении степеней неизвестного ещё применяются геометрические термины «квадрат», «куб» (что, кстати, сохранилось и до наших дней), однако при составлении уравнений Диофант спокойно складывает квадрат или куб со стороной [2]), т. е. трактует их не как геометрические образы, а как числа. Более того, он находит возможным ввести «квадратоквадраты», «квадрато-

[1]) Греки обозначали числа с помощью букв алфавита, над которыми сверху ставилась чёрточка. Первые 9 букв: $\bar{\alpha}$, $\bar{\beta}$,..., $\bar{\vartheta}$ обозначали числа от 1 до 9, следующие 9 букв обозначали десятки от 10 до 90, и следующие 9 — сотни. Так, $\bar{\sigma} = 200$, $\bar{\beta} = 2$, поэтому $\overline{\sigma\beta}$ есть запись числа 202, $\bar{\iota} = 10$, $\bar{\gamma} = 3$, т. е. $\overline{\iota\gamma} = 13$.

[2]) В так называемой «геометрической алгебре» греков операция сложения была определена только для однородных величин, т. е. отрезки можно было складывать с отрезками, площади с площадями, но нельзя было сложить отрезок с площадью (квадрат со стороной). Сложение понималось как геометрическая операция («приложение»), а не как арифметическое сложение соответствующих чисел.

кубы» и т. д., разумеется, никак не связывая их с пространствами высшего числа измерений, т. е. он употребляет геометрическую терминологию только благодаря сложившейся традиции.

Таким образом, мы здесь встречаемся с совершенно новым построением алгебры, которая основывается уже не на геометрии, как это было у Евклида, а на арифметике. Однако это не простой возврат к числовой алгебре Вавилона, а начало построения буквенной алгебры, которая наконец-то находит у Диофанта присущий ей язык.

§ 3. ДИОФАНТОВЫ УРАВНЕНИЯ

Но в «Арифметике» поражает не только совершенно новый язык, не только смелое расширение области чисел, но и особенно те проблемы, которые ставит и решает Диофант.

Чтобы понять сущность этих проблем и исследовать методы Диофанта, нам придётся дать некоторые сведения из алгебраической геометрии и теории неопределённых уравнений. В настоящее время задача решения неопределённых уравнений формулируется так: пусть дано m многочленов от n переменных, $m < n$, $f_1(x_1, x_2, \ldots, x_n)$, $\ldots$, $f_m(x_1, x_2, \ldots, x_n)$ с коэффициентами из некоторого поля k [1]). Требуется найти множество $M(k)$ всех рациональных решений системы

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases} \tag{1}$$

и определить его алгебраическую структуру. При этом решение $(x_1^{(0)}, \ldots, x_n^{(0)})$ называется *рациональным*, если все $x_i^{(0)} \in k$.

Множество $M(k)$, разумеется, зависит от поля k. Так, уравнение $x^2 + y^2 = 3$ не имеет ни одного рационального решения

[1]) *Полем* называется множество элементов, над которыми определены все четыре действия арифметики, обладающие обычными свойствами. При этом результат любой из этих операций над двумя элементами поля должен снова принадлежать полю. Примерами полей будут: 1) множество всех рациональных чисел, 2) множество чисел вида $a + b\sqrt{2}$, 3) множество всех действительных чисел. Читатель, незнакомый с понятием поля, может считать, что все рассуждения проводятся над полем $\mathbb{Q}$ рациональных чисел.

в поле $\mathbb{Q}$ рациональных чисел, но имеет бесконечно много решений в поле $\mathbb{Q}(\sqrt{3})$, т. е. в множестве чисел вида $a+b\sqrt{3}$, где a и b — рациональные числа [1]).

Наиболее важными для теории чисел являются случаи, когда 1) $k=\mathbb{Q}$, где $\mathbb{Q}$ — поле рациональных чисел, или 2) k есть поле вычетов по простому модулю p. Диофант рассматривал первый из этих случаев. Мы также будем всегда в дальнейшем считать, что $k=\mathbb{Q}$.

Мы ограничимся рассмотрением только таких задач Диофанта, которые сводятся к одному уравнению с двумя неизвестными, т. е. к случаю $m=1$, $n=2$:

$$f(x,y)=0. \tag{2}$$

Это уравнение определяет на плоскости $\mathbb{R}^2$ *алгебраическую кривую* Γ. Рациональное решение (2) будем называть *рациональной точкой* кривой Γ. В дальнейшем мы часто будем прибегать к языку геометрии, хотя сам Диофант нигде его не применяет. Однако геометрический язык стал в настоящее время столь неотъемлемой частью математического мышления, что многие факты будет легче понять и объяснить с его помощью.

Прежде всего необходимо дать какую-нибудь классификацию уравнений (2) или, что то же, алгебраических кривых. Наиболее естественной и ранее всего возникшей является классификация их по порядкам.

Напомним, что *порядком* кривой (2) называется максимальный порядок членов многочлена $f(x,y)$, где под порядком члена понимается сумма степеней при x и y. Геометрический смысл этого понятия заключается в том, что прямая пересекается с кривой порядка n ровно в n точках. При подсчёте точек надо, разумеется, учитывать кратность точек пересечения, а также комплексные и «бесконечно удалённые» (см. стр. 27) точки. Так, например, окружность $x^2+y^2=1$ и прямая $x+y=2$ пересекаются в двух комплексных точках, а гипербола $x^2-y^2=1$ и прямая $y=x$

[1]) Ясно, что сумма, разность и произведение двух чисел вида $a+b\sqrt{3}$ снова имеют тот же вид. Читателю предоставляется доказать, что и частное двух таких чисел можно представить в виде $a+b\sqrt{3}$, т. е. что $\mathbb{Q}(\sqrt{3})$ действительно является полем.

— в двух бесконечно удалённых точках, та же гипербола с прямой $x = 1$ имеет одну общую точку кратности 2.

Однако для целей *диофантова анализа* (такое название получила область математики, выросшая из задач решения неопределённых уравнений; впрочем, теперь её чаще называют диофантовой геометрией) классификация по порядкам оказалась слишком грубой.

Поясним сказанное на примере. Пусть задана окружность C: $x^2+y^2 = 1$ и любая прямая с рациональными коэффициентами, например, L: $y = 0$. Покажем, что рациональные точки этой окружности и прямой можно поставить во взаимно однозначное соответствие. Это можно сделать, например, так: закрепим точку $A(0, -1)$ окружности и поставим в соответствие каждой рациональной точке B прямой L точку B' окружности C, лежащую на пересечении C и прямой AB (рис. 1). То, что координаты точки B' будут рациональными, предоставим читателю доказать самому либо прочесть аналогичное доказательство у Диофанта (оно будет изложено в следующем параграфе). Очевидно, что такое же соответствие можно установить между рациональными точками любого конического сечения, если на нём лежит хотя бы одна рациональная точка, и рациональной прямой. Мы видим, что с точки зрения диофантова анализа окружность C и прямая L неотличимы: множества их рациональных решений эквивалентны. И это несмотря на то, что порядки обеих кривых различны.

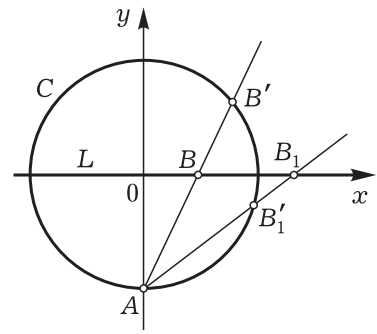

Рис. 1.

Более тонкой является классификация алгебраических кривых по р о д а м, которая была введена только в XIX веке Абелем и Риманом. Эта классификация учитывает число особых точек кривой Γ.

Будем считать, что в уравнении (2) кривой Γ многочлен $f(x, y)$ неприводим над полем рациональных чисел, т. е. он не раскладывается в произведение многочленов с рациональными коэффициентами. Как известно, уравнение касательной к

кривой Γ в точке $P(x_0, y_0)$ будет

$$y - y_0 = k(x - x_0),$$

где

$$k = -\frac{f'_x(x_0, y_0)}{f'_y(x_0, y_0)}\,.$$

Если в точке P производная f'_x или f'_y отлична от нуля, то угловой коэффициент k касательной имеет вполне определённое значение (если $f'_y(x_0, y_0) = 0$, а $f'_x(x_0, y_0) \neq 0$, то $k = \infty$ и касательная в P будет вертикальной).

Если же в точке P обе частные производные обращаются в нуль,

$$f'_x(x_0, y_0) = 0 \qquad \text{и} \qquad f'_y(x_0, y_0) = 0,$$

то точка P называется *особой*.

Например, у кривой $y^2 = x^2 + x^3$ точка $(0, 0)$ будет особой, так как в ней $f'_x = -2x - 3x^2$ и $f'_y = 2y$ обращаются в нуль.

Наиболее простыми особыми точками являются двойные, в которых хотя бы одна из производных f''_{xx}, f''_{xy} и f''_{yy} отлична от нуля. На рис. 2 изображена двойная точка, в которой кривая имеет две различные касательные. Другие более сложные особые точки изображены на рис. 3.

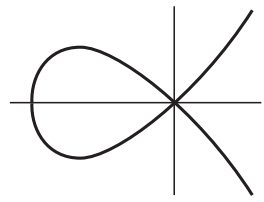

Рис. 2.

У алгебраической кривой может быть только конечное число особых точек. Действительно, пусть

$$f(x, y) = 0 \qquad (*)$$

— уравнение кривой, где $f(x, y)$ — неприводимый многочлен над полем $\mathbb{Q}$ рациональных чисел. Координаты особых точек

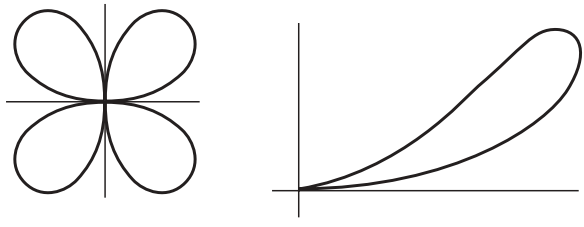

Рис. 3.

должны удовлетворять уравнениям

$$f'_x(x,y)=0, \qquad f'_y(x,y)=0$$

и уравнению $(*)$. Но система этих трёх алгебраических уравнений может иметь только конечное число решений.

Мы определим здесь род для таких плоских алгебраических кривых, которые не имеют никаких особых точек, кроме двойных. В общем случае, т. е. для произвольной алгебраической кривой с любыми особенностями, род определяется более сложно, однако мы не будем пользоваться этим определением, поэтому не будем его приводить.

Итак, пусть число двойных точек плоской алгебраической кривой Γ равно d $(d\geqslant 0)$, тогда *родом* кривой Γ называется целое число p, определяемое по формуле

$$p=\frac{(n-1)(n-2)}{2}-d,$$

где n — порядок кривой Γ. Можно показать, что $p\geqslant 0$.

Если Γ — прямая или кривая второго порядка, то из приведённой формулы видно, что $p=0$, т. е. это кривые одного и того же рода. Кривые третьего порядка имеют род 0 или 1 в зависимости от того, имеют ли они особую точку или нет. Например, род 1 будет иметь «кривая Ферма»: $x^3+y^3=1$.

Однако и классификация по родам не учитывает арифметических свойств кривой. Так, например, кривые $x^2+y^2=1$ и $x^2+y^2=3$ имеют род 0, между тем на первой из них лежит бесконечно много рациональных точек, а на второй — ни одной. Чтобы найти адекватную для целей диофантова анализа классификацию кривых, заметим, что, решая уравнение (1), мы часто прибегаем к замене переменных

$$x=\varphi(u,v), \qquad y=\psi(u,v), \tag{3}$$

где φ и ψ — рациональные функции, т. е. каждая из них может быть представлена в виде отношения двух многочленов. Подставляя (3) в уравнение (2), получим

$$G(u,v)=0. \tag{4}$$

Это уравнение определяет некоторую кривую Γ'. Для того чтобы рациональные точки кривой Γ, кроме, быть может, ко-

нечного числа их, переходили в рациональные точки кривой Γ' и, обратно, рациональным точкам кривой Γ' отвечали рациональные же точки кривой Γ, необходимо и достаточно, чтобы 1) функции φ и ψ имели рациональные коэффициенты и 2) уравнения (3) были обратимы, т. е. из них, в свою очередь, можно было бы найти

$$u = \varphi_1(x, y), \qquad v = \psi_1(x, y), \tag{3'}$$

где φ_1 и ψ_1 — рациональные функции с рациональными коэффициентами.

Если между двумя кривыми Γ и Γ' можно установить соответствие с помощью формул вида (3) и (3′) с рациональными коэффициентами, то кривые называются *бирационально эквивалентными*, а сами эти преобразования называются *бирациональными*.

Так, например, если $\varphi(u, v)$ и $\psi(u, v)$ — линейные функции, т. е.

$$\begin{cases} x = \varphi(u, v) = au + bv + c, \\ y = \psi(u, v) = a_1u + b_1v + c_1, \end{cases}$$

причём $\begin{vmatrix} a & b \\ a_1 & b_1 \end{vmatrix} \neq 0$, то u, v также выразятся через x, y линейно с рациональными коэффициентами, т. е. преобразование будет бирациональным. Приведём более сложный пример. Пусть задана кривая L:

$$y^2 = x^4 - x^3 + 2x - 2 = (x - 1)(x^3 + 2). \tag{$*$}$$

Покажем, что её можно бирационально преобразовать в кривую L' вида $v^3 = \varphi_3(u)$, где $\varphi_3(u)$ — многочлен третьей степени. Для этого разделим обе части уравнения ($*$) на $(x-1)^4$ и положим

$$x - 1 = \frac{1}{u}, \qquad \frac{y}{(x-1)^2} = v.$$

Тогда уравнение ($*$) преобразуется в

$$v^2 = 3u^3 + 3u^2 + 3u + 1.$$

При этом x и y выражаются через u, v рационально:

$$x = \frac{1 + u}{u}, \qquad v = \frac{v}{u^2}$$

и, обратно,

$$u = \frac{1}{x-1}, \qquad v = \frac{y}{(x-1)^2},$$

т. е. кривые L и L' бирационально эквивалентны [1]).

Множество рациональных точек M и M' двух бирационально эквивалентных кривых можно привести во взаимно однозначное соответствие, за исключением, быть может, конечного числа точек. Исключительными точками будут те, в которых числитель и знаменатель по крайней мере одной из функций (3) или (3′) одновременно обращаются в нуль (отсюда ясно, что у линейных преобразований исключительных точек нет). Во втором нашем примере точке $(1, 0)$ кривой L не отвечает ни одна точка кривой L', так как в ней обращаются в нуль числитель и знаменатель выражения для v: $v = \frac{y}{(x-1)^2}$.

С точки зрения диофантова анализа две бирационально эквивалентные кривые между собой равноправны. Между тем порядок кривой Γ' будет, вообще говоря, отличен от порядка кривой Γ. Но можно доказать, что две бирационально эквивалентные кривые имеют один и тот же род. Таким образом, хотя ни порядок кривой n, ни число её двойных точек d не являются инвариантами бирационального преобразования, но род p кривой, составленный из этих величин, будет таким инвариантом.

Обратное утверждение неверно: кривые одного и того же рода могут не быть бирационально эквивалентными. Это видно хотя бы из приведённого выше примера кривых $x^2+y^2 = 1$ и $x^2 + y^2 = 3$, которые имеют род 0: но на первой из них лежит бесконечно много рациональных точек, а на второй — ни одной.

Таким образом, кривые одного и того же рода разбиваются на классы бирационально эквивалентных между собой кривых. Вся сила введённых понятий была выявлена в работах Анри Пуанкаре, который в самом начале XX века положил совокупность бирациональных преобразований в основу клас-

[1]) Легко видеть, что аналогичным образом можно преобразовать любую кривую вида $y^2 = f_{2n}(x)$, где $f_{2n}(x)$ — многочлен степени $2n$, имеющий рациональный корень a, т. е. $f_{2n}(x) = (x-a)g_{2n-1}(x)$, в кривую $v^2 = \varphi_{2n-1}(u)$.

сификации и исследования проблем диофантова анализа. Мы будем говорить об этом в § 12.

Сейчас отметим только один, весьма важный для дальнейшего, факт: если Γ — кривая третьего порядка, которая имеет по крайней мере одну рациональную точку, то её уравнение с помощью бирациональных преобразований всегда можно привести к виду

$$y^2 = x^3 + ax^2 + b, \tag{5}$$

где a и b — рациональные числа. Мы часто будем считать в дальнейшем, что кривая Γ уже задана в виде (5).

§ 4. ОЦЕНКА МЕТОДОВ ДИОФАНТА ИСТОРИКАМИ НАУКИ

В следующих параграфах мы покажем, что Диофант владел общим методом для определения рациональных точек на кривых второго порядка. Как показал Пуанкаре, этот метод применим для всех кривых рода 0, имеющих рациональную точку. Диофант нашёл также общие методы для отыскания рациональных точек на кривых третьего порядка, причём методы эти оказались глубоко отличными от тех, которые он применял для кривых второго порядка. Из работ Пуанкаре следует, что эти методы Диофанта применимы для нахождения рациональных точек на любых кривых рода 1. Никаких других общих методов для нахождения рациональных точек алгебраических кривых до сих пор не существует.

Мы покажем также, какую роль сыграли идеи и методы Диофанта в истории математики, как ими пользовались математики от Виета и Ферма до Эйлера.

Между тем большинство историков науки, в противоположность математикам, до сих пор недооценивали труды Диофанта. Многие из них считали, что Диофант ограничивался нахождением только одного решения и применял для этого искусственные приёмы, различные для разных задач. Такого мнения придерживался, например, Г. Ганкель, который писал: «...современному математику после изучения 100 решений Диофанта трудно решить 101-ю задачу... Диофант скорее

ослепляет, чем приводит в восторг» (H. Hankel, Zur Geschichte der Mathematik in Altertum und Mittelalter, Leipzig, 1874, стр. 165).

Но, может быть, такая оценка объясняется тем, что книга Ганкеля была написана до работ Пуанкаре, проливших новый свет на проблемы диофантовых уравнений? Но, вот, перед нами книга О. Беккера и И. Гофмана «История математики», вышедшая в 1951 году (O. Becker, J. Hofmann, Geschichte der Mathematik, Bonn). На стр. 90 мы читаем: «Диофант не даёт никакого общего метода, но применяет, по-видимому, для каждой новой задачи новый неожиданный искусственный приём, напоминающий восточные». Аналогичные высказывания делает и Ван-дер-Варден в своей книге «Пробуждающаяся наука»: «Обычно он (т. е. Диофант) удовлетворяется каким-нибудь одним решением, не делая различия, будет ли оно целочисленным или дробным. Его метод меняется от одного случая к другому». И специально о неопределённых уравнениях второго порядка: «Ему удаётся так хитро устроить, чтобы в этом (т. е. результирующем) квадратном уравнении выпал либо член с x^2, либо постоянная величина, и удалось для x найти рациональное решение». И это говорится об общем методе!

Более правильную оценку Диофанта мы находим у Г. Г. Цейтена: «Вообще говоря, Диофант старается найти какое-нибудь одно решение задачи, не отыскивая общего решения её, которое включает в себя все возможные частные решения, но не следует придавать особенного значения этому факту, если желать понять полученные Диофантом результаты, ибо частные его решения заключаются лишь в том, что он сейчас же придаёт определённые значения вспомогательным количествам, служащим для решения задачи» (История математики в древности и средние века, ГОНТИ, 1938, стр. 167–168).

После этого Цейтен разбирает способы Диофанта для решения неопределённых уравнений второго порядка. Однако и он не видит у Диофанта методов для решения неопределённых уравнений третьего порядка. До сих пор эти методы приписываются различным математикам нового времени. Так,

Т. Сколем в своей книге «Диофантовы уравнения» (Skolem, Diophantische Gleichungen, Berlin, 1938) методы Диофанта приписывает Коши и Люка, а сам Люка — Коши и Ферма.

Итак, с общими методами решения неопределённых уравнений Диофанту так же не повезло, как и с отрицательными числами!

Но приступим к рассмотрению его задач.

§ 5. НЕОПРЕДЕЛЁННЫЕ УРАВНЕНИЯ ВТОРОГО ПОРЯДКА

Два вида таких уравнений были рассмотрены до Диофанта. Это уравнения $x^2 + y^2 = z^2$ и $x^2 - ay^2 = 1$. Первое из них появилось ещё в Древнем Вавилоне. Формулы для его решения были найдены пифагорейцами:

$$x = k^2 - 1, \qquad y = 2k, \qquad z = k^2 + 1.$$

Второе полностью решается в «Началах» Евклида для случая $a = 2$, причём не в рациональных, а в целых числах. Решение его для произвольного неквадратного a, вероятно, знал Архимед, поставивший перед Эратосфеном известную «Задачу о быках».

Диофант в книге II своей «Арифметики» рассматривает различные неопределённые уравнения второго порядка и устанавливает, по существу, следующую теорему: *неопределённое уравнение второго порядка от двух переменных либо не имеет ни одного рационального решения, либо имеет их бесконечно много, причём в последнем случае все решения выражаются как рациональные функции параметра*

$$x = \varphi(k), \qquad y = \psi(k),$$

где φ *и* ψ *— рациональные функции.*

Чтобы показать это, приведём сначала задачу 8 книги II.

«Данный квадрат разделить на два квадрата [1]).

Пусть предложено 16 разделить на два квадрата. И положим первый x^2, а другой тогда будет $16 - x^2$; таким образом,

[1]) При переводе задач Диофанта мы будем пользоваться для обозначения неизвестной и её степеней современными обозначениями.

должно быть

$$16 - x^2 = \square.$$

Образуем этот квадрат из нескольких x минус столько единиц, сколько содержится в стороне 16; пусть будет $2x - 4$, что в квадрате даст

$$4x^2 + 16 - 16x.$$

Это равно

$$16 - x^2.$$

К обеим частям прибавим отрицательные (члены) и сделаем приведение подобных. Тогда

$$5x^2 = 16x \qquad \text{и} \qquad x = \tfrac{16}{5}\,.$$

Один будет $\frac{256}{25}$, другой $\frac{144}{25}$, сумма их будет $\frac{400}{25} = 16$, и каждый из них будет квадратом».

Попробуем теперь выделить метод Диофанта «в чистом виде». Итак, пусть дано уравнение

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

которое представляет окружность с центром в начале координат. Одним из рациональных решений этого уравнения будет $(0, -a)$. Диофант делает подстановку:

$$\begin{cases} x = x, \\ y = kx - a. \end{cases} \tag{7}$$

Не имея обозначений для произвольного k, он берёт $k = 2$, отмечая, однако, что следует образовать квадрат из «нескольких x минус столько единиц, сколько содержится в стороне 16», т. е. в нашей символике это в точности $kx - 4$.

Подстановку (7) можно интерпретировать геометрически как проведение через точку $(0, -a)$ прямой

$$y = kx - a. \tag{7'}$$

Эта прямая встретит окружность (6) ещё в одной точке, координаты которой будут рациональными функциями от k. Действительно,

$$x^2 + (kx - a)^2 = a^2$$

и

$$x = \frac{2ak}{k^2 + 1}\,, \qquad y = kx - a = a\,\frac{k^2 - 1}{k^2 + 1}\,.$$

Таким образом, каждому рациональному значению k отвечает

одна и только одна рациональная точка кривой (6). Наоборот, как легко видеть, если мы соединим произвольную рациональную точку кривой (6) с точкой $(0, -a)$, то получим прямую с рациональным угловым коэффициентом.

Ещё яснее метод Диофанта виден из решения задачи 9 книги II, которую он формулирует так:

> «Данное число, являющееся суммой двух квадратов, разбить на два других квадрата».

Диофант задаёт число 13, которое равно сумме $4 + 9$. Таким образом, одно решение $(2, 3)$ уже известно. Чтобы найти другое, Диофант полагает первое число равным $x = t + 2$, второе $y = 2t - 3$, т. е. он проводит прямую через точку $(2, -3)$, замечая, как и прежде, что вместо множителя 2 можно взять любое другое число.

Интересно отметить, что в качестве известной точки он берёт не указанную нами и имеющую положительные координаты, но выбирает точку с отрицательной ординатой, что соответствует отрицательному решению. Вообще Диофант в промежуточных выкладках охотно оперирует с отрицательными числами, хотя окончательное решение должно быть всегда рациональным и положительным.

Диофант применяет ту же процедуру и в задаче 16, 17 и др. книги II.

Легко видеть, что метод Диофанта совершенно общий; он позволяет найти все рациональные точки кривой второго порядка, если эта кривая содержит хотя бы одну рациональную точку. Действительно, пусть дано уравнение второго порядка от двух переменных

$$f_2(x, y) = 0 \tag{8}$$

и пусть оно имеет рациональное решение (a, b). Следуя Диофанту, сделаем подстановку:

$$\begin{cases} x = a + t, \\ y = b + kt \end{cases}$$

и получим

$$f_2(a + t, b + kt) = f_2(a, b) + tA(a, b) + \\ + ktB(a, b) + t^2C(a, b, k) = 0.$$

Но $f_2(a,b)=0$, поэтому

$$t=-\frac{A(a,b)+kB(a,b)}{C(a,b,k)}\,.$$

Таким образом, для каждого рационального k мы найдём одно и только одно рациональное решение.

Если заданное уравнение имеет вид

$$y^2=a^2x^2+bx+c, \tag{9}$$

то Диофант несколько видоизменяет приём, полагая

$$y=ax+m.$$

Тогда

$$x=\frac{c-m^2}{2am-b}\,.$$

Постараемся выяснить геометрический смысл этой второй подстановки. Для этого нам придётся перейти к однородным или проективным координатам. Поскольку эти координаты очень удобны для исследования свойств алгебраических кривых и мы будем неоднократно применять их в дальнейшем, остановимся на этом вопросе подробнее. До сих пор мы рассматривали, как это принято в аналитической геометрии, аффинную плоскость $\mathbb{R}^2$, каждая точка которой задаётся упорядоченной парой действительных чисел (x,y). Теперь рассмотрим проективную плоскость $\mathbb{P}^2$, каждую точку которой будем характеризовать упорядоченной тройкой действительных чисел (u,v,z), из которых хотя бы одно отлично от нуля. Точки (u,v,z) и (u_1,v_1,z_1) будем считать одинаковыми тогда и только тогда, когда $u_1=ku$, $v_1=kv$ и $z_1=kz$, причём $k\neq 0$. Таким образом, бесконечно много троек определяют одну и ту же точку. Любой набор u, v, z, задающий точку, называется её *однородными координатами*.

Установим теперь соответствие между точками плоскостей $\mathbb{R}^2$ и $\mathbb{P}^2$. Пусть (u,v,z) есть некоторая точка $\mathbb{P}^2$. Если $z\neq 0$, то возьмём тройку $\left(\frac{u}{z}\,,\frac{v}{z}\,,1\right)$, которая определяет ту же точку. Поставим в соответствие этой точке точку плоскости $\mathbb{R}^2$ с координатами (x,y), где $x=\frac{u}{z}\,$, $y=\frac{v}{z}\,$.

Если же $z = 0$, то точке $(u, v, 0)$ не будет отвечать ни одна точка плоскости $\mathbb{R}^2$. Такие точки будем называть *бесконечно удалёнными* или *несобственными*. Все такие точки лежат на бесконечно удалённой прямой $z = 0$. Поскольку координата z вполне равноправна с остальными координатами, то мы получаем возможность рассматривать на плоскости $\mathbb{P}^2$ бесконечно удалённые точки и бесконечно удалённую прямую как вполне равноправные с конечными точками и прямыми.

Для перехода от уравнения

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

записанного в аффинных координатах, к уравнению в однородных координатах полагаем

$$x = \frac{u}{z}\,, \qquad y = \frac{v}{z}\,.$$

Сделав соответствующую подстановку и приведение к общему знаменателю, получим уравнение

$$\Phi(u, v, z) = 0,$$

где $\Phi(u, v, z)$ — многочлен относительно u, v и z. Например, уравнение гиперболы

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

в однородных координатах примет вид

$$u^2 - v^2 = z^2.$$

Чтобы найти бесконечно удалённые точки этой кривой, положим $z = 0$ (иначе говоря, найдём её точки пересечения с бесконечно удалённой прямой). Тогда $v = \pm u$, т. е. получим две точки $(1, 1, 0)$ и $(1, -1, 0)$ [1]). Обе они имеют рациональные координаты. Такие точки называют *рациональными бесконечно удалёнными*.

Вернёмся к подстановке Диофанта. Уравнение (9) в однородных координатах запишется так:

$$v^2 = a^2u^2 + buz + cz^2. \qquad (9')$$

[1]) Поскольку $v = u$ либо $v = -u$, то эти точки будут иметь вид $(u, u, 0)$ и $(u, -u, 0)$. Умножая на $1/u$, получим $(1, 1, 0)$ и $(1, -1, 0)$.

Точки $(1, a, 0)$ и $(1, -a, 0)$ будут её рациональными бесконечно удалёнными точками. Проведём через первую из них прямую. Общее уравнение прямой в однородных координатах имеет вид

$$Au + Bv + Cz = 0.$$

Но наша точка лежит на этой прямой, т. е.

$$A \cdot 1 + B \cdot a + C \cdot 0 = 0.$$

Значит, можно положить $A = ka$, $B = -k$, $C = km$, где m произвольно. Таким образом, уравнение искомой прямой будет

$$au - v + mz = 0,$$

или, снова переходя к аффинным координатам, получим

$$y = ax + m.$$

Но это и есть подстановка, применённая Диофантом. Итак, она эквивалентна проведению произвольной прямой через рациональную бесконечно удалённую точку кривой (9). Оговоримся сразу же, что мы вовсе не считаем, будто Диофант имел понятие о бесконечно удалённых точках кривой. Он просто пользовался эквивалентными соображениями. В истории математики нам известно немало примеров, когда основные факты некоторой теории были найдены до возникновения самой теории и до возникновения её основных понятий. Так было, например, с арифметикой квадратичных полей, которая была построена Эйлером, Лагранжем и Гауссом до введения квадратичных полей и даже до появления понятия алгебраического числа. Это было сделано в рамках теории квадратичных форм, но открытые там факты были эквивалентны арифметике квадратичных полей.

Так было и в «Арифметике» Диофанта, где некоторые общие предложения алгебраической геометрии были открыты и изучены, но без геометрической интерпретации, в рамках чистой алгебры и теории чисел.

Зададимся теперь вопросом, знал ли Диофант, что число решений поставленных им задач бесконечно? Или он, действительно, довольствовался нахождением одного рационального решения?

В книге II он ничего не говорит об этом и бесконечность решений можно усмотреть только из метода Диофанта. Однако в задаче 19 книги III он пишет: «мы уже знаем, что заданный квадрат можно разбить на два квадрата бесконечным числом способов». Далее, задачу 19 книги IV Диофант формулирует так:

> «Найти общие (или неопределённые) выражения для трёх чисел таких, что произведение любых двух из них вместе с единицей давало бы квадрат».

Диофант находит эти выражения в виде $x + 2$, x и $4x + 4$ и пишет:

> «Итак, проблема решена с помощью общих выражений (или в неопределённом виде), так что произведение любых двух из них вместе с единицей даёт квадрат, как бы ни было выбрано x. Ибо найти общие (или неопределённые) выражения означает дать такую формулу, что, каково бы ни было значение x, после его подстановки удовлетворяются условия (задачи)».

Заметим, что методы Диофанта для решения неопределённых уравнений

$$y^2 = ax^2 + bx + c$$

совпадают с так называемыми «подстановками Эйлера», которые хорошо известны каждому, изучавшему математический анализ. И там и тут x и y выражаются с помощью рациональных функций от одного параметра; делается это с помощью одних и тех же подстановок, только при вычислении интеграла $\int \dfrac{dx}{\sqrt{ax^2 + bx + c}}$ нам не нужно требовать, чтобы коэффициенты этих функций сами были рациональными числами. Поэтому можно положить

$$y = \sqrt{a}\,x + t \qquad \text{или} \qquad y = xt + \sqrt{c}.$$

У Диофанта же, поскольку речь шла о рациональных точках, все подстановки должны были иметь рациональные коэффициенты. Поэтому ему приходилось учитывать это добавочное требование.

§ 6. НЕОПРЕДЕЛЁННЫЕ УРАВНЕНИЯ ТРЕТЬЕГО ПОРЯДКА

В книге IV Диофант рассматривает неопределённые уравнения третьего и четвёртого порядков. Здесь дело обстоит гораздо сложнее: если кривая третьего порядка и имеет рациональные точки, то координаты их, вообще говоря, не могут быть выражены рациональными функциями одного параметра. Однако, зная одну или две рациональные точки кубической кривой, можно найти ещё одну её рациональную точку. Действительно, любая прямая пересекает кривую третьего порядка в трёх точках, координаты которых можно найти например, из уравнения третьей степени, получающегося исключением y из уравнений кривой Γ:

$$f_3(x, y) = 0 \tag{10}$$

и прямой. Если два корня этого результирующего уравнения рациональны, то и третий будет рациональным (это можно усмотреть хотя бы из того, что сумма корней кубического уравнения равна коэффициенту при x^2, взятому с обратным знаком, делённому на коэффициент при x^3; если коэффициенты уравнения рациональны и два корня рациональны, то и третий корень, очевидно, рационален). На этом замечании основаны следующие две процедуры:

1) если P — рациональная точка кривой Γ, то в точке P проводится к кривой Γ касательная с рациональным угловым коэффициентом k. Она будет иметь ещё одну точку пересечения с Γ, которая также будет рациональной. (Действительно, решая совместно уравнение касательной и кривой, получим результирующее кубическое уравнение, которое имеет двойной рациональный корень, значит, и третий его корень будет рациональным.)

2) Если P_1 и P_2 — рациональные точки кривой Γ, то проводится прямая P_1P_2 и ищется третья её точка пересечения с Γ. По предыдущему, координаты этой точки рациональны.

В дальнейшем будем называть эти способы *методами касательной* и *секущей* Диофанта. Покажем, что мы имеем право

приписать оба эти метода Диофанту. Для этого рассмотрим его задачи.

Задача 24 книги IV:

> «Данное число разбить на два числа так, чтобы их произведение было равно кубу без стороны.
>
> Пусть дано 6. Я полагаю 1-е число x, тогда 2-е будет $6-x$. Остаётся сделать, чтобы одно на другое было кубом без стороны, но оно будет $6x - x^2$; это и должно равняться кубу без стороны. Я образую куб из x с каким-нибудь коэффициентом минус 1; пусть $2x - 1$, его куб минус сторона будет
>
> $$8x^3 + 4x - 12x^2.$$
>
> Это равно $6x - x^2$.
>
> Если коэффициенты при x в обеих частях были бы равны, то остались бы равные члены с x^3 и x^2; тогда x было бы рациональным. Но $4x$ получается как избыток $3 \cdot 2x$ над $2x$; и $3 \cdot 2x - 2x$ даёт $2 \cdot 2x$; однако, по предположению, должно быть 6. Итак, дело сводится к отысканию такого числа, чтобы коэффициент при x, умноженный на 2, давал бы 6. Это будет 3.
>
> Так как я хочу, чтобы $6x - x^2$ равнялось кубу минус сторона, то полагаю сторону куба $3x - 1$; этот куб минус его сторона будет
>
> $$27x^3 + 6x - 27x^2 = 6x - x^2 \qquad \text{и} \qquad x = \tfrac{26}{27}\,.$$
>
> По формулам: 1-е $= \frac{26}{27}$, 2-е $= \frac{136}{27}$ ».

Постараемся теперь выделить метод Диофанта в чистом виде. Пусть задано число a. Обозначим одно из искомых чисел x, другое $a - x$. По условию,

$$x(a - x) = y^3 - y. \tag{11}$$

Одним из рациональных решений будет $(0, -1)$. Следуя Диофанту, проведём через эту точку прямую

$$y = kx - 1 \tag{$*$}$$

(Диофант берёт сначала $k = 2$) и найдём её точки пересечения с кривой (11):

$$ax - x^2 = k^3x^3 - 3k^2x^2 + 2kx.$$

Для того чтобы x получилось рациональным, достаточно положить

$$2k = a, \qquad \text{т. е.} \qquad k = \frac{a}{2}, \tag{$**$}$$

что и делает Диофант. После этого найдём

$$x = \frac{3k^2 - 1}{k^3} = 2\,\frac{3a^2 - 4}{a^3}.$$

Посмотрим, что означает условие $(**)$ для прямой $(*)$. Для того чтобы это выяснить, применим метод Диофанта к произвольному уравнению третьего порядка от двух переменных (10), которое имеет рациональное решение (a, b): $f_3(a, b) = 0$. Проведём через точку $P(a, b)$ прямую

$$y - b = k(x - a) \tag{12}$$

или

$$\begin{cases} x = a + t, \\ y = b + kt. \end{cases} \tag{13}$$

Тогда

$$f_3(a + t, b + kt) = f_3(a, b) + tA(a, b) + ktB(a, b) + \\ + t^2C(a, b, k) + t^3D(a, b, k) = 0.$$

Но $f_3(a, b) = 0$ и, если положить

$$A(a, b) + kB(a, b) = 0, \tag{14}$$

то получим

$$k = -\frac{A(a, b)}{B(a, b)} = -\frac{\dfrac{\partial f_3}{\partial x}}{\dfrac{\partial f_3}{\partial y}}(P),$$

т. е. угловой коэффициент нашей прямой (12) должен быть выбран так, чтобы она была касательной к кривой (10) в точке $P(a, b)$. Таким образом, здесь Диофант пользуется методом касательной.

Этим же способом Диофант решает задачу 18 книги VI, а также, вероятно, и задачу

$$x^3 + y^3 = a^3 - b^3,$$

рассмотренную, по свидетельству самого Диофанта, в его книге «Поризмы», которая до нас не дошла.

Заметим, что попутно Диофант получает чисто алгебраический способ определения углового коэффициента k касательной, равного производной $\frac{dy}{dx}$ или

$$\frac{dy}{dx} = -\frac{\frac{\partial f_3}{\partial x}}{\frac{\partial f_3}{\partial y}}.$$

Этот способ, который не требует предельного перехода, т. е. может быть осуществлен чисто алгебраически (над полем без топологии), сыграл большую роль в историческом процессе формирования призводной, особенно у Ферма и Декарта, а в настоящее время широко применяется в алгебраической геометрии.

Перейдём теперь к задаче 26 книги IV, где применяется метод секущей.

> «Найти два числа, произведение которых вместе с каждым из них будет кубом.
>
> Положим первое x с каким-нибудь коэффициентом, равным кубу, пусть 8; второе x^2-1. Одно условие удовлетворено, ибо прибавление к произведению первого даёт куб.
>
> Остаётся сделать так, чтобы при прибавлении к тому же второго тоже получался куб. Но прибавление второго даёт
>
> $$8x^3 + x^2 - 8x - 1 = \text{кубу}.$$
>
> Образуем куб из $2x-1$, что даёт $x = \frac{14}{13}$. Далее, по формулам: первое $\frac{112}{13}$, второе $\frac{27}{169}$ ».

Обозначим, следуя Диофанту, первое неизвестное через a^3x, второе через $x^2 - 1$. Тогда первое условие задачи выполнено, а второе даёт:

$$a^3x^3 + x^2 - a^3x - 1 = y^3. \tag{15}$$

Диофант делает подстановку $y = ax - 1$ и получает

$$x = \frac{a^3 + 3a}{1 + 3a^2}.$$

Остановимся несколько подробнее на применённом здесь методе. Одним из рациональных решений уравнения (15) будет $(0, -1)$. Проведём через эту точку прямую $y = kx - 1$ и

найдём её точки пересечения с (15):

$$(a^3 - k^3)x^3 + (1 + 3k^2)x^2 - (a^3 + 3k)x = 0.$$

Диофант приравнивает нулю не коэффициент при x, как это имело место в предыдущем случае, а коэффициент при x^3 и получает

$$a^3 - k^3 = 0, \qquad k = a.$$

Что означает такое приравнивание с геометрической точки зрения? Для выяснения этого вопроса запишем уравнение (15) в однородных координатах, положив $x = \frac{u}{z}$, $y = \frac{v}{z}$:

$$a^3u^3 + u^2z - a^3uz^2 - z^3 = v^3. \qquad (15')$$

Мы видим, что эта кривая имеет две рациональные точки $P_1(0, -1, 1)$ и $P_2(1, a, 0)$; соединяющая их прямая есть

$$v = au - z.$$

Она-то и даёт в пересечении с (15′) третью рациональную точку. Таким образом, здесь Диофант применяет метод секущей для случая, когда одна из заданных рациональных точек является конечной, а другая — бесконечно удалённой, или несобственной.

Диофант применяет свои методы касательной и секущей и в других задачах книг IV, V и VI.

§ 7. ДИОФАНТ И ТЕОРИЯ ЧИСЕЛ

В тех книгах «Арифметики», которыми мы располагаем, исследования по теории чисел, в собственном смысле слова, отсутствуют. Однако, ставя некоторые задачи или решая их, Диофант иногда формулирует, при каких условиях эта задача возможна или невозможна [1]), или отмечает, что некоторое полученное в процессе решения число невозможно представить в том или ином виде, например, как сумму двух квадратов. Именно таким образом и появляются в «Арифметике» теоремы теории чисел. Судя по одному замечанию самого Диофанта все эти и другие теоремы такого рода были им рас-

[1]) Такое ограничительное условие называлось у древних *диоризмом*.

смотрены в специальной книге «Поризмы», которая до нас не дошла.

Поэтому нам ничего другого не остаётся, как судить о знаниях Диофанта в теории чисел на основании замечаний и диоризмов, имеющихся в «Арифметике». Начнём с задачи 19 книги III.

«Найти четыре числа такие, чтобы квадрат суммы их, если к нему прибавить одно из них, или отнять, оставался бы квадратом.

Так как во всяком прямоугольном треугольнике, если к квадрату гипотенузы прибавить или из него отнять удвоенное произведение сторон, заключающих прямой угол, получится квадрат, то я ищу сперва четыре прямоугольных треугольника, имеющих равные гипотенузы. Это то же, что разбить некоторый квадрат на два квадрата (четырьмя способами), а мы уже знаем, что заданный □ можно разбить на два квадрата бесконечным числом способов (ἀπειραχῶς — *апейрахос*).

Итак, пусть предложены два прямоугольных треугольника в наименьших числах, как 3, 4, 5 и 5, 12, 13. Умножим каждый из предложенных на гипотенузу другого; тогда первый треугольник будет 39, 52, 65, а второй 25, 60, 65. Это и есть прямоугольные треугольники, имеющие равные гипотенузы.

По своей природе 65 может быть разложено на два квадрата двумя способами: на 16 и 49, и по-другому, на 64 и 1. Это происходит потому, что число 65 есть произведение 13 и 5, каждое из которых разбивается на два квадрата.

Теперь от предложенных 49 и 16 я беру стороны, они будут 7 и 4, и образую из двух чисел 7 и 4 прямоугольный треугольник 33, 56, 65.

Подобным образом 64 и 1 имеют стороны 8 и 1, и я образую из них другой прямоугольный треугольник, стороны которого будут 16, 63, 65.

И вот получены четыре прямоугольных треугольника, имеющих равные гипотенузы. Итак, вернёмся к первоначальной задаче; я полагаю сумму четырёх (чисел) $65x$, а каждое из этих четырёх равным x^2 с коэффициентами, являющимися учетверёнными площадями, именно, первое — $4056x^2$, второе — $3000x^2$, третье — $3696x^2$ и четвёртое — $2016x^2$.

Тогда сумма четырёх чисел

$$12768x^2 \quad \text{равна} \quad 65x,$$

что даёт

$$x = \tfrac{65}{12\,768}\,.$$

По формулам будут с одним и тем же знаменателем первое — 17 136 600, второе — 12 675 000, третье — 15 615 600, четвёртое — 8 517 600, а знаменатель (равен) 163 021 824».

Эта задача замечательна во многих отношениях. Во-первых, здесь Диофант впервые говорит о прямоугольных треугольниках «в наименьших числах» и об образовании таких треугольников из «двух чисел». На самом деле речь, конечно, идёт о решении в рациональных числах неопределённого уравнения

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

о котором мы говорили в § 5. Наиболее общие формулы для его решения привёл Евклид в «Началах». Диофант без специальных оговорок пользуется этими формулами, дающими при взаимно простых p и q все целые решения этого уравнения, не имеющие общего делителя:

$$z = p^2 + q^2, \qquad x = 2pq, \qquad y = p^2 - q^2.$$

(Поскольку уравнение однородно, то расширение области решения до поля рациональных чисел не даёт тут ничего нового.) Эти решения можно получить тем же методом, который Диофант применил в задаче 8 книги II для разложения заданного квадрата в сумму двух квадратов (см. § 5).

Во-вторых, она содержит утверждение, что произведение двух целых чисел, каждое из которых является суммой двух квадратов, само представимо суммой двух квадратов и притом по крайней мере двумя различными способами (если только перемножаемые числа не равны между собой). При этом, если $p = a^2 + b^2$ и $q = c^2 + d^2$, то

$$pq = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2.$$

Именно в примечаниях к этой задаче Ферма высказал своё знаменитое утверждение, что каждое простое число вида $4n+1$ представимо в виде суммы двух квадратов и притом только одним способом. Здесь же он дал приём для определения, сколькими способами заданное число можно представить в виде суммы двух квадратов.

Были ли известны эти предложения Диофанту? Для ответа на этот вопрос рассмотрим ещё одну задачу Диофанта, снабженную диоризмом, говорящим о представимости некоторого числа суммой двух квадратов — задачу 9 книги V.

> «Разделить единицу на две дроби так, чтобы прибавление к каждой из частей заданного (числа) делало бы его квадратом».

Вслед за условием Диофант формулирует ограничение (диоризм), которое надо наложить на заданное число, чтобы задача была возможной. К сожалению, после слов: «Необходимо, чтобы заданное число не было бы нечётным и чтобы удвоенное от него и единица...» текст испорчен. Существует несколько реконструкций его, о которых мы скажем позже. Но сначала приведём текст задачи.

> «Пусть предложено к каждой части прибавить 6 так, чтобы получились квадраты.
>
> Так как мы хотим разбить 1 на такие части, чтобы при прибавлении к каждой из них 6 получился $\square$, то сумма квадратов будет 13. Таким образом, требуется разбить 13 на два квадрата, каждый из которых больше, чем 6.
>
> Если теперь я разобью 13 на два квадрата, разность которых меньше 1, то я решу требуемое. Я беру половину от 13, получится $6\frac{1}{2}$, и ищу дроби, которые при прибавлении к $6\frac{1}{2}$ дают квадраты. Всё учетверим. Итак, я ищу квадратную дробь, которая при прибавлении к 26 давала бы $\square$. Если прибавляемая дробь $\frac{1}{x^2}$, то получим
>
> $$26 + \tfrac{1}{x^2} = \square.$$
>
> Всё на x^2. Получаем $26x^2 + 1 = \square$: пусть его сторона $5x + 1$, и получим $x = 10$.
>
> Итак, $x^2 = 100$, $\frac{1}{x^2} = \frac{1}{100}$.
>
> Значит, прибавляемое к 26 будет $\frac{1}{100}$, а значит, к $6\frac{1}{2}$ получим прибавляемое $\frac{1}{400}$, что даст $\square$ со стороной $\frac{51}{20}$.
>
> Итак, необходимо разбить 13 на два квадрата, построив для каждого сторону, приближенно равную $\frac{51}{20}$, и я ищу, что вычтенное из трёх и прибавленное к двум даст именно $\frac{51}{20}$.
>
> Итак, я образую два квадрата, один из $11x + 2$, другой из $3 - 9x$, тогда сумма их квадратов будет
>
> $$202x^2 + 13 - 10x = 13$$
>
> и получим $x = \frac{5}{101}$.

> Значит, будет сторона одного квадрата $\frac{257}{101}$, а другого $\frac{258}{101}$. И если из каждой из них в квадрате удалить 6, то получим одну часть единицы $\frac{5358}{10201}$, другую $\frac{4843}{10201}$, и ясно, что каждая вместе с 6 даст □».

Условия задачи мы можем записать в виде системы трёх уравнений:

$$\begin{cases} x + y = 1, \\ x + a = u^2, \\ y + a = v^2. \end{cases}$$

Складывая два последние уравнения, получим

$$2a + 1 = u^2 + v^2.$$

Поэтому число a должно быть выбрано так, чтобы $2a + 1$ представлялось в виде суммы двух квадратов. Общие условия для того, чтобы число нельзя было представить в виде суммы двух квадратов, целых или дробных, после Диофанта были найдены только Пьером Ферма (XVII век), который сформулировал их следующим образом:

> «Если число после деления на наибольший содержащийся в нём квадрат даёт частное, которое делится на простое число вида $4n - 1$, то заданное число не будет квадратом и не может быть разложено в сумму двух целых или дробных квадратов».

Эти условия могут быть выведены из одной замечательной теоремы, которую сформулировал Ферма, а доказал Эйлер, а именно: суммой двух квадратов представимы те и только те простые числа, которые имеют вид $4n + 1$.

Знал ли Диофант доказательство своего диоризма и подозревал ли он о том, что выставленные им условия не только необходимы, но и достаточны для представимости целого числа суммою двух квадратов?

Этому вопросу посвятил специальное исследование один из знаменитых математиков XIX века, младший современник Гаусса, Карл Густав Якоб Якоби (1804–1851). Прежде всего, он провёл тщательный филологический анализ текста Диофанта и предложил следующую его реконструкцию:

«Необходимо, чтобы заданное число не было нечётным, и чтобы удвоенное его и единица не имело делителя, кратного четырём без единицы».

Примерно так же этот текст был впоследствии восстановлен большим знатоком античности и издателем Диофанта Полем Таннери (издание 1893 года).

Это условие действительно будет необходимо, если к нему прибавить оговорку «после деления на наибольший содержащийся в нём квадрат», но, по-видимому, Диофант подразумевает это. В таком случае условие будет и достаточным, т. е. будет полностью характеризовать множество целых чисел, представимых суммой двух квадратов.

Якоби полагает, что Диофант имел доказательство того, что высказанное им условие является необходимым, т. е. умел обосновать свой диоризм. Он приводит в своей статье реконструкцию этого доказательства, пользуясь при этом только методами, которые применяли в своих работах Евклид и Диофант.

Якоби не сомневается в том, что Диофант знал и о достаточности своих условий, однако не мог этого доказать, так как для этого нужны были средства, выходящие за пределы античной математики.

В задаче 14 книги V Диофант сформулировал условие, необходимое для того, чтобы некоторое число могло быть представлено суммой трёх квадратов. Диоризм заключается в том, что число не должно иметь вид $8n+7$. И здесь доказательство необходимости не должно было составить труда для Диофанта, однако он нигде не утверждает, что всякое нечётное число, не имеющее вид $8n+7$, действительно представляется суммой трёх квадратов, хотя мог чисто индуктивно найти и это предложение. Зная принцип математиков древности высказывать только такие предложения, которые они могли доказать, можно смело утверждать, что Диофант умел доказывать все свои диоризмы. А это значит, что он был не только гениальным алгебраистом, не только основателем диофантова анализа, но и выдающимся исследователем в области собственно теории чисел.

§ 8. ДИОФАНТ И МАТЕМАТИКИ XV–XVI ВЕКОВ

Комментировать Диофанта начали ещё в древности. Разбору его книг были посвящены труды знаменитой Гипатии, дочери александрийского учёного Теона. Гипатия жила в конце IV–начале V века н. э. в Александрии и славилась там как блестящий оратор и знаток философии Платона.

Сочинения Гипатии до нас, к сожалению, не дошли.

После Гипатии мы не знаем ни одного александрийского математика. Последние греческие учёные Прокл, Исидор и Симпликий развивали своё учение уже не в Александрии, а в Афинах. Но и здесь к началу VII века научная мысль угасла. Античная наука погибла вместе с гибелью античного общества. В IX–XIII веках возникли новые научные центры: Константинополь, а также Багдад и другие города арабского Востока. Отсюда начиная с XII века научная мысль проникала в Европу. Идеи Диофанта шли двумя различными потоками. Первый из них можно назвать алгебраическим, второй — теоретико-числовым или арифметическим. При этом то новое, что внёс Диофант в алгебру, стало известно учёным Европы лет на 300 раньше, чем его арифметические идеи. Это и неудивительно. Новая алгебра и была воспринята как византийскими комментаторами Диофанта (Максим Плануда, Георгий Пахимер, жившие в XIII веке), так и арабскими математиками, особенно Абуль Вафой (X век) и его школой. Правда, арабы не пользовались буквенными символами, а именовали степени неизвестного словами. Кроме того, при наименовании степеней неизвестного они пользовались не аддитивным принципом, как это делал Диофант, а неудобным мультипликативным, т. е., например, x^6 они называли не «кубо-кубом», как Диофант, а «квадрато-кубом», а для x^5 они вообще не могли составить название из предыдущих степеней, поскольку 5 — число простое и на множители не раскладывается. Приходилось называть его «глухим» или «первым невыразимым». Аналогично дело обстояло с x^7, который называли «вторым невыразимым», далее, с x^{11} и всеми степенями с простыми показателями. Такой принцип обозначения перешёл от арабов в Европу и им пользовались в эпоху Возрождения в Италии,

а затем и немецкие алгебраисты, известные под именем коссистов. Исключение составил очень талантливый математик XIII века, современник Данте, Леонардо Пизанский. В своей знаменитой «Книге об абаке» (Liber abaci) он не только применил аддитивный принцип обозначения степеней неизвестного, но и впервые в Европе рассмотрел задачи, сводящиеся к неопределённым уравнениям.

Что касается правил Диофанта оперирования с многочленами и уравнениями, то они повторялись почти всеми алгебраистами средних веков.

Отрицательные числа были восприняты гораздо менее охотно. Арабские математики вообще от них отказались, а европейцы принимали их с большим недоверием. Долгое время они именовали отрицательные числа «ложными числами» и старались обходиться без них.

Но в «Арифметике» Диофанта имелся и другой, гораздо более глубокий круг идей, связанный с решением неопределённых уравнений, с диофантовым анализом. Долгое время о них ничего не знали. В XV–XVI веках в Европе сложилась несколько парадоксальная ситуация: учёные пользовались буквенной алгеброй, восходящей к Диофанту, развивали её дальше, но не были знакомы с трудами Диофанта.

Первым прочёл их, по-видимому, известный астроном XV века Регионтан (Иоганн Мюллер). Путешествуя по Италии, он открыл рукопись Диофанта в Венеции и сообщил об этом в письме к своему другу. Рукопись поразила его богатством содержания. Он решил перевести её, но не раньше, чем найдёт все 13 книг, о которых пишет Диофант во Введении. Однако, были найдены только 6 книг, те, которые известны и нам, и перевод так и не был сделан.

Прошло ещё 100 лет. За это время ни один из крупных алгебраистов, а их было немало, — достаточно назвать Джироламо Кардано и Николо Тарталья, ничего не знали о Диофанте. Но вот в 1572 году в «Алгебре» Рафаэля Бомбелли, профессора университета в Болонье, вдруг появляются 143 задачи из «Арифметики» Диофанта! В предисловии Бомбелли пишет, что «в прошлом году труд, посвящённый этому предмету, был найден в библиотеке Господа нашего в Ватикане, со-

ставленный неким Диофантом, греческим автором, жившим в эпоху Антонина Пия». Заметим, что Антонин Пий был Римским императором в середине II века н. э. Откуда взял своё утверждение о времени жизни Диофанта Бомбелли, абсолютно не известно. Прочтя рукопись, Бомбелли убедился, что автор её «весьма сведущ в науке чисел». И вот «с целью обогатить мир произведением такой важности» Бомбелли принялся совместно с римским математиком Пацци, который первый обнаружил рукопись, за перевод. «Мы перевели пять книг из семи,— сообщает Бомбелли,— но не смогли окончить остальное из-за других работ, которые выпали на нашу долю». О каких семи книгах идёт речь? Ватиканская рукопись содержит их только шесть! Может быть, седьмая была утеряна? Если бы до нас дошёл перевод пяти первых книг, выполненный Бомбелли и Пацци, мы могли бы сравнить их с теми книгами, которые мы имеем, и судить о том, соответствует ли наше разделение задач по книгам тому, которое было у Бомбелли. Но, увы, никаких следов этого перевода не осталось.

«Алгебра» Бомбелли замечательна во многих отношениях. Здесь были усовершенствованы алгебраические обозначения для степеней неизвестного, здесь впервые появились мнимые числа $a + bi$, где $i^2 = -1$, причём очень чётко были сформулированы правила действий с ними. Наконец, с помощью мнимых чисел был исследован так называемый «неприводимый» случай кубического уравнения. Но для нас сейчас книга Бомбелли важна тем, что в ней впервые появились задачи Диофанта, правда, вырванные из контекста. Однако влияние «Арифметики» сказалось на всей книге Бомбелли: в первоначальной рукописи его собственные задачи были облечены в псевдопрактическую форму, в окончательном варианте они формулируются абстрактно, как и у Диофанта. Он изменил и некоторые термины, приблизив их к тем, которые нашёл у Диофанта.

Но уже через три года после выхода в свет «Алгебры» был опубликован первый перевод «Арифметики» на латынь. Он был выполнен известным филологом и философом того времени Ксиландром (настоящее имя его — Гильом Хольцман). Перевод этот был, в целом, хорош, хотя чувствовалось, что он

был выполнен человеком, далёким от математики.

После этого задачи четырёх первых книг Диофанта появились в книге известного математика и механика Симона Стевина (1585 год), а во втором издании, подготовленном талантливым алгебраистом Альбером Жираром,— и задачи из последних двух книг.

Но методы Диофанта обрели новую жизнь только в произведениях двух крупнейших математиков Франции XVI–XVII веков — Франсуа Виета и Пьера Ферма.

§ 9. МЕТОДЫ ДИОФАНТА У ВИЕТА И ФЕРМА

Франсуа Виет (1540–1603) по праву считается родоначальником буквенного исчисления, до создания которого говорить об алгебре можно только с известными оговорками. Он первый после Диофанта сделал существенно новый шаг в построении такого исчисления и именно тем, что ввёл символы для произвольных постоянных величин (или параметров), фигурирующих в задачах. Только после этого появились первые алгебраические формулы и стало возможным часть умственных операций заменить буквенными.

Франсуа Виет был также первым математиком Европы, обратившим внимание на метод Диофанта для нахождения рациональных точек кубической кривой и хорошо понявшим этот метод.

В задаче 12 книги V Диофант пишет: «а мы имели в Поризмах, что разность любых двух кубов есть сумма двух кубов». Очевидно, речь идёт о решении уравнения

$$x^3 + y^3 = a^3 - b^3, \qquad (*)$$

где $a > b > 0$ и x, y — положительные. Однако, решение этой задачи в самой «Арифметике» отсутствует.

В своей книге, носящей странное название «Зететика», — слово, придуманное автором для обозначения науки о приведении различных проблем к уравнениям, — Виет ставит ещё две аналогичные задачи:

1) $x^3 - y^3 = a^3 + b^3$ $\qquad (x > y > 0,\ a > 0,\ b > 0)$,
2) $x^3 - y^3 = a^3 - b^3$ $\qquad (x > y > 0,\ a > b > 0)$.

Все три задачи он решает с помощью метода касательной Диофанта. Так, например, для решения задачи $(*)$ Виет полагает

$$x = t - b, \qquad y = a - kt$$

и получает после подстановки

$$t^3(1 - k^3) + 3t^2(ak^2 - b) + 3t(b^2 - a^2k) = 0.$$

Затем он требует, чтобы $b^2 - a^2k = 0$, что равносильно требованию, чтобы прямая $y = a - k(x + b)$ была касательной к кривой $(*)$ в точке $(-b, a)$, и находит

$$t = \frac{3a^3b}{a^3 + b^3}\,.$$

Аналогично решаются и две другие задачи.

Впоследствии Ферма добавил к трём задачам Виета ещё одну,

$$x^3 + y^3 = a^3 + b^3.$$

Она вызывала затруднения, так как при её решении обычным способом либо x либо y получаются отрицательными, т. е. сумма двух кубов представляется не суммой двух новых кубов, а их разностью. Ферма вышел из затруднения, осуществив при помощи подстановки $x = t + l$ сдвиг всей кривой. Он очень гордился этим, называя такой сдвиг, который он применял и в других случаях, «мой метод».

В 1621 году Баше де Мезириак выпустил новое издание «Арифметики» Диофанта. Впервые был опубликован не только перевод на латынь (сделанный заново и имеющий значительные преимущества по сравнению с переводом Ксиландра), но и греческий текст. Однако это издание стало знаменитым не только благодаря качеству перевода и обстоятельным комментариям Баше, — на одном из его экземпляров Пьер Ферма записывал свои мысли и результаты, относящиеся к теории чисел. Именно здесь, на полях напротив задачи 8 книги II, в которой Диофант раскладывает заданный квадрат в сумму двух квадратов (см. § 5), Ферма записал: «Наоборот, невозможно разложить куб на два куба, биквадрат на два биквадрата и вообще никакую степень, бóльшую квадрата,

на две степени с тем же показателем. Я дал этому поистине чудесное доказательство, но поля книги слишком узки для него». Это и есть знаменитая Большая или Великая теорема Ферма, прославившая имя своего автора далеко за пределами математики. Но и в самой нашей науке Великая теорема сыграла совершенно исключительную роль. Она служила предметом раздумий и исследований для Эйлера, Лежандра, Дирихле, Куммера и других крупнейших математиков и побудила их к построению новой области математики — высшей арифметики или арифметики полей алгебраических чисел.

Но кто же был автором Великой теоремы? Что мы о нём знаем? Несколько больше, чем о Диофанте, но гораздо меньше, чем о других его современниках.

Пьер Ферма родился в 1601 году на юге Франции близ Тулузы в зажиточной семье, принадлежащей к третьему сословию. Ферма получил хорошее образование: он прекрасно владел латынью, итальянским и испанским, причём писал на этих языках и по-французски изящные стихи. Греческий он знал настолько хорошо, что делал поправки ко многим учёным переводам (в том числе и к переводу Диофанта) и мог бы прославиться как знаток эллинизма. Получив юридическое образование, Ферма занял место советника Парламента (т. е. суда) города Тулузы. Здесь прошла почти вся его жизнь, которая внешне, вероятно, протекала как и у его сотоварищей по суду, как у многочисленных его родственников-коммерсантов. Ферма женился, имел пятерых детей, редко выезжал из Тулузы... Однако, эта размеренная и тихая с виду жизнь на самом деле была напряжённой и полной бурь. Истинным её содержанием была математика, которую он полюбил, читая древних: Архимеда, Аполлония, Диофанта. Одной из первых математических работ Ферма была реконструкция утерянного трактата Аполлония «О плоских местах», о котором было известно из сообщений Паппа Александрийского. С тех пор математика завладела им. Это особенно хорошо видно из его переписки. Живя вдалеке от научных центров того времени, Ферма вынужден был излагать свои результаты и ставить проблемы в письмах. Их сохранилось более ста. Они до сих пор читаются с захватывающим интересом — они

дышат страстью к познанию математических истин, которая некогда с такой силой охватила их автора.

Ферма бесспорно был первым математиком своего времени. Он создал наиболее общие новые методы той части нашей науки, которая получила название анализа бесконечно малых, наряду с Декартом он был творцом аналитической геометрии, вместе с Паскалем заложил основы теории вероятностей. Как и все учёные его времени, Ферма живо интересовался приложениями математики к анализу явлений физического мира. Он занимался оптикой, где с помощью принципа минимума, носящего теперь его имя, сумел объяснить, как движется луч света в неоднородной среде.

Но любимой областью Ферма была теория чисел. И здесь он не имел себе равных. Он сумел выбрать среди множества интересных вопросов и частных задач те основные проблемы, исследование которых и создало теорию чисел как науку. Проблемами Ферма занимались все крупные математики XVIII и XIX веков, от Эйлера и до Гильберта.

Мы говорим о «проблемах», а не о «теоремах», потому что большинство утверждений Ферма дошло до нас без доказательств: они сформулированы либо на полях его экземпляра «Арифметики» Диофанта, либо в письмах, где предлагается другим учёным попробовать свои силы для их обоснования. Исключение составляет только Великая теорема для биквадратов, доказательство которой он записал. Зато Ферма подробно описал новый общий метод доказательства теоретико-числовых предложений, который сам он назвал «методом бесконечного или неопределённого спуска». Приведём выдержку из письма Ферма, в которой он описывает новый метод:

> «...Поскольку обычные методы, которые изложены в книгах, недостаточны для доказательства столь трудных предложений (речь идёт о теоремах теории чисел, И. Б.), я нашёл совершенно особый путь для того, чтобы достичь этого.
>
> Я назвал этот способ доказательства *бесконечным* или *неопределённым спуском*; вначале я пользовался им только для доказательства отрицательных предложений, как-то:
>
> что не существует числа, меньшего на единицу кратного трёх, которое составлялось бы из квадрата и утроенного квадрата;

что не существует прямоугольного треугольника в целых числах, площадь которого была бы квадратным числом. Доказательство проводится путём приведения к абсурду таким способом:

Если бы существовал какой-нибудь прямоугольный треугольник в целых числах, который имел бы площадь, равную квадрату, то существовал бы другой треугольник, меньший этого, который обладал бы тем же свойством. Если бы существовал второй, меньший первого, который имел бы это же свойство, то существовал бы в силу подобного рассуждения третий, меньший второго, который имел бы то же свойство, и, наконец, четвёртый, пятый, спускаясь до бесконечности. Но если задано число, то не существует бесконечности по спуску меньших его (я все время подразумеваю целые числа). Откуда заключают, что не существует никакого прямоугольного треугольника с квадратной площадью» [1]).

Заметим, что предложение о площади прямоугольного треугольника, стороны которого выражаются в целых числах, на примере которого Ферма демонстрирует свой метод, равносильно тому, что не существует двух биквадратов, разность которых была бы квадратом. Значит, тем более эта разность не может быть биквадратом. Таким образом, из этого предложения следует Великая теорема для биквадратов. Доказательство этого предложения, выполненное методом спуска, до нас дошло. Это и есть единственное теоретико-числовое доказательство Ферма, которым мы располагаем. Впоследствии с помощью метода спуска Эйлер доказал Великую теорему для $n = 3$ и $n = 4$.

В наши дни метод спуска Ферма сделался незаменимым орудием при исследовании проблем диофантова анализа. Однако применение этого метода к проблемам, относящимся к рациональным точкам кривой или некоторого другого многообразия, потребовало введения нового понятия «высоты точки».

Пусть, например, дано неопределённое уравнение

$$f(x, y) = 0, \qquad (*)$$

относительно которого требуется доказать, что оно не имеет решений в рациональных числах. Для доказательства пе-

[1]) Это письмо к Каркави опубликовано в Oeuvres de Fermat, Париж, 1891, т. II, стр. 43.

рейдём к однородным координатам, положив

$$x = \frac{u}{z}, \qquad y = \frac{v}{z};$$

получим

$$\Phi(u, v, z) = 0. \qquad (**)$$

Каждому рациональному решению $(*)$ отвечает решение $(**)$ в целых числах. Поэтому достаточно показать, что уравнение $(**)$ не имеет ни одного целочисленного решения.

Так, например, если уравнение $(*)$ имеет вид

$$Ax^n + By^n = C,$$

то уравнение $(**)$ будет

$$Au^n + Bv^n = Cz^n.$$

Пусть теперь u, v, z — решение $(**)$ в целых числах. Назовём тогда *высотой* точки (u, v, z) наибольшее из чисел $|u|$, $|v|$, $|z|$. Чтобы провести «спуск», надо доказать, что если уравнению $(**)$ удовлетворяют координаты точки высоты h, то ему будут удовлетворять и координаты некоторой другой точки высоты $h_1 < h$. Но поскольку существует только конечное число целых чисел, меньших h, то уравнение $(**)$ неразрешимо в целых числах, а значит, и уравнение $(*)$ — в рациональных.

Нам остаётся рассказать о трактовке неопределённых уравнений

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

второго и третьего порядков в работах Ферма. Самое большее, что можно здесь утверждать, сводится к следующему: Ферма хорошо понял Диофанта и умело применял его методы, к которым он добавил только сдвиг кривой. Задачи, сводящиеся к нахождению рациональных решений неопределённых уравнений третьего порядка, встречаются как на полях экземпляра «Арифметики», принадлежавшего Ферма, так и в сочинении де Бильи, написанного после смерти Ферма с целью разъяснить методы последнего. В этом сочинении, озаглавленном «Новое искусство» (Inventum novum), которое было присоединено к собранию трудов Ферма (это сделал Поль

Таннери), методы Диофанта применяются обстоятельно и методически, однако ничего нового к ним не добавлено.

§ 10. ДИОФАНТОВЫ УРАВНЕНИЯ У ЭЙЛЕРА И ЯКОБИ. СЛОЖЕНИЕ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ [1])

Первый этап развития учения о неопределённых уравнениях второго и третьего порядков, начало которому положил Диофант, нашёл своё завершение в работах Леонарда Эйлера (1707–1783).

Величайший математик XVIII века, один из первых петербургских академиков, Леонард Эйлер занимает в нашей науке столь большое место, что буквально нельзя найти такую область математики, в которой ему не принадлежали бы фундаментальные результаты, глубокие идеи или мощные общие методы. Что касается рассматриваемого нами вопроса, то воздействие работ Эйлера было двояким. Сам он в своей «Алгебре» [2]) систематически рассмотрел вопрос о решении в рациональных числах неопределённых уравнений вида

$$y^2 = ax^2 + bx + c \tag{16}$$

и

$$y^2 = ax^3 + bx^2 + cx + d \tag{17}$$

и чётко сформулировал, в чём заключается различие между обоими случаями. Так, переходя к исследованию уравнений (17), Эйлер пишет:

> «Мы должны заметить заранее, что здесь нельзя найти общего решения, как это было в предыдущих случаях, и метод, употребляемый ниже, приводит не к бесчисленному множеству решений одновременно, но теперь каждая операция позволяет нам узнать только одно значение x».

И он показывает, как найти новое решение при помощи метода касательной Диофанта. При этом все рассуждения про-

[1]) Алгебраическая кривая рода 1 называется эллиптической.

[2]) Эта книга была впервые издана на русском языке под названием «Универсальная арифметика» (1768–1769). Впоследствии она несколько раз издавалась на немецком и французском языках.

водились чисто аналитически, без применения каких бы то ни было геометрических терминов.

Эйлер заметил [1]), что кривые третьего порядка в частных случаях могут вести себя как кривые второго порядка, т. е. что неизвестные x и y могут быть выражены в виде рациональных функций (с рациональными коэффициентами) от одного параметра. Он сформулировал условия, при которых это будет иметь место. А именно, если уравнение задано в виде (17), то для этого нужно, чтобы многочлен, стоящий в правой части, имел кратный рациональный корень:

$$F_3(x) = ax^3 + bx^2 + cx + d = a(x - \alpha)^2(x - \beta).$$

Сам Эйлер доказал только достаточность этого условия: он показал, что в этом случае рациональные выражения для x и y можно найти при помощи подстановки

$$y = k(x - \alpha).$$

Применяя указанную подстановку, получим

$$k^2(x - \alpha)^2 = a(x - \alpha)^2(x - \beta),$$

откуда

$$x = \frac{k^2 + a\beta}{a} \qquad y = k\frac{k^2 + a\beta - a\alpha}{a}\,.$$

Нетрудно показать, что условие Эйлера равносильно тому, что кривая $y^2 = F_3(x)$ имеет одну двойную точку, т. е. род её равен нулю. Действительно, из уравнений

$$\begin{cases} y^2 = ax^3 + bx^2 + cx + d, \\ 3ax^2 + 2bx + c = 0, \\ 2y = 0, \end{cases}$$

определяющих особые точки, получим, что абсцисса двойной точки должна быть общим корнем многочлена $F_3(x) = ax^3 + bx^2 + cx + d$ и его производной $F_3'(x) = 3ax^2 + 2bx + c$,

[1]) Это заметил ещё Диофант. Так, задача 6 книги IV приводится к уравнению $x^3 + 16x^2 = y^3$, откуда x и y находятся как рациональные функции параметра:

$$x = \frac{16}{a^3 - 1}\,, \qquad y = ax = \frac{16a}{a^3 - 1}\,.$$

т. е. кратным корнем многочлена $F_3(x)$. Этот корень можно найти, применяя к $F_3(x)$ и $F_3'(x)$ алгоритм Евклида, откуда следует, что корень будет рациональным.

Впоследствии Пуанкаре показал, что условие Эйлера не только достаточно, но и необходимо (см. § 12).

В последние годы жизни Эйлер вновь обратился к диофантову анализу. Он усовершенствовал свои методы и впервые применил метод секущей Диофанта в случае, если известны две конечные рациональные точки кривой (17). А именно, пусть

$$F_3(\alpha) = f^2, \qquad F_3(\beta) = g^2; \tag{18}$$

тогда Эйлер полагал

$$y = f + \frac{g-f}{\beta-\alpha}(x-\alpha) \qquad \text{или} \qquad y = g + \frac{f-g}{\alpha-\beta}(x-\beta),$$

что равносильно проведению прямой через точки (α, f) и (β, g), и находил новое рациональное значение x из уравнения

$$F_3(x) = \left[f + \frac{g-f}{\beta-\alpha}(x-\alpha)\right]^2.$$

Для этого нужно только учесть равенства (18).

Эти работы были опубликованы только в 1830 году после смерти Эйлера.

Но Эйлеру принадлежат и другие исследования, с первого взгляда как будто не связанные с задачами Диофанта, но именно они внесли в трактовку этих задач совершенно новую точку зрения. Мы имеем в виду знаменитую теорему сложения эллиптических интегралов, открытую Эйлером.

Пусть дана кривая

$$y^2 = x^3 + ax + b, \ ^1) \tag{19}$$

и точка $A(x, y)$ на ней. Обозначим

$$\Pi(A) = \int_\infty^x \frac{dx}{y}.$$

[1]) Сам Эйлер рассмотрел теорему для кривых $y^2 = F_3(x)$ и $y^2 = F_4(x)$. Мы ограничимся первым случаем. Второй случай, который мы опускаем, может быть сведён к первому.

Теорема Эйлера утверждает, что для любых точек $A(x, y)$ и $B(x_1, y_1)$ кривой Γ существует такая точка $C(x_2, y_2)$ этой кривой, что

$$\Pi(A) + \Pi(B) = \Pi(C). \tag{20}$$

При этом координаты точки C выражаются рационально через координаты точек A и B (т. е. в виде рациональных функций с рациональными коэффициентами[1])). Это — *первая теорема Эйлера.*

Вторая теорема Эйлера утверждает, что если задано уравнение

$$\Pi(D) = n\Pi(A), \tag{21}$$

где A и D — точки кривой Γ, а n — любое целое число, положительное или отрицательное, то координаты точки D рационально выражаются через координаты точки A.

В частности, если $n = 2$, то получаем уравнение

$$\Pi(D) = 2\Pi(A). \tag{22}$$

Соотношение (21) называют иногда *теоремой умножения эллиптических интегралов.*

Если теперь точки A и B рациональные, то рациональными будут точки C и D, т. е. благодаря теореме Эйлера из двух или одной рациональных точек кривой Γ можно получать новые её рациональные точки.

Эту-то связь теоремы сложения с диофантовым анализом и отметил впервые знаменитый немецкий математик Карл Густав Якоб Якоби. Он это сделал в своей статье «О применении теории эллиптических и абелевых интегралов в диофантовом анализе» (De usu theoriae integralium ellipticorum et integralium abelianorum in analysi Diophańtea), которая была опубликована в журнале Крелля, самом солидном немецком математическом журнале прошлого века, в 1834 году. Современные Якоби учёные, по-видимому, не обратили на неё внимания, хотя в ней содержались интересные и глубокие соображения.

[1]) Для этих функций Эйлер находит явное выражение, так что, зная координаты точек A и B, можно вычислить координаты точки C.

В начале статьи Якоби высказывает удивление, что учёный муж (т. е. Эйлер) не заметил связи, о которой пойдёт речь и которая бросается в глаза. Затем он приводит формулировку теоремы сложения Эйлера (для случаев когда заданы две точки и когда задана только одна точка) и отмечает, что, зная конечное число рациональных точек $A_1, \ldots, A_s$ кривой Γ, можно получить бесконечно много новых рациональных точек этой кривой из соотношения

$$\Pi(A) = m_1\Pi(A_1) + \ldots + m_s\Pi(A_s),$$

где $m_1, \ldots, m_s$ — любые целые числа. Аналогично, исходя из одной рациональной точки A, можно получить бесконечную последовательность таких точек, пользуясь соотношением (22). Однако, придавая в этой формуле числу n значения ± 2, ± 3 и т. д., мы не обязательно будем получать всё новые и новые точки. Может случиться, что при некотором n

$$n\Pi(A) = \Pi(A),$$

т. е. через конечное число шагов мы вернёмся к исходной точке. Якоби отмечает это и находит условие, при котором такое равенство будет иметь место (мы не будем приводить это условие, так как нам пришлось бы углубиться в изучение периодов интегралов $\Pi(A)$), что не входит в наши намерения). Точки, для которых существует такое n, что $n\Pi(A) = \Pi(A)$, будем называть *точками конечного порядка*.

В конце статьи Якоби намечает, как перенести полученные результаты на случай алгебраических кривых высших порядков. При этом вместо теоремы сложения Эйлера он пользуется более общими теоремами Абеля. Мы не будем здесь на этом останавливаться, отметим только, что эти идеи Якоби получили развитие только в наши дни.

Вернёмся к основному содержанию статьи. Покажем, что в ней Якоби близко подошёл к открытию структуры множества рациональных точек эллиптической кривой. Для такого открытия ему недоставало не аппарата, которым он прекрасно владел, но совершенно новой точки зрения, которая только постепенно и с трудом пробивала себе дорогу в XIX веке. По-

пробуем пояснить суть этой точки зрения. Рассмотрим множество M рациональных точек кривой Γ. Если A и B — любые две точки этого множества, то согласно теореме Эйлера в M найдётся такая точка C, что

$$\Pi(A) + \Pi(B) = \Pi(C).$$

Условимся считать точку C «суммой» точек A и B и писать

$$A \oplus B = C.$$

Мы обвели знак + кружочком, чтобы подчеркнуть, что речь здесь идёт не о сложении чисел.

Итак, во множестве M мы определили закон композиции (операцию), который каждым двум элементам A и B из M ставит в соответствие третий элемент C из M.

В современной математике множество S, в котором определён закон композиции $\oplus$, называется *группой*, если выполняются следующие условия:

1. Для любых трёх элементов A, B и C из S

$$(A \oplus B) \oplus C = A \oplus (B \oplus C).$$

(*ассоциативность*).

2. В множестве S существует *нейтральный элемент* N — такой, что для любого A из S

$$A \oplus N = A.$$

3. Для каждого элемента A существует *обратный* (или *противоположный*) элемент A' из S — такой, что

$$A \oplus A' = N.$$

Если, кроме того, для любых элементов из S

$$A \oplus B = B \oplus A,$$

то группа называется *коммутативной* или *абелевой*.

Так, множество всех целых чисел образует абелеву группу по сложению, множество рациональных положительных чисел — абелеву группу по умножению, множество квадратных матриц второго порядка, определители которых отличны от

нуля, образует некоммутативную группу по умножению. В последнем случае роль нейтрального элемента играет единичная матрица.

Обычно, по аналогии с числовыми операциями, законы композиции в произвольных группах также называют *сложением* или *умножением*. В соответствии с этим нейтральный элемент называют *нулём* или *единицей*. (При этом становятся естественными названия противоположного или обратного элементов.)

Посмотрим, будет ли группой наше множество точек M с введённой операцией сложения.

Что касается первого условия, т. е. свойства ассоциативности, то оно следует из аналогичного свойства сложения интегралов, для которых, разумеется,

$$\big[\mathbf{\Pi}(A)+\mathbf{\Pi}(B)\big]+\mathbf{\Pi}(C)=\mathbf{\Pi}(A)+\big[\mathbf{\Pi}(B)+\mathbf{\Pi}(C)\big].$$

Но существует ли во множестве M точка, которая играет роль нуля? И имеется ли для каждой точки этого множества «противоположная» точка?

Начнём с нуля. Если M — множество рациональных точек кривой $\mathbf{\Gamma}$, т. е. точек, координаты которых — конечные рациональные числа, то нуля в нём нет. Для того чтобы говорить о сложении точек множества M, необходимо дополнить его ещё одной точкой O, которая и будет играть роль нуля. О том, как это сделать, мы скажем подробно в следующем параграфе, а пока примем это на веру. Ясно, что для этой точки O должно быть

$$\mathbf{\Pi}(O)=0.$$

Теперь мы сможем для любой точки A найти «противоположную». Действительно, естественно считать, что $A\oplus A'=O$, если

$$\mathbf{\Pi}(A)+\mathbf{\Pi}(A')=\mathbf{\Pi}(O)=0.$$

Но тогда за A' нужно принять точку, симметричную с A относительно оси Ox. Действительно, если координаты точки A суть (x,y), то координатами точки A' будут $(x,-y)$ и

$$\mathbf{\Pi}(A')=\int_\infty^x\frac{dx}{-y}=-\int_\infty^x\frac{dx}{y}=-\mathbf{\Pi}(A).$$

Заметим, что

$$\Pi(A) + \Pi(B) = \Pi(B) + \Pi(A),$$

т. е.

$$A \oplus B = B \oplus A,$$

а значит, наша группа коммутативна.

Итак, исходя из теорем Эйлера и на основании связи, замеченной Якоби, можно было бы определить сложение во множестве рациональных точек эллиптической кривой, дополнив его только одной точкой, и тогда это множество получило бы структуру коммутативной группы. Точки конечного порядка, о которых говорит Якоби, являются элементами конечного порядка этой группы (элемент группы называется элементом конечного порядка, если некоторое n-е кратное его равно нулю группы).

Таков перевод замечаний Якоби на современный нам язык.

Однако, поскольку математики первой половины XIX века не были склонны переносить арифметические операции на точки или другие объекты, далёкие от чисел, то Якоби выражал те же результаты иначе. Вместо «сложения» точек A и B, он говорил о сложении интегралов $\Pi(A)$ и $\Pi(B)$, причём последнее сложение понимается в обычном смысле слова.

§ 11. ГЕОМЕТРИЧЕСКИЙ СМЫСЛ ОПЕРАЦИИ СЛОЖЕНИЯ ТОЧЕК

Поставим теперь вопрос: имеет ли связь теорема сложения Эйлера с методами касательной и секущей Диофанта? Ведь в обоих случаях по двум или одной рациональной точке кривой Γ определяются новые её рациональные точки. Ни Эйлер, ни Якоби ничего не говорят об этой связи. А между тем такая связь имеется!

Уточним поставленный нами вопрос. По двум точкам A и B кривой Γ найдём по теореме Эйлера точку C кривой такую, что

$$\Pi(C) = \Pi(A) + \Pi(B).$$

С другой стороны, проведём через A и B прямую и найдём её точку пересечения C' с кривой Γ. Имеется ли какая-нибудь

связь между точками C и C'? Оказывается, имеется, и очень простая. Обе точки расположены симметрично относительно оси Ox, т. е. если координаты точки C суть (x_2, y_2), то координатами точки C' будут $(x_2, -y_2)$.

Теперь мы можем придать операции сложения точек на кривой простой геометрический смысл: суммой точек A и B будет точка C кривой Γ, симметричная с точкой C' пересечения кривой Γ с прямой AB.

Однако, этим способом мы не можем сложить точку A с собой, т. е. получить точку $2A$. По первому методу Диофанта проведём в точке A касательную к Γ и найдём её точку пересечения D' с кривой. Эта точка D' будет симметричной с точкой D, полученной по методу Эйлера: $\Pi(D) = 2\Pi(A)$. Значит, мы можем чисто геометрически определить точку $2A$ и, вообще, nA при любом целом n.

Какая же точка при такой интерпретации сложения точек будет играть роль нуля?

Для ответа на этот вопрос перейдём, как это мы делали в § 6, к однородным координатам. Положим

$$x = \frac{u}{z}, \qquad y = \frac{v}{z},$$

тогда уравнение (19) примет вид

$$v^2 z = u^3 + auz^2 + bz^3. \tag{19'}$$

Из уравнения (19′) видно, что при $z = 0$ будет $u = 0$, а v — произвольно. Поскольку координаты каждой точки определены с точностью до постоянного множителя, то можно принять $v = 1$.

Условимся теперь считать, что набору чисел (0, 1, 0) отвечает несобственная точка нашей кривой. Мы будем обозначать её буквой O. Будем, кроме того, считать, что точка O', симметричная с O относительно оси абсцисс, совпадает с O.

Покажем, что точка O и будет играть роль нуля. Для этого заметим, что все вертикальные прямые $u = cz$ пересекаются в точке O. Действительно, при $z = 0$ и $u = 0$, а v можно принять равным 1.

Пусть теперь дана некоторая рациональная точка A кривой Γ, имеющая координаты (x_0, y_0). Тогда, согласно только

что доказанному, прямая, проходящая через A и O, будет вертикальной, т. е. уравнением её будет

$$x = x_0.$$

Эта прямая пересечёт кривую Γ в трёх точках: точке A, точке O и точке $A'(x_0, -y_0)$, симметричной с A относительно оси абсцисс. Согласно нашему определению сумма точек A и O есть точка, симметричная с A', т. е. сама точка A. Таким образом,

$$A \oplus O = A.$$

Наконец, точкой, противоположной точке A, будет $A'(x_0, -y_0)$. Действительно, соединяющая их прямая будет вертикальной, следовательно, она пересечёт кривую Γ ещё и в точке O. Тогда по определению суммой A и A' будет точка, симметричная с O, но она, по условию, совпадает с самой точкой O, т. е.

$$A \oplus A' = O.$$

Заметим, что определённая нами точка O такова, что для неё

$$\Pi(O) = \int_{\infty}^{\infty} \frac{dx}{y} = 0.$$

Таким образом, и из теоремы сложения Эйлера можно было бы усмотреть, что роль нуля должна играть бесконечно удалённая точка.

Итак, «сложение» точек эллиптической кривой можно определить из процедур Диофанта. Знали ли об этом Эйлер и Якоби? Точнее, знали ли они, что три точки кривой Γ, удовлетворяющие соотношению

$$\Pi(A) + \Pi(B) + \Pi(C) = 0,$$

лежат на одной прямой? Ни Эйлер, ни Якоби не упоминают об этом, хотя по крайней мере Якоби этот факт должен был быть хорошо известен. Возможно, что о нём знал и Эйлер. Но, во-первых, оба они формулировали теорему сложения для кривой

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e, \qquad (*)$$

не выделяя специально случая кривой третьего порядка. А для кривой $(*)$, если она даже имеет рациональные точки,

формулы сложения не будут иметь простого и однозначно определённого геометрического смысла. Кроме того, ни Эйлер, ни Якоби не придавали значения геометрическому истолкованию аналитических соотношений.

Как ни просты изложенные здесь соображения о «сложении» точек эллиптической кривой, прошло ещё около 70 лет прежде, чем они были положены в основу систематического изучения структуры множества её рациональных точек. Это было сделано в начале XX века замечательным французским математиком Анри Пуанкаре (1854–1912).

§ 12. АРИФМЕТИКА АЛГЕБРАИЧЕСКИХ КРИВЫХ

Работа Якоби, о которой мы говорили, осталась незамеченной и к идее построения арифметики на эллиптической кривой обратился только Пуанкаре. Однако за время, прошедшее между 1834 годом и концом XIX века, было много сделано в изучении геометрии алгебраических кривых. Ещё в работах замечательного норвежского математика Нильса Хенрика Абеля (1802–1829) появилось понятие рода алгебраической кривой [1]). Из других соображений к тому же понятию пришёл крупнейший математик Германии Бернгард Риман (1826–1866). В своей знаменитой работе «Теория абелевых функций» (1857) он положил в основу классификации уравнений $F(s,z)=0$ б и р а ц и о н а л ь н ы е п р е о б р а з о в а н и я — Риман называл их *рациональными подстановками* — и показал, что *род кривой является инвариантом таких преобразований*. Риман писал:

> «Станем считать принадлежащими к одному классу все неприводимые алгебраические уравнения между двумя величинами, переводящиеся одно в другое посредством рациональных подстановок; итак, уравнения $F(s,z)=0$ и $F_1(s_1,z_1)=0$ принадлежат к одному классу, если s и z можно выразить рационально через s_1 и z_1 таким образом, чтобы уравнение $F(s,z)=0$ перешло в $F_1(s_1,z_1)=0$, и притом s_1 и z_1 также рационально выражаются через s и z» [2]).

[1]) Определение рода кривой см. в § 3.

[2]) Б. Р и м а н, Сочинения, М.–Л., Гостехиздат, 1948, стр. 117.

В последующих работах Клебша и других немецких математиков были заложены основы теории алгебраических кривых. Однако, как правило, такие кривые рассматривали над полем комплексных чисел (т. е. коэффициенты уравнений принимали комплексными), поэтому арифметикой этих кривых не занимались.

Анри Пуанкаре начинает свой мемуар «Об арифметических свойствах алгебраических кривых» [1]) с важного замечания, что арифметические свойства многих объектов самым тесным образом связаны с преобразованиями этих объектов: так, например, если речь идёт о квадратичных формах от двух переменных, то, как показал Гаусс, такими преобразованиями будут линейные подстановки с целыми коэффициентами. «Можно предположить, — пишет он далее, — что изучение аналогичных групп преобразований окажет большие услуги Арифметике. Это меня и побудило опубликовать следующие соображения, хотя они составляют скорее программу изучения, чем настоящую теорию» [2]).

Пуанкаре начал искать, каким способом можно связать между собой и систематизировать проблемы диофантова анализа. Для этого он решил провести новую классификацию многочленов от двух переменных с целыми рациональными коэффициентами. За основу такой классификации он выбрал совокупность бирациональных преобразований с рациональными коэффициентами. Выше мы говорили, что аналогичную классификацию вводил и Риман. Отличие состоит в том, что Риман рассматривал бирациональные преобразования с комплексными коэффициентами, а Пуанкаре — с рациональными, что и позволило ему подойти к изучению арифметических свойств кривых.

Итак, согласно Пуанкаре две кривые

$$f_1(x, y) = 0 \qquad \text{и} \qquad f_2(x, y) = 0$$

эквивалентны или *принадлежат одному классу*, если от одной из них к другой можно перейти путём бирационально-

[1]) H. Poincaré, Sur les propriétés arithmétiques des courbes algèbriques, Journ. de mathém. pures et appl. Paris, 5-me série, **7** (1901), 161–234.

[2]) Там же, стр. 161.

го преобразования с рациональными коэффициентами [1]). Так, например, любые две прямые

$$ax + by + c = 0 \qquad \text{и} \qquad a'x + b'y + c' = 0,$$

коэффициенты которых рациональны, эквивалентны.

Чтобы показать это, Пуанкаре выбирает фиксированную рациональную точку F, лежащую вне обеих прямых, и ставит в соответствие каждой точке A первой прямой точку A' второй, которая получится при пересечении её с прямой AF (рис. 4). Значит, все прямые с рациональными коэффициентами принадлежат одному классу.

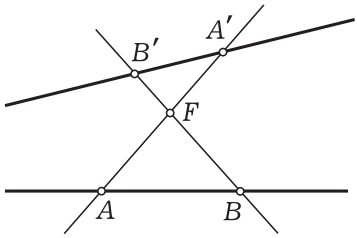

Рис. 4.

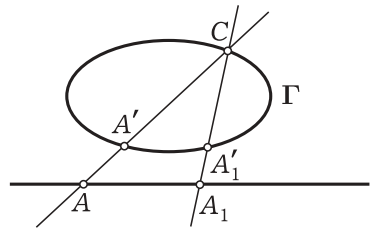

Рис. 5.

После этого он переходит к коническим сечениям, т. е. кривым второго порядка, и показывает, что если на коническом сечении $f(x, y) = 0$ (с целыми или рациональными коэффициентами) имеется хотя бы одна рациональная точка C, то оно эквивалентно рациональной прямой. Для этого он ставит в соответствие каждой точке A фиксированной рациональной прямой L точку A' конического сечения Γ так, чтобы точки A, A' и C лежали на одной прямой (рис. 5). Этот результат, как мы видели, был установлен ещё Диофантом.

Затем Пуанкаре рассматривает кубические кривые рода 0. Поскольку, по определению рода,

$$0 = \frac{(3-1)(2-1)}{2} - d,$$

то отсюда получаем $d = 1$, т. е. кривая должна иметь одну двойную точку. Пуанкаре утверждает, что эта точка необходимо будет рациональной. Мы не будем здесь останавливаться на доказательстве этого факта. Заметим только, что достаточ-

[1]) То есть это как раз такое определение бирациональной эквивалентности, которое было дано нами в § 3.

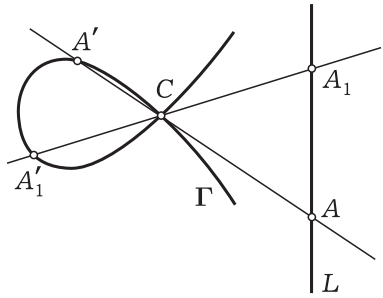

Рис. 6.

ность наличия двойной точки у кривой $y^2 = F_3(x)$ для того, чтобы x и y можно было выразить как рациональные функции одного параметра, была доказана ещё Эйлером, (см. § 10 настоящей книги).

Однако доказательства необходимости у Эйлера не было. Достаточность наличия двойной точки для того, чтобы кубика[1]) была эквивалентна рациональной прямой, Пуанкаре доказывает тем же способом, что и Эйлер, только проводит доказательство не аналитически, а геометрически. Он берёт эту двойную точку C в качестве основной, фиксирует некоторую рациональную прямую L и ставит в соответствие каждой точке A этой прямой точку A' кубической кривой Γ, лежащую на прямой AC (рис. 6).

После этого Пуанкаре доказывает основную теорему, которая полностью решает вопрос о множестве M рациональных точек кривой рода 0.

Т е о р е м а. *Всякая кривая рода* 0 *и порядка* m, $m > 2$, *бирационально эквивалентна кривой порядка* $m - 2$.

Следовательно, всякая кривая рода 0 и нечётного порядка ($m = 2k + 1$) бирационально эквивалентна прямой, а чётного порядка ($m = 2k$) — коническому сечению.

Отсюда, в частности, следует, что на всякой кривой рода 0 нечётного порядка существует бесконечно много рациональных точек.

Вопрос же о рациональных точках кривых рода 0 и чётного порядка сводится к определению рациональных точек конического сечения, а структура этого множества была изучена ещё Диофантом.

[1]) То есть кривая третьего порядка.

Заметим, что аналогичные результаты, относящиеся к кривым рода 0, были получены за 10 лет до Пуанкаре в работе Давида Гильберта и Адольфа Гурвица «О диофантовых уравнениях рода 0» [1]). В этой же работе уже было обращено внимание на то, что множество рациональных точек алгебраической кривой инвариантно относительно бирациональных преобразований с рациональными коэффициентами. Пуанкаре был, по-видимому, незнаком с этой работой, по крайней мере он нигде о ней не упоминает. К тому же основной интерес его мемуара состоит не в этих результатах, а в исследовании кривых рода 1.

Эти исследования Пуанкаре начинает с рассмотрения простейших кривых рода 1, т. е. кривых третьего порядка. Если такая кривая $\mathbf{\Gamma}$ имеет хотя бы одну рациональную точку, то её уравнение, как мы говорили, можно привести с помощью бирациональных преобразований к виду

$$y^2 = x^3 + ax + b. \qquad (*)$$

Предположим, что оно уже задано в таком виде. Пуанкаре излагает методы касательной и секущей Диофанта (разумеется, не упоминая имени последнего) для нахождения новых рациональных точек кривой $\mathbf{\Gamma}$, если известны одна или две её рациональные точки. Оба метода он формулирует сначала геометрически, а затем связывает их с теоремой сложения Эйлера, отмечая (чего не делал Якоби), что три точки A, B и C эллиптической кривой $\mathbf{\Gamma}$, удовлетворяющие соотношению

$$\mathbf{\Pi}(A) + \mathbf{\Pi}(B) + \mathbf{\Pi}(C) = 0, \qquad (**)$$

лежат на одной прямой. Пуанкаре уточняет и смысл этого равенства.

Дело в том, что интеграл $\displaystyle\int_a^u \frac{dx}{y}$, где y определяется из уравнения $(*)$, является бесконечнозначной функцией своего верхнего предела. Он несколько напоминает функцию $\displaystyle\int_0^u \frac{dx}{\sqrt{1-x^2}} = \arcsin u$, которая имеет свои «главные значения» в про-

[1]) D. Hilbert und A. Hurwitz, Über die Diophantischen Gleichungen von Geschlecht Null. Acta Math. **14** (1890), 217–224.

межутке $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, а остальные значения получаются из них путём прибавления кратных периода 2π.

Подобно этому и $\int_0^u \frac{dx}{\sqrt{x^3+ax+b}}$ имеет «главные значения», от которых все остальные отличаются на слагаемые вида $m_1\omega_1 + m_2\omega_2$, где m_1 и m_2 — целые рациональные числа, а ω_1 и ω_2 — периоды, причём отношение между ними есть комплексное число, мнимая часть которого не равна нулю. Но поскольку в равенстве $(**)$ фигурируют три интеграла, каждый из которых определён с точностью до периодов, то, как замечает Пуанкаре, слагаемые можно подобрать так, чтобы сумма равнялась нулю. Такое уточнение, которое казалось излишним Эйлеру и Якоби при их формальном взгляде на математические соотношения, сделалось необходимым в работе начала XX века.

Пуанкаре явно определяет сложение рациональных точек на эллиптической кривой Γ и показывает, что множество M таких точек образует коммутативную группу. Уже из определения сложения и удвоения точек ясно, что если $A_1, \ldots, A_s$ принадлежат множеству M, то и

$$A = m_1A_1 + \ldots + m_sA_s \qquad (***)$$

также принадлежит M.

Пуанкаре ставит вопрос: можно ли выбрать точки $A_1, \ldots, A_s$ так, чтобы из формулы $(***)$ получались все рациональные точки кривой Γ?

В переводе на язык теории групп это означает: имеет ли группа рациональных точек кривой Γ конечное число образующих? Таким образом, Пуанкаре начинает более глубокое исследование структуры множества M.

Пуанкаре называет точки $A_1, \ldots, A_s$, из которых можно получить все остальные путём рациональных операций, *фундаментальной системой рациональных точек*. Он замечает, что фундаментальную систему можно выбрать бесконечным числом способов. Будем выбирать фундаментальные точки так, чтобы число их было наименьшим возможным.

Наименьшее число рациональных точек r, из которых все остальные получаются по формуле $(***)$, Пуанкаре называет

рангом кривой Γ[1]).

Можно показать, что ранг является инвариантом при бирациональных преобразованиях, т. е. что это одно из важных внутренних свойств кривой.

Относительно ранга Пуанкаре ставит следующий вопрос: «Какие значения может принимать целое число, которое мы назвали рангом рациональной кубики?».

Этот вопрос был воспринят последующими математиками как утверждение, что ранг эллиптической кривой всегда конечен, т. е. что группа её рациональных точек имеет конечное число образующих. Это утверждение получило название гипотезы Пуанкаре. Оно было доказано только в 1922 году английским математиком Л. Дж. Морделлом. Это был самый выдающийся результат со времён Пуанкаре. Теорему о том, что ранг кривой рода 1 над полем рациональных чисел всегда конечен, он получил при помощи метода спуска Ферма.

После рассмотрения кубик Пуанкаре переходит к другим кривым рода 1. Он доказывает следующую основную теорему:

Пусть $f(x, y) = 0$ — кривая рода 1 и порядка m. Если на ней лежит хотя бы одна рациональная точка, то она бирационально эквивалентна кривой третьего порядка.

Этим полностью решается вопрос о кривых рода 1: на такой кривой либо нет ни одной рациональной точки либо кривая эквивалентна кубике, а тогда множество её рациональных точек имеет ту же структуру, что и у кривой $(*)$.

Мемуар Пуанкаре содержит ещё и другие интересные идеи и «программы изучения», однако мы не можем здесь на них останавливаться. Отметим только один факт, интересный с точки зрения истории математики: Пуанкаре, по-видимому, ничего не знал о работах своих предшественников по арифметике алгебраических кривых. Процедуры Диофанта и их связь с теоремой сложения Эйлера были ему известны из об-

[1]) Теперь *рангом* r эллиптической кривой Γ называют такое наименьшее число рациональных точек $A_1, \ldots, A_r$, что любая рациональная точка A кривой имеет вид

$$A = m_1 A_1 + \ldots + m_r A_r + P,$$

где P — некоторая точка конечного порядка.

щей теории алгебраических кривых. (Ведь складывать можно не только рациональные точки! Да и геометрически рациональные точки ничем особым не выделяются.) Но мысль применить известные факты и методы для изучения арифметических свойств кривых возникла у Пуанкаре независимо. Таким образом, эта мысль возникала по крайней мере трижды: в середине III века н. э. у Диофанта, в 30-х годах XIX века у Якоби и, наконец, в начале XX века у Анри Пуанкаре. Это — не единичный факт в истории математики: так, трижды открывалась проективная геометрия — один раз в античности, второй — в работах Дезарга и Паскаля (XVII век), наконец, «в последний раз» — в начале XIX века в работах Понселе и других. «В последний» в том смысле, что с этого времени и до наших дней преемственность и традиция в этих исследованиях уже не прерывается. То же относится и к арифметике алгебраических кривых после Пуанкаре.

§ 13. ЗАКЛЮЧЕНИЕ

Остановимся теперь на некоторых обобщениях, результатах и гипотезах, относящихся к арифметике алгебраических кривых.

Одно из обобщений было намечено уже в мемуаре Пуанкаре. От Диофанта и до Пуанкаре арифметические свойства кривых рассматривали над полем рациональных чисел, т. е. коэффициенты уравнения

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

кривой Γ, всех бирациональных преобразований и координаты искомых точек должны были принадлежать полю рациональных чисел $\mathbb{Q}$. Пуанкаре предложил провести подобные рассмотрения над полями алгебраических чисел, например, над квадратичным полем $\mathbb{Q}(\sqrt{D})$. В этом случае точка называется рациональной, если её координаты принадлежат рассматриваемому полю.

Но можно строить арифметику кривых и над совершенно произвольным полем k, например, полем рациональных функций от одного переменного или над конечным полем (по-

лем вычетов по модулю p).

В 1929 году французский математик Андре Вейль при помощи метода спуска Ферма доказал гипотезу Пуанкаре о конечности ранга эллиптической кривой над произвольным полем k.

Другое обобщение, начатое также Пуанкаре, относится к арифметике алгебраических кривых рода $p > 1$. В этом случае сложение точек определить уже нельзя, но можно определить «сложение» для групп из p точек, где p — род кривой. Такое «сложение» было намечено ещё в работе Якоби, о которой мы говорили, о нём же писал в последнем параграфе своего мемуара Пуанкаре. А. Вейль в той же работе 1929 года показал, что гипотеза о конечности ранга верна и для алгебраических кривых любого рода и над любым полем k.

Параллельно с этим рассматривался вопрос о целых точках (т. е. точках с целыми координатами) на алгебраической кривой. Ещё в 1923 году Л. Дж. Морделл показал, что уравнение

$$Ey^2 = Ax^3 + Bx^2 + Cx + D$$

имеет только конечное число целых рациональных решений. Наиболее общий результат тут был получен немецким математиком К. Л. Зигелем, который, применив методы А. Туэ и методы Морделла–Вейля, показал, что число целых точек кривой

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

над полем k алгебраических чисел, если род кривой $p > 0$, всегда к о н е ч н о.

Что касается рациональных точек на кривой рода $p > 1$, то согласно гипотезе Морделла таких точек существует лишь конечное число. Эта гипотеза до сих пор не доказана. Здесь можно отметить только результат советского математика Ю. И. Манина, который рассмотрел кривые не над полем рациональных чисел (как того требует гипотеза Морделла), а над полем K алгебраических функций, и показал, что все кривые рода $p > 1$, кроме некоторого простого специального класса таких кривых, имеют в поле K конечное число рациональных точек.

Отметим, что все теоремы, доказанные относительно системы образующих группы рациональных точек эллиптической кривой, являются чистыми теоремами существования: неизвестно никакого эффективного приёма для нахождения образующих. Остаётся открытым вопрос Пуанкаре о том, какие значения может принимать число, которое он назвал рангом эллиптической кривой. До сих пор неизвестно, существуют ли кривые, ранг которых был бы больше 11, но и не доказано, что ранг не может принимать сколь угодно больших значений. Единственный результат здесь получен советским математиком А. И. Лапиным, который доказал, что над полем рациональных функций существуют кривые сколь угодно большого ранга.

Глубокие результаты, относящиеся к установлению существования рациональных точек на эллиптической кривой, принадлежат советскому математику И. Р. Шафаревичу и американскому математику Дж. Тэйту. Однако здесь мы не можем привести не только доказательства, но и формулировки результатов, так как для этого требуются более обширные сведения из современной алгебры и алгебраической геометрии, чем мы имеем право предполагать в этой брошюре. К тому же мы от истории вопроса перешли к современности и читатель сможет, если захочет, более подробно познакомиться с нынешним состоянием диофантовых уравнений по обзорным статьям. Укажем, например, на статью Дж. Касселса «Диофантовы уравнения со специальным рассмотрением эллиптических кривых», опубликованную в журнале «Математика» (№ 1 и № 2 за 1968 год).

ЛИТЕРАТУРА

I. Издания сочинений Диофанта. Общепринятый теперь текст «Арифметики» Диофанта и его небольшого трактата «О многоугольных числах» был издан в 1893 году (вместе с переводом на латинский язык) известным французским историком науки Полем Таннери. Во втором томе издания собраны все греческие комментарии к сочинениям Диофанта. Приведём название и выходные данные этого издания:

Diophanti Alexandrini, Opera omnia cum graecis commentariis, Editit et latine interpretatus est Paulus Tannery. Lipsiae, 1893–1895, vol. 1–2.

С издания Таннери сделаны следующие переводы:

1) на французский язык
Diophante d'Alexandrie, Les six livres arithmétiques et le livre des nombres polygones, trad. par Paul Ver Eecke, Bruges, 1926 (переизд. Paris, 1959).
2) на немецкий язык
Diophantus Alexandrinus, Arithmetik des Diophantos aus Alexandria, Aus dem Griech. übertr. and erklärt von Arthur Czwalina, Göttingen, 1952.
3) на английский язык
Heath Th. L., Diophantus of Alexandria, A Study in the History of Greek Algebra, Cambridge, 1910 (эта книга была переиздана в Нью-Йорке в 1964 году).

II. Литература о Диофанте очень бедна. О нём можно прочитать в общих курсах истории математики, например,

1. Б. Л. Ван-дер-Варден, Пробуждающаяся наука (перевод И. Н. Веселовского). М., Физматгиз, 1959.
2. Г. Г. Цейтен, История математики в древности и в средние века (перевод П. Юшкевича). М.–Л., Гостехиздат, 1932

а также в книге

3. А. В. Васильев, Целое число. Петербург, 1919

и в статье

4. И. Г. Башмакова, Диофант и Ферма. В сб. «Историко-математические исследования», вып. 17. М., «Наука», 1966.

III. Литература о диофантовых уравнениях и алгебраической геометрии.

1. З. И. Боревич и И. Р. Шафаревич, Теория чисел. М., «Наука», 1964.
2. Г. Дэвенпорт, Высшая арифметика. М., «Наука», 1965.
3. Л. Е. Диксон, Введение в теорию чисел. Тбилиси, 1941.
4. Т. Н. Skolem, Diophantiche Gleichungen. Berlin, 1938.
5. И. Р. Шафаревич, Основы алгебраической геометрии. Успехи матем. наук, 1969, т. 24, № 6.

СОДЕРЖАНИЕ

Изабелла Григорьевна Башмакова

ДИОФАНТ И ДИОФАНТОВЫ УРАВНЕНИЯ

М., 1972 г., 68 стр. с илл.

Редакторы *Н. Н. Гендрихсон*, *Ф. И. Кизнер*
Техн. редактор *А. П. Колесникова* Корректор *Н. В. Румянцева*
OCR обработка и конвертация в TEX — *E.G.A.* (`ega-math.narod.ru`)

Сдано в набор 29/X 1971 г. Подписано к печати 11/I 1972 г. Бумага $84 \times 108^1/_{32}$. Физ. печ. л. 2,125. Условн. печ. л. 3,57. Уч.-изд. л. 3,56. Тираж 40 000 экз. Т-01509. Цена книги 12 коп. Заказ 2970.

Издательство «Наука»
Главная редакция физико-математической литературы.
117071, Москва, В-71, Ленинский проспект, 15

2-я типография издательства «Наука». Москва, Шубинский пер., 10