ГЛАВА VI

СОЗДАНИЕ ПРЕДПОСЫЛОК СОВРЕМЕННОЙ АЛГЕБРЫ. ФОРМИРОВАНИЕ ТЕОРИИ ЧИСЕЛ

Декарт, связавший в единой науке — аналитической геометрии — методы алгебры и геометрии, считал, что он создал единую науку, синтезировавшую и как бы поглотившую обе эти дисциплины. Однако использование алгебраического аппарата в аналитической геометрии не повело к упразднению алгебры. Алгебра развивалась в дальнейшем своим оригинальным путем, имея собственную научную проблематику. Этой проблематикой оказалась по преимуществу теория алгебраических уравнений. Последняя включала в себя как формирование общей теории уравнений, так и накопление способов численного и графического их решения. Научная разработка подобных проблем приводила одновременно и к перестройке основ алгебры, связанной с расширением понятия числа, и к усовершенствованию алгебраического буквенно-символического аппарата. Развитие этих двух сторон алгебры, по существу определяющих ее содержание и предмет, достигло к концу рассматриваемого здесь столетия такого состояния, что сделало необходимым и возможным переход к качественно новым проблемам этой науки, связанным с возникновением теории Галуа и теории групп.

К алгебре примыкали, еще не будучи отчетливо отделены от нее, вычислительные арифметические приемы, в том числе методы элементарной комбинаторики, а также теоретические проблемы арифметики — теория чисел. В сознании ученых

XVIII в. они до известной степени объединялись в единую науку, для которой даже существовало специальное название — универсальная, или всеобщая, арифметика. Рассмотрению путей развития основных частей этой науки посвящена настоящая глава.

Алгебра. Самостоятельность путей развития алгебры определилась уже к началу XVIII в., когда в 1707 г. вышла в свет «Всеобщая арифметика» И. Ньютона. В ней алгебра излагалась в тесной связи с развитием вычислительных методов, как высшая стадия арифметики; геометрические вопросы были отнесены в область приложений. С самого начала Ньютон вводит операции как над буквенно-символическими выражениями, так и над числами (целыми и дробными). Введя читателя в технику тождественных алгебраических преобразований, Ньютон затем знакомит его с методами решения уравнений. На большом числе примеров, взятых из геометрии, механики и других наук, он демонстрирует сведение задачи к составлению алгебраического уравнения, корень которого будет являться решением задачи. Замыкают книгу данные общей теории уравнений, а также графическое решение последних с помощью геометрического построения корней.

«Всеобщая арифметика» является краткой записью лекций по алгебре, которые Ньютон читал в Кембриджском университете в 1673—1683 гг. В ней нет доказательств. Она не представляет собрания всех алгебраических достижений Ньютона. В других его работах содержится немало открытий в области алгебры. Среди них: обобщение формулы степени бинома на случай дробно-рациональных показателей, сообщенное в одном письме Ньютона Ольденбургу в 1676 г.; способ численного решения уравнений, известный под его именем и поныне; параллелограмм, т. е. способ разложения y, заданного уравнением $P_n(x, y)=0$ (где P_n — полином), в ряд по дробным степеням x и др.

Алгебраическая тематика «Всеобщей арифметики» была в центре внимания многих видных математиков XVIII в. Способы численного решения уравнения (как точного, так и приближенного) разрабатывали Галлей, Лагранж, Мурайль, Фурье и др. Многочисленные попытки дать строгое доказательство формулы бинома в ее наиболее общей форме прекратились лишь тогда, когда Гаусс в работе о гипергеометрическом ряде (1811) решил эту проблему. Параллелограмм Ньютона получил в работах Стирлинга, де Гюа, Крамера

и других многообразные приложения: к теории алгебраических кривых, аналитических функций и др.[1].

Вслед за «Всеобщей арифметикой» Ньютона появился ряд монографий, содержащих систематическое построение алгебры. «Трактат об алгебре» Маклорена (1748) являлся еще по преимуществу комментарием к книге Ньютона, в которой не было приведено доказательств. Последующие же сочинения, в особенности знаменитая «Универсальная арифметика» Эйлера, показали возросшую степень выделения алгебры как самостоятельной науки.

Продиктованная слепнущим Эйлером около 1767 г. «Универсальная арифметика» появилась в 1768—1769 гг. на русском языке. Помимо переизданий она была переведена на латинский, английский, французский и голландский языки. Ее влияние на определение научной проблематики алгебры и на структуру курса алгебры в университетах было очень большим. Монографический характер этой книги и цели, которые ставил перед подобными сочинениями их автор, позволяют по ее содержанию судить о состоянии алгебры во второй половине XVIII в.

«Универсальная арифметика» состоит из двух частей. В трех отделах первой части Эйлер уделил основное внимание обобщению правил решения арифметических задач и развитию буквенно-символического аппарата алгебры. Так, в первом отделе разъяснены операции над числами и одночленами, над радикалами, комплексными числами. Здесь же введены логарифмы.

Второй отдел посвящен операциям над многочленами. Кроме того, даются правила извлечения корней из чисел и алгебраических выражений (полиномов). Наконец, вводятся ряды как средство выражения дробно-рациональных функций и биномов с дробными и отрицательными показателями степени.

Третий отдел по содержанию самый разнохарактерный. В нем введены: действительное число (посредством алгоритма попеременного вычитания), многоугольные числа, пропорции и прогрессии (как арифметические, так и геометрические), периодические десятичные дроби и задачи на проценты.

---

[1] См., например, Н. Г. Чеботарев. Многоугольник Ньютона и его роль в развитии математики. В кн.: Н. Г. Чеботарев. Собр. соч., т. III. Изд-во АН СССР, М.—Л., 1950, стр. 47—80.

Методам решения алгебраических уравнений и их общей теории посвящен первый отдел второй части. Здесь собраны методы решения алгебраических уравнений первых четырех степеней, а также систем линейных уравнений. Кроме того, рассмотрены способы приближенного вычисления корней алгебраических уравнений.

Последний отдел (второй отдел «Универсальной арифметики») включает в себя преимущественно методы нахождения целочисленных решений неопределенных уравнений первой и более высоких степеней. К ним присоединены решения других задач теоретико-числового характера. Так, здесь рассмотрена великая теорема Ферма и даны ее доказательства для $n = 3$ и $n = 4$. Введены подстановки Эйлера, обращающие квадратный трехчлен в точный квадрат.

Таким образом, предмет алгебры в XVIII в. определился. Она превратилась в науку об алгебраических уравнениях. В нее также входила разработка буквенно-символического аппарата, необходимого для решения уравнений. Алгебра тесно взаимодействовала с арифметикой, сохраняя в своем составе численные методы. С другой стороны, имело место столь же тесное взаимопроникновение методов и задач алгебры и теории чисел, преимущественно в области, относящейся к диофантову анализу. Современная элементарная алгебра в значительной мере сохранила в своей структуре эти особенности.

Сравнение «Всеобщей арифметики» Ньютона и «Универсальной арифметики» Эйлера позволяет нам отметить начало и (в значительной степени) итог формирования алгебры в XVIII в. Теперь рассмотрим кратко эволюцию научного содержания этой обширной и важной части математики и процесс создания предпосылок для нового, современного этапа ее истории.

В основе алгебраических исследований лежит понятие о количестве, величине, числе. Общность и поле приложений буквенно-алгебраических методов определяются общностью понятия числа. В течение XVIII в. это понятие переживало период медленного развития. Оно постепенно обогащалось, серьезно отставая, однако, от вычислительной практики и от приложений математического анализа.

Понятие действительного числа включало в себя: натуральные числа, положительные дроби, иррациональности. Последние имели и дошедшее до нас от времен античности общее определение через отношение с привлечением геометрических соображений: число есть то, что относится к едини-

це, как один отрезок прямой к другому, принятому за единицу. Однако общая концепция иррационального числа завоевала себе права гражданства лишь во второй половине XVIII в.

Большие споры еще кипели вокруг понятия отрицательного числа. В разноречивом хоре суждений преобладали противопоставления отрицательных чисел положительным. Находились даже ученые (Мазер, 1758; Френд, 1796), не признававшие отрицательных чисел, равно как и мнимых. Правила действий с отрицательными числами не имели убедительного доказательства. Лишь в следующем, XIX веке удалось представить отрицательные числа включенными в единую числовую систему и дать этому представлению убедительное доказательство.

Мнимые числа в алгебре появляются в виде корней уравнений. Их изучение, однако, продвинулось не в алгебраических трактатах, а под давлением настоятельных необходимостей математического анализа. Именно в рамках анализа постепенно отыскивались и внедрялись правила формальных операций с мнимыми и комплексными числами. В 40-х годах Даламбер и Эйлер доказали, что всякое выражение, содержащее мнимые величины, приводится к виду $\alpha+\beta i$ (где α и β — действительные). Очевидная полезность комплексных чисел вызывала усиление внимания к вопросу об их сущности. Однако эта проблема оставалась нерешенной. Первый, кто разработал (по-видимому в интересах геодезической и картографической практики) способ геометрической интерпретации комплексных чисел точками на плоскости, был датчанин, землемер Вессель (1797 г., опубликовано в 1799 г.). Однако его работа осталась незамеченной, равно как и аналогичная интерпретация Аргана Ж. (1806). Только когда в 20-х годах XIX в. Гаусс и Коши ввели и обосновали операции над числами вида $\alpha\pm\beta i$, ввели термин «комплексное число», нашли «модуль» (Коши, 1821) или «норму» (Гаусс, 1828) комплексного числа, определили понятие сопряженности комплексных чисел, положение последних в математике существенно упрочилось. Комплексные числа вошли в алгебру.

Кстати упомянем еще об одной арифметико-алгебраической трудности, преодоленной лишь к концу XVIII в. Речь идет о введении аппарата десятичных дробей. Еще в 1585 г. голландский инженер и математик Стевин ввел их и показал их полезность. Но в течение более двухсот последующих лет десятичные дроби употреблялись лишь в астрономической

вычислительной практике. Понадобились усилия многих крупнейших математиков (Лагранж, Лаплас, Монж и др.), разработавших в период 1790—1799 гг. единую десятичную метрическую систему (введена во Франции 24 апреля 1799 г.), чтобы аппарат десятичных дробей приобрел повсеместную актуальность. В XIX столетии, по мере перехода на десятичную систему новых государств, этот аппарат сделался частью элементарно-математической подготовки учащихся.

Часть алгебры, относящаяся к решению уравнений, составляла главное ее содержание. Этой проблеме посвящено огромное количество работ. В безбрежном море книг и статей — печатных свидетельств колоссальных усилий математиков, направленных на ее решение, — можно, впрочем, выделить некоторые направления.

Первое из них сложилось из попыток отыскания регулярного элементарно-алгебраического алгоритма (вроде метода Тартальи—Кардано для кубического уравнения и метода Феррари — для уравнения четвертого порядка), пригодного для решения уравнений степени выше четвертой. Авторами этих попыток руководила лишь интуитивная уверенность в возможности отыскания такого алгоритма, по крайней мере для действительных корней. Из большого числа работ этого направления приведем два примера: Чирнгаузена и Эйлера.

Метод Чирнгаузена, опубликованный в 1683 г., состоял в следующем. Пусть дано уравнение

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0.$$

Введем вспомогательное уравнение

$$y = b_1 x^{n-2} + b_2 x^{n-3} + \ldots + b_{n-1}$$

с неопределенными пока коэффициентами. Если из обоих уравнений удастся исключить x (а это возможно), то получим

$$y^n + c_1 y^{n-1} + \ldots + c_n = 0.$$

Коэффициенты $c_1, c_2, \ldots, c_n$ — функции коэффициентов b_i, $b_2, \ldots, b_n$ и $a_1, a_2, \ldots, a_n$. Теперь подберем $b_1, b_2, \ldots, b_n$ так, чтобы $c_1 = c_2 = \ldots = c_{n-1} = 0$. Тогда $y = \sqrt[n]{-c_n}$, и мы получим возможность заменить данное уравнение другим — степени $n-2$. Чирнгаузен сумел осуществить этот метод лишь для $n=3$ и опубликовал его без дальнейших проверок. Позднее

Эйлер проделал все выкладки для $n=4$. Для $n \geqslant 5$ это, разумеется, оказалось невозможным. Попытки подбора $b_1, b_2, \ldots, b_n$ приводили к уравнениям, степень которых была больше пяти.

Отправляясь от приемов Тартальи, Эйлер пытался не раз подобрать для корней уравнений подходящие виды иррациональностей. В случае $x^3=ax+b$ соответствующее выражение известно. Это $x=\sqrt[3]{\alpha}+\sqrt[3]{\beta}$. Для уравнения $x^4=ax^2+bx+c$ Эйлер получал кубическую резольвенту подстановками $x=\sqrt{\alpha}+\sqrt{\beta}+\sqrt{\gamma}$, или $x=\sqrt[4]{\delta}+\sqrt[4]{\varepsilon}+\sqrt[4]{\varphi}$. Однако экстраполировать этот прием, как надеялся Эйлер, вообще на уравнения вида

$$x^n = a_1 x^{n-2} + a_2 x^{n-3} + \ldots + a_{n-1}, \quad n > 4$$

подстановкой

$$x = \sum_{k=1}^{n-1} \sqrt[n]{\alpha_k}$$

не удалось. Около 1764 г. Эйлер обобщил эту подстановку

$$x = \alpha_0 + \sum_{k=1}^{n-1} \beta_k \sqrt[n]{\alpha_k}.$$

Такую же форму подстановки одновременно открыл Варинг. Однако и эта весьма общая подстановка, позднее использованная Абелем для доказательства невозможности решения в радикалах общего уравнения пятой степени, не дала нужного результата.

Число попыток отыскания решения уравнений степени $n \geqslant 5$ элементарно-алгебраическими средствами было очень велико. По существу это был единственный путь решения проблемы, доступный в то время математикам. Он был равнозначен становлению позднейшей алгебраической теории резольвент. Кстати сказать, в ходе этих попыток сформировался и термин «резольвента» из латинского *aequatio resolvens*, что означает: разрешающее уравнение. В современной математике этот термин употребляется в разных смыслах. Мы имеем в виду алгебраический аспект: резольвента алгебраического уравнения $P_n(x)=0$ суть тоже алгебраическое уравнение $g(x)=0$, такое, что: а) его коэффициенты являются рациональными функциями коэффициентов уравнения $P_n(x)=0$, б) знание его корней позволяет найти корни уравнения $P_n(x)=0$ посредством решения уравнений степени,

низшей, чем n. По-видимому, первый, кто ввел термин «резольвента», был Эйлер (около 1732 г.).

Неудачи в поисках алгебраических алгоритмов, упомянутые выше, видимо, были одной из причин появления большого числа работ, посвященных приближенному нахождению корней уравнений как графическими, так и численными методами. Графические методы алгебраисты заимствовали из аналитической геометрии. Выбор кривых для геометрического решения уравнений определялся либо соображениями легкости их построения, либо наименьшей степенью соответствующих этим кривым алгебраических уравнений. Например, многие ученые (Лопиталь, Стирлинг, Бернулли, Ньютон, Крамер и др.) пришли к мысли строить корни уравнения

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0$$

как точки пересечения кривой

$$y = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x$$

и прямой $y=-a_n$. Более поздние построения опирались на графическое суммирование кривых

$$y = a_0x^n,\ y = a_1x^{n-1},\ \ldots,\ y = a_{n-1}x + a_n,$$

для чего был даже придуман специальный прибор.

Среди числовых приближенных методов упомянем метод Ньютона, который он продемонстрировал на примере $y^3-2y-5=0$. Обозначим целочисленную часть корня, с которой начинает Ньютон, буквой ε для общности. Положив $y=\varepsilon+p$, подставив его в уравнение и отбрасывая, в силу малости p, все его степени, кроме первой, найдем приближение p_1 в первом десятичном знаке. Затем, положив $p=p_1+q$, повторяем всю операцию сначала и т. д. Так получаются последовательные приближения корня: $x=\varepsilon,\ p_1\ p_2\ldots$

Уточнение этого метода, принадлежащее Галлею, состоит в том, что берется первое приближение ε корня уравнения $P_n(x)=0$. Затем величина $\varepsilon+p$ подставляется в уравнение, члены которого располагаются по степеням p:

$$P_n(\varepsilon + p) = P_n(\varepsilon) + Ap + Bp^2 + \ldots = 0.$$

Затем p определяется из квадратного уравнения

$$Bp^2 + Ap + P_n(\varepsilon) = 0.$$

Ньютон применил аналогичный метод к решению буквенных уравнений с двумя неизвестными $f(x, y)=0$, или, что то

же самое, к приближенному вычислению значения неявных функций. Связанное с этим разрешение уравнения относительно одного из неизвестных, т. е. представление $f(x, y)=0$ в виде $y=f_1(x)$, где $f_1(x)$ есть степенной ряд, вообще бесконечный, Ньютон производил с помощью специального приема, получившего название параллелограмма Ньютона. Разновидности этого метода известны под названием прямоугольника, треугольника, многоугольника, диаграммы, но неизменно связаны с именем его творца [1].

Численные методы требуют в качестве предварительных данных решения ряда общих вопросов: об определении числа положительных, отрицательных и мнимых корней, об отделении корней и об определении границ, между которыми находятся корни. В XVII в. было рассмотрено большое число частных видов уравнений. М. Ролль в конце века установил, что между двумя корнями уравнения $f'(x)=0$ может находиться не более одного корня уравнения $f(x)=0$. Верхняя граница действительных корней уравнения

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0,$$

по Роллю, равна $|a_k|+1$, где a_k — наибольший по модулю отрицательный коэффициент уравнения.

Не вдаваясь в частности, отметим, что для указанного круга проблем уже в XVII—XVIII вв. были в основном найдены те теоремы, которые сейчас составляют содержание соответствующих глав курсов высшей алгебры [2]. Поэтому мы укажем лишь на редко употребляющийся метод, принадлежащий Лагранжу.

Пусть известно первое приближение p корня x уравнения, такое, что $p<x<p+1$. Подставим в уравнение $x=p+\frac{1}{y}$ Новое уравнение имеет действительный корень $y>1$, так как

$$1>\frac{1}{y}>0, \qquad \varepsilon(y)=q,$$

т. е.

$$y=q+\frac{1}{z}.$$

---

[1] См. ст. Н. Г. Чеботарев. Многоугольник Ньютона и его роль в развитии математики. В кн.: Н. Г. Чеботарев. Собр. соч., т. III, стр. 47—80.

[2] См., например, Г. М. Шапиро. Высшая алгебра. Учпедгиз, М., 1938.

Повторяя этот прием, получим

$$x = p + \cfrac{1}{q + \cfrac{1}{z_+} \ \ldots}.$$

Если цепная дробь обрывается, то корень рационален. Если же он иррационален, то цепные дроби позволяют оценить, с какой погрешностью осуществлено любое последовательное приближение.

Практически приемы решения алгебраических уравнений, накапливаясь, открывали перспективы для развития теоретической части алгебры. Будущее этой науки постепенно раскрывалось в разнообразных теоретических исследованиях, группирующихся вокруг двух проблем (разрешимости алгебраических уравнений в радикалах и доказательства основной теоремы алгебры).

Мы уже указывали[1], что Жирар (1629) и Декарт (1637) впервые установили, что алгебраическое уравнение может иметь столько корней, сколько единиц имеет его наивысшая степень. В XVIII в. постановка этой проблемы трансформировалась. Теперь уже требовалось доказать, что всякое алгебраическое уравнение степени n имеет именно n корней (действительных и комплексных). В качестве эквивалентного утверждения предлагалось доказать разложимость левой части уравнения в произведение линейных и квадратных множителей с действительными коэффициентами. Над решением этой и других связанных с ней проблем трудились Даламбер, Эйлер, Лагранж, Гаусс и многие другие математики.

Первое доказательство было дано Даламбером (1746). Оно состояло в установлении факта, что

$$\min |P_n(x)| = 0.$$

Однако соображения Даламбера были нестрогими, содержали в явной форме апелляцию к средствам математического анализа и не облегчали затруднений алгебраистов.

Полученное почти одновременно доказательство Эйлера (опубликованное в 1751 г.) опиралось на рассмотрение графиков кривых

$$y = P_n(x)$$

[1] См. К. А. Рыбников. История математики, ч. 1, стр. 135.

соответственно при четном и нечетном n. Оказывалось при этом, что уравнение $P_n(x)=0$ при n нечетном имеет один вещественный корень или нечетное их число, при n четном существует четное число вещественных корней или же их вовсе нет; если свободный член уравнения четной степени отрицателен, то уравнение имеет во всяком случае два вещественных корня разных знаков. Трудность была тем самым сведена к доказательству теоремы для уравнений четной степени $2m$. Так как $2^{n-1}<2m<2^n$, то, домножая уравнение 2^n-2m линейными множителями вида $x-\alpha$, видим, что доказательство достаточно проводить для уравнений, степени которых имеют вид 2^n. Относительно уравнений последнего типа Эйлер высказал важную теорему: левая часть алгебраического уравнения степени 2^n ($n>1$, целое) разлагается на два множителя степени 2^{n-1}, и наметил пути ее доказательства [1].

При этом он нашел два важных свойства алгебраических уравнений: а) рациональная функция корней уравнения, которая принимает при всех возможных подстановках корней κ различных значений, удовлетворяет алгебраическому уравнению степени κ, коэффициенты которого суть рациональные функции коэффициентов данного уравнения; б) рациональная функция корней уравнения, инвариантная относительно перестановок корней, есть рациональная функция коэффициентов исходного уравнения.

Уточняя доказательство Эйлера, Лагранж ввел и разработал теорию подобных функций, т. е. функций, инвариантных при подстановках одной и той же группы и только при них. У Лагранжа речь идет о подобии симметрических функций корней уравнения в случае, если все 2κ значений, которые способны они принимать при всех перестановках корней, различны между собой. Относительно подобных функций Лагранж доказал, что они рационально выражаются друг через друга и через коэффициенты данного уравнения.

Смысл доказательств Эйлера и Лагранжа с современной точки зрения таков. Пусть дано уравнение $P_n(x)=0$. Его коэффициенты — элементы поля D действительных чисел. K — поле Галуа данного уравнения. Степень K над D: $n=2^r\cdot\kappa$ (κ — нечетное). По теореме Силова, существует подгруппа H порядка 2^r группы Галуа G этого уравнения. Образуем

---

[1] См. И. Г. Башмакова. О доказательстве основной теоремы алгебры. В сб.: «Историко-математические исследования», вып. X. Гостехиздат, М., 1957, стр. 257—304.

q — поле элементов, инвариантных относительно подстановок из H:

$$D \subset q \subset K.$$

Степень K над q есть 2^r, степень q над D — нечетное κ. Поле q образуется присоединением к D корня v неприводимого над D многочлена $P_1(x)$ степени κ. Но κ нечетно; следовательно, $q=D$[2] [1].

Рассмотрим K над D. Его степень 2^r. Если $K = D(\eta)$, то η — есть корень уравнения $P_2(x)=0$ степени 2^r с действительными коэффициентами, как в уравнениях, рассматривавшихся Эйлером.

Известно, что группы порядка степени простого числа, т. е. p^r разрешимы; их нормальные делители имеют простые порядки p. Здесь же $p = 2$. Значит,

$$D \subset K_1 \subset \ldots \subset K_r = K,$$

где каждое из промежуточных нормальных полей квадратичное по отношению к предыдущему. Соответствующие квадратные уравнения, которые нужно решать над предыдущим полем, чтобы получить последующее, имеют либо действительные, либо комплексные корни. Пусть K_i —первое поле, совпадающее с полем комплексных чисел; последующие поля будут тоже совпадать с этим же полем. В противном случае все поля совпадут с D.

Обратно, если исходить из $K = K_r$, то для отыскания корня уравнения $P_2(x) = 0$ степени 2^r надо решить над D одно уравнение степени 2^{r-1}. Его корни породят поле K_{r-1}, а над ним — одно квадратное уравнение. Возможно повторение этого рассуждения для степени на единицу ниже и т. д.

Элементы этих идей новой алгебры явственно угадываются в доказательствах Эйлера и Лагранжа.

Другая группа элементов теории Галуа была накоплена в ряде исследований проблемы приводимости уравнений. Ньютон первый вышел за пределы вопроса о приводимости уравнений над полем рациональных чисел. Он предложил алгоритм для решения вопроса о том, может ли уравнение «быть приведено при помощи какого-либо иррационального делителя, или, что то же самое... нельзя ли так разделить уравнение на две равных части, чтобы из каждой вы могли извлечь корень» [2].

[1] Так как единственными неприводимыми уравнениями нечетной степени над полем действительных чисел являются линейные уравнения.

[2] И. Ньютон. Всеобщая арифметика. Изд-во АН СССР, М., 1948, стр. 270.

Помимо постановки вопроса о возможности приведения уравнения над различными областями это рассуждение содержит некоторую идею теории Галуа. В самом деле, Ньютон ставит по существу вопрос о присоединении к полю рациональных чисел иррациональностей вида $\sqrt{\kappa}$ и о приводимости уравнения над этим расширенным полем. Иначе говоря, речь идет об отыскании квадратичных подполей поля разложения полинома.

Алгоритмы Ньютона, а вслед за ним и Варинга для решения вопроса о том, распадется ли заданное уравнение на множители, если область рациональных чисел расширить присоединением квадратичной, биквадратичной или кубической иррациональности, просты, но громоздки. Ньютон и Варинг представляли всякий раз полином в виде произведения множителей с неопределенными коэффициентами, зависящими от иррациональностей исследуемого вида. Затем следовали попытки такого подбора неопределенных коэффициентов, чтобы искомое разложение осуществилось.

Громоздкие методы не открывали перспектив и приводили к ошибкам. Тем не менее они были полезны. В них фактически рассматривались поля алгебраических чисел, определялся общий вид элементов этих полей.

Накопление предпосылок нового этапа развития алгебры в XVIII в. достигает кульминационного пункта в исследованиях Лагранжа, нашедших отражение в его «Размышлениях об алгебраическом решении уравнений» (1771—1772). В этом сочинении Лагранж критически пересмотрел все накопившиеся к тому времени методы и попытки решения алгебраических уравнений. К открытым уже резольвентам он добавил еще одну, весьма общего характера.

Он рассмотрел алгебраическое уравнение

$$x^n + b_1 x^{n-1} + b_2 x^{n-2} + \ldots = 0$$

и, в соответствии с методом Чирнгаузена, вспомогательное уравнение

$$y = -(x^{n-1} + fx^{n-2} + gx^{n-3} + \ldots + \kappa)$$

с неопределенными коэффициентами f, g, ..., κ. Исключим x из обоих уравнений:

$$y^n + Ay^{n-1} + By^{n-2} + \ldots + Py + T = 0.$$

Подберем коэффициенты f, g, ..., так, чтобы

$$A = B = \ldots = P = 0.$$

Тогда решение заданного уравнения сведется к решению системы уравнений: $y^n = -T$ и $n-1$ уравнения, в которых находятся неопределенные коэффициенты $f, g, \ldots$. Корни первого из уравнений будут:

$$y_1 = \sqrt[n]{-T},\ y_1\alpha,\ y_1\alpha^2, \ldots, y_1\alpha^{n-1},$$

где $\alpha, \alpha^2, \ldots, \alpha^{n-1}$ — первообразные корни единицы (корни уравнения $y^n - 1 = 0$). Подставляя эти значения в выражение для x:

$$x = a_0 + a_1 y + a_2 y^2 + \ldots + a_{n-1} y^{n-1},$$

получим систему n уравнений:

$$x_1 = a_0 + a_1 y_1 + a_2 y_1^2 + \ldots + a_{n-1} y_1^{n-1};$$

$$x_2 = a_0 + a_1 y_1 \alpha + a_2 y_1^2 \alpha^2 + \ldots + a_{n-1} y_1^{n-1} \alpha^{n-1};$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$x_n = a_0 + a_1 y_1 \alpha^{n-1} + a_2 y_1^2 \alpha^{n-2} + \ldots + a_{n-1} y_1^{n-1} \alpha.$$

Вследствие того, что

$$1 + \alpha + \alpha^2 + \ldots = 0;$$

$$1 + \alpha^2 + \alpha^4 + \ldots = 0;$$

$$\ldots\ldots\ldots\ldots$$

получим

$$na_0 = x_1 + x_2 + x_3 + \ldots$$

$$na_1 y_1 = x_1 + \alpha^{n-1} x_2 + \alpha^{2(n-1)} x_3 + \ldots$$

$$na_2 y_1 = x_1 + \alpha^{n-2} x_2 + \alpha^{2(n-2)} x_3 + \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Упростим систему с учетом $\sum_{i=1}^{n} x_i = -m$, откуда $a_0 = -\frac{m}{n}$. Положив

$$T = -y_1^n = -1,\ a_{n-1} = \frac{c^1}{n},\quad a_{n-2} = \frac{c''}{n}, \ldots,$$

$$a_1 = \frac{c^{(n-1)}}{n},$$

получим

$$t = x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots$$

линейную функцию корней уравнения, названную позднее резольвентой Лагранжа.

Функция $\theta = t^n$ при всех перестановках

$$\begin{pmatrix} x_1, & x_2, & \ldots, x_n \\ x_{i1}, & x_{i2}, & \ldots, x_{in} \end{pmatrix}$$

корней уравнения $P_n(x) = 0$ принимает $\kappa \leqslant n!$ значений. Коэффициенты уравнения

$$\theta^k + b_1\theta^{k-1} + \ldots + b_k = \prod_{i=1}^{k} (\theta - \theta_i) = 0$$

суть симметрические функции от θ_i $(i = 1, 2, \ldots, k)$. Последние в свою очередь являются симметрическими функциями корней x_i $(i=1, 2, \ldots, n)$. Следовательно, корни x_i $(i=1, 2, \ldots, n)$ можно определить через $k \leqslant n!$ корней θ_k.

Однако все известные для уравнений степени $n \leqslant 4$ способы отыскания резольвент, приводят при $n \geqslant 5$ к резольвенте степени $k > n$. Это заставило Лагранжа сомневаться в том, что рассмотренные им методы могли решать уравнения степени $n \geqslant 5$. Однако он считал, что рассмотренные им группы подстановок корней уравнений являются «дорогой к решению», так как он обнаружил на этом пути решения класса так называемых циклических уравнений, т. е. уравнений с циклической группой подстановок.

Лагранж достиг весьма большой общности. Он рассматривал уравнения с произвольными буквенными коэффициентами. Относительно их он исследовал поля рациональных функций корней. Он ввел группу подстановок корней уравнения (симметрическую группу) и изучил соответствие между ее подгруппами и подполями рациональных функций, инвариантных относительно подстановок этих подгрупп. Наконец, Лагранж доказал и первые теоремы теории групп, например, что порядок подгруппы есть делитель порядка группы.

Вслед за Лагранжем подстановки корней уравнений подверг изучению Руффини. Он предложил в 1799 г. доказательство неразрешимости в радикалах уравнения степени $n \geqslant 5$. Однако это доказательство не было общим, так как Руффини принял без доказательства, что корни резольвент рационально выражаются через корни исходного уравнения. В последующих работах, появившихся в 1801, 1802, 1806 и 1813 гг., он пытался доказать это предложение, но полного обоснования так и не смог добиться. Однако он провел си-

стематическое исследование конечных перестановок и доказал ряд важных теорем. При этом он впервые ввел термин «группа». В 1814 г. Руффини открыл и сформулировал правило приближенного вычисления корней уравнений, переоткрытое в 1819 г. Горнером.

Алгебра, таким образом, развивалась в течение XVIII в. как наука о решении алгебраических уравнений. В ней получили известное завершение проблемы, связанные с элементарно-математическими средствами решения уравнений. Были разработаны основные предпосылки для создания теории Галуа и теории групп. Алгебра на рубеже XIX в. находилась накануне коренной перестройки, сделавшей ее соединением ряда алгебраических наук, предметом изучения которых стали объекты сложной и абстрактной природы: группы, поля, кольца и т. д.

Развитие алгебры в этот период демонстрирует еще раз общую закономерность развития математики: новые области математики рождаются в недрах старых, их основные понятия и методы оперирования проходят период «эмбрионального» развития. Затем происходит возникновение новой математической дисциплины. Характерной особенностью процесса возникновения является переворот в методе. Выделение сопровождается возникновением нового символического аппарата, несущего двоякую роль: отражения реальных математических процессов и оперативную. Новыми областями в данном случае являются теория Галуа и теория групп.

Теория чисел. В первой части настоящей книги и в ряде глав второй части мы неоднократно отмечали отдельные факты истории теории чисел. Эта область математики, в которой изучаются свойства целых, рациональных и алгебраических чисел, а также свойства любых других чисел, вытекающие из приближений их рациональными числами, выросла из арифметики. В XVIII в. она еще тесно была связана с алгеброй. Однако своеобразие проблематики и методов теории чисел уже осознавалось достаточно определенно. Накопившийся запас теоретико-числовых фактов также способствовал выделению теории чисел в особую область математики. Ниже мы даем очерк основных моментов истории теории чисел.

Еще в Древней Греции, как мы упоминали, были выделены по принципу общности свойств различные подмножества целых чисел: простые, квадратные, совершенные, полигональные, составляющие пифагорейские тройки и др. Там же была разработана стройная теория делимости, доказана бесконечность числа простых чисел в натуральном ряде, изобретен ал-

горитм Евклида. Сочинения Диофанта представили много примеров раннего и высокого развития неопределенного анализа. История математики в Китае и Индии свидетельствует о раннем появлении ряда теорем теории сравнений и других фактов теории чисел.

Однако развитие теории чисел происходило весьма медленно. Между новыми открытиями проходили десятилетия, а иногда и века. Теоретико-числовые результаты достигались в большинстве выдающимися учеными и оставались изолированными. Возможными причинами этого являлись: специфичность предмета теории чисел, возрастающая абстрактность в постановке задач этой теории, необычайная трудность их решения, требующая высокого развития математики и незаурядных личных качеств ученого. В силу этих причин существенное обогащение теории чисел и ее формирование и обособление имели место лишь в XVII—XVIII вв. В этот период ее проблемами занимались несколько крупных ученых: Ферма, Декарт, Б. Паскаль, Валлис, Лейбниц, Эйлер и др.

В течение XVII в. наибольших результатов добился П. Ферма. В его переписке и на полях принадлежавшей ему книги сочинений Диофанта содержится большое число теоретико-числовых результатов. В частности, Ферма записал там свою знаменитую «великую» теорему: уравнение $x^n + y^n = z^n$ для целых показателей при $n > 2$ неразрешимо в целых числах. Приписка Ферма гласила, что он владеет поистине чудесным доказательством, но на полях недостаточно места, чтобы его записать. Однако общее доказательство этой теоремы не найдено до настоящего времени, хотя ею занимались многие величайшие математики и бесчисленное множество любителей. Теорема приобрела популярность в начале XX в., когда за решение этой задачи некий Вольфскель установил премию в 100 тысяч марок (премия была отменена в конце первой мировой войны).

Своей постановкой великая теорема, по-видимому, была обязана стремлению Ферма обобщить теорему о составлении пифагорейских троек целых чисел [1]. Тот же источник, древнегреческую математику, можно с большой уверенностью назвать и для малой теоремы Ферма [2]. В связи с этим он исследовал делимость чисел и проблему нахождения всех делителей заданного числа. К этому же кругу вопросов относятся работы Ферма о совершенных и других числах специальной структуры.

[1] См. К. А. Рыбников. История математики, ч. 1, стр. 27.
[2] См. там же, стр. 186.

Большое место в исследованиях Ферма, разумеется, занял неопределенный анализ Диофанта, т. е. целочисленные решения неопределенных уравнений и их систем. Особенное внимание он уделил уравнениям вида $ax^2 + 1 = y^2$, где a не есть точный квадрат. Относительно этого уравнения (за которым впоследствии, в силу случайной обмолвки Эйлера, утвердилось наименование теоремы Пелля) Ферма умел а) находить его наименьшее решение; б) получать, зная наименьшее, все остальные решения.

К XVIII в. в математике накопилось много теоретико-числовых фактов, порой весьма важных и сослуживших в дальнейшем полезную службу при появлении новых областей математики. Однако эти факты не были систематизированы, связи между ними не раскрыты, возможности применяемых методов не изучены. К тому же после работ Ферма, Паскаля и др. в теории чисел наступило полувековое затишье, почти непрерываемое, вплоть до того времени, когда теорией чисел занялся Эйлер. С его именем связано становление теории чисел как науки. Проблемы этой области математики находились в поле зрения Эйлера в течение всей его жизни. Им он посвятил, как подсчитано, огромное число работ: около 150.

По-видимому, первым стимулом к занятиям Эйлера теорией чисел была переписка с Гольдбахом. Последний в письме от 1 декабря 1729 г. спрашивал: «Известно ли тебе замечание Ферма о том, что все числа вида $2^{2^{x-1}} + 1$, именно 3, 5, 17 и т. д., суть простые, причем сам он, по его признанию, не смог этого доказать, и, насколько я знаю, после него никто не доказал» [1].

Вскоре (1732—1733) Эйлер доказал, что теорема Ферма неверна уже для $x = 6$, ибо число $2^{2^5} + 1 = 4\,294\,967\,297$ делится на 641. Кроме того, он доказал ряд теорем, относящихся к проблеме делимости, в том числе малую теорему Ферма.

Нахождение доказательств, обобщений или опровержений теорем Ферма было только первым этапом теоретико-числовых исследований Эйлера. В последующем он охватил и развил все основные разделы теории чисел, как алгебраической, так и аналитической, определив ее состав и методы на много лет вперед.

---

[1] Correspondance mathématique et physique de quelques célèbres géomètres du XVIII siècle, t. I. St. Pet., 1843, S. 10.

Работы Эйлера определили проблематику, структуру и методы алгебраической теории чисел, т. е. той ее части, в которой используются по преимуществу методы арифметики и алгебры и не привлекается по возможности аппарат теории функций и анализа бесконечно малых.

Здесь ему прежде всего принадлежат работы по теории делимости, выросшей к нашему времени в теорию сравнений. Помимо доказательства малой теоремы Ферма Эйлер ввел функцию $\varphi(m)$, значение которой равно числу чисел, меньших m и взаимно простых с ним. Относительно этой функции он доказал, что если a и b взаимно просты, то $\varphi(ab) = \varphi(a)\varphi(b)$ и что $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, если p — простое и α — целое. Затем он нашел выражение $\varphi(m)$ для произвольного m, если известно представление m в виде произведения простых чисел, и доказал, что $a^{\varphi(m)} - 1$ делится на m, если a и m — взаимно просты.

Эйлер ввел понятие первообразного корня по модулю m: число g называется первообразным корнем по модулю m, если $g^k - 1$ делится на m тогда и только тогда, когда k кратно $\varphi(m)$. Им введено также понятие индекса числа N по модулю m при основании g, т. е. показателя степени κ числа g, такого, что разность $g^k - N$ делится на m. Он нашел ряд свойств индексов, доказал существование первообразного корня по любому простому p и теорему Вильсона: $(m-1)! + 1$ делится на m, если m — простое число.

Эйлер ввел понятие степенных вычетов и создал их теорию. Число a он назвал вычетом степени n по модулю p, если существует такое целое число x, что $x^n - a$ делится на p. Он показал, что свойства степенных вычетов важны не только для решения двучленных сравнений

$$x^n - a \equiv 0 \pmod{p},$$

но и для других задач, например для задачи представления чисел квадратичными формами. Занимаясь свойствами квадратичных вычетов, он открыл (1722) знаменитый и теперь закон взаимности: даны два простых числа p и q; если хотя бы одно из них имеет вид $4n+1$, то сравнения

$$x^2 \equiv p \pmod{q}, \tag{1}$$

$$x^2 \equiv q \pmod{p} \tag{2}$$

являются одновременно разрешимыми. Если же и p и q имеют вид $4n+3$, то из разрешимости одного из уравнений следует неразрешимость другого.

После Эйлера квадратичный закон взаимности доказал Лежандр.[1] Гаусс до 1801 г. дал восемь доказательств этого закона. Наконец, Лежандр к 1808 г. нашел удобную форму записи квадратичного закона взаимности:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

введя символ

$$\left(\frac{p}{q}\right) = \begin{cases} +1, \text{ если } p \text{ есть квадратичный вычет по mod } q \\ -1, \text{ если } p \text{ есть квадратичный невычет по mod } q \end{cases}.$$

Не менее велики заслуги Эйлера в разработке проблем диофантова анализа (решения неопределенных уравнений в целых и рациональных числах), для нужд которого он разработал и строго обосновал теорию непрерывных дробей. Здесь прежде всего заслуживает упоминания доказательство великой теоремы Ферма для $n = 3$ и $n = 4$. Для этого Эйлер использовал и развил метод спуска, изобретенный Ферма. Этот метод состоит в следующем. Пусть существует нетривиальное решение (x_0, y_0, z_0) уравнения Ферма, удовлетворяющее условию $x_0y_0z_0 \neq 0$. Тогда оказывается возможным найти другое нетривиальное решение (x_1, y_1, z_1), элементы которого также натуральны и соответственно меньшие по величине, чем (x_0, y_0, z_0). Продолжая, мы придем к неограниченной последовательности убывающих троек натуральных чисел, т. е. к противоречию. Эйлер доказал множество теорем, примыкающих к указанной теореме Ферма, более подробное рассмотрение и перечисление которых представляло бы интерес лишь для специалистов.

Из других задач диофантова анализа Эйлер уделил большое внимание задаче отыскания целочисленных решений уравнения второго порядка с двумя неизвестными и с целыми коэффициентами

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

Вопрос о получении бесконечного числа решений, если известно одно решение (x_0, y_0), Эйлер свел к решению уравнения Пелля

$$x^2 - Dy^2 = 1$$

(D — натуральное, не квадратное число).

В широкую и разветвленную алгебраическую теорию чисел, создаваемую Эйлером, входят работы о представлении чисел квадратичными формами $ax^2 + by^2$. Еще Валлис (1685)

[1] Однако доказательство Лежандра было неполным.

утверждал, что всякое число можно разложить на множители единственным образом. Ему принадлежит теорема, что число простых делителей числа $m = p^{\lambda} \cdot q^{\mu} \cdot r^{\nu}$ (p, q, r... — простые) равно $(\lambda+1)(\mu+1)(\nu+1)$..., а их сумма равна

$$\frac{p^{\lambda+1}-1}{p-1} \cdot \frac{q^{\mu+1}-1}{q-1} \cdot \frac{r^{\nu+1}-1}{r-1} \cdots$$

Для нахождения простых делителей больших чисел Эйлер и строил метод, основанный на представлении этих делителей в виде квадратичных форм. Последние должны обладать тем свойством, что простые числа представляются, если возможно, единственным образом, а сложные — неединственным или не представляются вообще. Оказалось, что подобное свойство зависит от произведения $n = ab$. Те числа n, которые порождают подобные формы, Эйлер назвал удобными и нашел критерий удобности числа: число n является удобным, если для каждого целого $x < \sqrt{3n}$, взаимно простого с n, сумма $n + x^2$ будет или простое, или удвоенное простое, или квадрат простого, или степень числа два. Удобных чисел Эйлер нашел 65, наибольшее из них — 1848. Предположение Эйлера, что 1848 — последнее удобное число, до сих пор не доказано.

В трудах Эйлера содержались все предпосылки для создания системы алгебраических методов теории чисел. Они послужили источником для позднейших исследований. Например, исследования Эйлера о представлении чисел значениями квадратичных форм и о виде простых делителей легли в основу созданной Гауссом общей теории квадратичных форм. Попытка Куммера (1847) продолжить работу Эйлера по решению великой теоремы Ферма, помимо доказательства ее для $n \leqslant 100$, привела к открытию отсутствия единственности разложения на простые множители в алгебраических полях и к созданию теории идеалов. Работы по теории сравнений и открытие квадратичного закона взаимности повлекли обобщения Э. Куммера, Д. Гильберта и др., завершенные наиболее общей формой этого закона, найденной и доказанной И. Р. Шафаревичем.

Особо важным этапом развития теории чисел являлось применение к решению ее задач методов математического анализа. Эта часть теории чисел — аналитическая — берет свое начало также в XVIII в. в трудах Эйлера. Последний разработал аналитические методы для решения проблемы распределения простых чисел в ряду натуральных чисел, а

также для ряда аддитивных проблем. Эти методы раскрывают связи между свойствами целых чисел и свойствами аналитических функций.

Первая из указанных проблем получила для своего решения методы, основанные на применении так называемой дзета-функции, введенной Эйлером,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

и тождества Эйлера

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - \frac{1}{p^s}}$$

(n — натуральные, p — простые).

Рассматривая значения обеих частей этого тождества при $s > 1$ и сколь угодно близких к единице, Эйлер смог дать аналитическое доказательство известного со времен Евклида факта бесконечности числа простых чисел в натуральном ряду. Кроме того, он высказал утверждение (не дав ему строгого доказательства):

$$\sum_{p \leqslant x} \frac{1}{p} \cong \ln \sum_{n \leqslant x} \frac{1}{n}.$$

Настойчивые поиски аналитически выраженного закона распределения простых чисел, как известно, не привели к успеху до сих пор. Некоторые подходы к решению, впервые после Евклида, появились у Эйлера, высказавшего предположение, что неограниченная арифметическая прогрессия, a_0 и d которой — простые, содержит неограниченно много простых чисел. Лежандр, разделявший с Эйлером эту уверенность, тоже не дал доказательства. Доказать гипотезу Эйлера удалось только в 1837 г. Дирихле.

Лишь в 1798 г. Лежандр отыскал эмпирическую формулу для функции $\pi(x)$, значения которой равны числу простых чисел $p \leqslant x$:

$$\pi(x) = \frac{x}{\ln x - 1{,}08366}.$$

Позднее Чебышев (1848) установил, что $\pi(x)$ при возрастании x колеблется около отрезков ряда, асимптотически приближающего

$$\mathrm{Li}(x) = \int_2^x \frac{dx}{\ln x},$$

и дал близкие оценки амплитуды этих колебаний.

Для комплексной плоскости Риман заметил, что порядок разности $\pi(x) - \mathrm{Li}(x)$ зависит от расположения так называемых нетривиальных нулей функции $\zeta(s)$, действительные части которых лежат между нулем и единицей. Он высказал также гипотезу, что все действительные части при этом лежат на прямой $x = \frac{1}{2}$. Строгое доказательство для оценки значения $\pi(x)$ в предельном случае

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{Li}(x)} = 1$$

появилось лишь в 1896 г. Относительно же гипотезы Римана авторы настоящего доказательства Адамар и Валле-Пуссен смогли найти только, что на прямой

$$x = 1, \quad s = x + iy$$

нет нулей $\zeta(s)$.

Весьма значительным является вклад математиков XVIII в. (по преимуществу Эйлера) в аддитивную теорию чисел, где изучаются разложения больших целых чисел N на слагаемые

$$N = a_{1i_1} + a_{2i_2} + \ldots + a_{si_s},$$

взятые из некоторых числовых последовательностей $\{a_{jk}\}$.

Задачи аддитивной теории чисел (или, как ее тогда называли partitio numerorum) ведут свое происхождение, по-видимому, от задачи Фибоначчи[1] о гирях: как подобрать числа (веса гирь), a_1, a_2, a_3, ..., чтобы всякое число могло быть представлено как их сумма. Лейбниц (1674) в связи с этой задачей отметил, что число 3 допускает три разбиения, 4 — пять разбиений, 5 — семь, 6 — одиннадцать, а 7 — пятнадцать разбиений.

Эйлер занимался проблемами partitio numerorum с 1741 г. Он исходил из двух бесконечных произведений

$$\prod_1^\infty (1 + a_k z) \quad \text{и} \quad \prod_1^\infty (1 - a_k z)^{-1}.$$

[1] См. К. А. Рыбников. История математики, ч. 1, стр. 111.

Разложим вслед за Эйлером эти произведения в ряд по степеням z. Коэффициент при z^n первого степенного ряда есть сумма всех произведений по n в каждом из чисел a_k без повторений. Во втором ряду будут те же суммы, но с произвольными повторениями a_k.

Для решения задачи о числе представлений целого числа N суммами k натуральных чисел, одинаковых или различных, Эйлер рассматривал два произведения:

$$f_1(x) = \prod_1^{\infty} (1 + x^k z) = \sum_0^{\infty} A_k(x)\, z^k;$$

$$f_2(x) = \prod_1^{\infty} (1 + x^k z)^{-1} = \sum_0^{\infty} B_k(x)\, z^k,$$

где

$$A_n(x) = \sum_{k=1}^{\infty} a_{nk} x^k; \quad B_n(x) = \sum_{k=1}^{\infty} b_{nk} x^k.$$

Здесь $a_{n,\,k}$ — число представлений числа κ в виде суммы n различных положительных слагаемых, а $b_{n,\,k}$ — число представлений κ в виде суммы n произвольных положительных слагаемых без учета порядка сложения.

Далее, Эйлер находил функциональные уравнения для $f_1(z)$ и $f_2(z)$ и с их помощью определял функции $A_n(x)$ и $B_n(x)$:

$$A_n(x) = \frac{x^{\frac{n(n+\nu)}{2}}}{(1-x)\ldots(1-x^n)}; \quad B_n(x) = \frac{x^n}{(1-x)\ldots(1-x^n)}.$$

Разлагая в степенной ряд функцию

$$\frac{1}{(1-x)\ldots(1-x^n)} = \sum_{k=0}^{\infty} C_{n,k} x^k,$$

Эйлер свел свою задачу к задаче отыскания числа решений уравнения

$$N = \sum_{k=1}^{n} k x_k$$

в целых неотрицательных числах $x_1, \ldots, x_n$, которое равно $C_{n,N}$. Он построил для этого таблицу чисел $C_{n,N}$.

Далее, переходя к определению чисел C_n из

$$\sum_0^\infty C_n x^n = \prod_{k=1}^\infty \frac{1}{1-x^k},$$

или, что то же, к определению числа решений уравнения

$$N = \sum_{k=1}^n k x_k$$

в целых неотрицательных $x_1, \ldots, x_n$, он эмпирически нашел, что

$$\prod_1^\infty (1-x^n) = 1 + \sum_1^\infty (-1)^n \left(x^{\frac{3n^2-n}{2}} + x^{\frac{3n^2+n}{2}} \right).$$

Опираясь на соотношения между произведениями и степенными рядами, Эйлер доказал много предложений о числе разнообразных представлений целых чисел. Отметим здесь два из них:

во-первых, тождество для суммы делителей числа n ($\int$ — знак суммы)

$$\int(n) = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) +$$
$$+ (-1)^k \left[\int\left(n - \frac{3k^2-k}{2}\right) + \int\left(n - \frac{3k^2+k}{2}\right) \right];$$

во-вторых, теорему, что всякое целое число может быть единственным образом представлено суммой степеней числа 2, что вытекает из

$$\prod_0^n (1 + x^{2k}) = \sum_0^\infty x^n.$$

Метод Эйлера по существу являлся методом производящих функций. После примерно столетнего перерыва, с конца XIX в., этот метод нашел широкие применения как в теории чисел, так и в других математических дисциплинах: комбинаторном анализе, теории вероятностей и др. В теории чисел он

был существенно усовершенствован И. М. Виноградовым, а также Г. Харди и Дж. Литлвудом.

К аддитивным задачам теории чисел, поставленным в XVIII в., относится и задача Варинга (1770): всякое натуральное число $\geqslant 2$ представимо суммой n-ных степеней натуральных чисел, причем число членов r суммы зависит только от n. Варинг не дал ее доказательства. Как и в большинстве задач теории чисел, успех и в этом случае достигался трудно. Так Лагранж доказал, что для $n=2$, $r=4$. Затем было установлено, что для $n=3$, $r \leqslant 7$, что $r>n$. Лишь в 1909 г. Гильберт дал первое общее доказательство. Он установил, что r — конечно для всех n, но не смог дать для r достаточно хорошую оценку. В 1919 г. Харди и Литлвуд нашли, что $r \leqslant n \cdot 2^{n-1}$, а позднее, что $r \leqslant (n-2)2^{n-1}+5$. В 1934 г. И. М. Виноградов при помощи созданного им нового метода тригонометрических сумм существенно продвинул задачу Варинга, дав почти исчерпывающую оценку $r \leqslant 3n(\ln n + 11)$ для больших n. Этим же методом он доказал одну из проблем Гольдбаха, что всякое достаточно большое нечетное число является суммой трех простых чисел. Две другие проблемы Гольдбаха: всякое четное число есть сумма двух простых и всякое нечетное число есть сумма простого и двух квадратов — остаются нерешенными до настоящего времени.

В завершение нашего обзора аналитических методов теории чисел XVIII в. мы упомянем исследования об арифметической природе чисел. В части, относящейся к числам π и e, применение аппарата цепных дробей, разработанного главным образом Эйлером, позволило Ламберту в 1767 г. доказать иррациональность числа π[1], а также e^m для m — рационального. Трансцендентность этих чисел была установлена лишь в конце XIX в.: доказательство трансцендентности числа e дано в 1873 г. Ш. Эрмитом, а числа π — в 1882 г. Ф. Линдеманом. К работам Эйлера относится постановка проблемы об арифметической природе чисел типа $a^{\sqrt{n}} = b$. Эйлер во «Введении в анализ бесконечно малых» (1748; § 105) указывал, что логарифм рационального числа при рациональном основании, если он не целый, должен быть трансцендентным. В частности, он утверждал, что в выражении $a^{\sqrt{n}} = b$ (где n не есть квадратное число) a и b не могут быть одновременно рациональными. В более общем виде

[1] См. И. Г. Ламберт. Предварительные сведения для ищущих квадратуру и спрямление круга. В сб.: «О квадратуре круга». ГТТИ. М.—Л., 1934, стр. 105—166.

эту проблему сформулировал Д. Гильберт, как проблему об арифметической природе чисел a^b, для a и b алгебраических. В 1929—1934 гг. А. О. Гельфонд полностью решил эту задачу, доказав, что число вида a^b (где a — алгебраическое, отличное от нуля и единицы, а b — алгебраическая иррациональность) является трансцендентным.

Теория чисел в XVIII в. по существу переросла в отдельную область математики. В ней определились практически все главные проблемы и направления. В сочинениях Эйлера, Лагранжа, Лежандра, Ламберта и других математиков были выработаны многочисленные методы теории чисел, как элементарно-алгебраические, так и аналитические. Все эти исследования, естественно, нуждались в систематизации, в приведении к логически-стройной структуре с единых позиций. Эта работа в конце XVIII в. была начата Лежандром, который выпустил в 1797—1798 гг. «Опыт теории чисел», имея целью построить систему сведений о свойствах целых чисел. В дальнейших переизданиях он дополнял ее результатами Гаусса, Абеля и других математиков XIX в. В двух томах этой книги содержится огромный материал, накопленный в теории чисел, что придает ей помимо исторического практическое значение, как весьма полезного справочника.

Характер и направление исследований по теории чисел в течение почти всего XIX в. были, по существу, определены работами Гаусса. Свое основное сочинение в этой области — «Арифметические исследования» — Гаусс начал в 1797 г., и к 1801 г., когда его автору было всего 24 года, оно вышло в свет. Последующие теоретико-числовые работы Гаусса появились в 1811 г. и в период 1828—1832 гг.; это свидетельствует о постоянном интересе Гаусса к теории чисел.

Открытия Гаусса в теории чисел огромны. Мы, к счастью, имеем возможность отослать заинтересованного читателя к прекрасной статье Б. Н. Делоне «Работы Гаусса по теории чисел»[1], ограничившись здесь краткими и предварительными оценками.

Мы уже упоминали, что Гаусс много сил отдал изучению квадратичного закона взаимности, дав ему 8 (!) строгих доказательств. Изучая квадратичные формы, он по существу создал арифметику квадратичных расширений. Эта часть его исследований послужила исходным пунктом и образцом для последующей разработки арифметики алгебраических расши-

---

[1] В сб. «Карл Фридрих Гаусс» Изд-во АН СССР, М., 1956, стр. 11—112.

рений, вплоть до работ Д. Гильберта по теории полей классов.

Гаусс открыл и доказал биквадратичный закон взаимности и построил арифметику целых комплексных чисел. Аппарат теории сравнений, столь употребительный в наши дни, обязан своим возникновением Гауссу. Для построения в XIX в. теории алгебраических чисел эта группа открытий Гаусса послужила отправным пунктом и образцом.

В своих исследованиях Гаусс ввел и изучил целый ряд групп: группу классов форм одного дискриминанта, группу родов и др. На конкретных примерах он первый изучил структуру абелевых групп. В частности, он показал, что абелева группа является прямым произведением групп циклических, доказав тем самым основную теорему теории абелевых групп.

Считается общепризнанным, что со времени работ Гаусса теория чисел развивается уже как стройная теория[1], задачи которой побуждают к развитию новых и тонких методов анализа (в особенности теории функций комплексного переменного), алгебры и даже геометрии. Определились и основные направления теории чисел. Это: а) разработка специальных методов теории чисел, носящих иногда название элементарных; б) аналитические методы, применяемые по преимуществу к задачам распределения; в) диофантовы уравнения и диофантовы приближения.

Далее мы будем иметь возможность возвращаться к вопросам развития теории чисел (например, в связи с рассмотрением фундаментальных исследований П. Л. Чебышева). При этом, однако, характер и размеры настоящей книги не позволят нам дать общий, более или менее детальный, обзор теории чисел и ее взаимосвязей с другими математическими науками.

Методы теории вероятностей и комбинаторного анализа. Обзор развития математики в XVIII в., предпринятый нами в первых шести главах, был бы неполон, если бы мы опустили теоретико-вероятностные работы и применяемый в них аппарат. По-видимому, теория вероятностей в те времена не занимала еще заметного места среди других дисциплин. Но будущие успехи математики (как и вообще науки), получая необходимые предпосылки в наиболее развитых ее областях, выкристаллизовываются, выделяются чаще всего в областях

---

[1] См. А. О. Гельфонд и Ю. В. Линник. Чисел теория. БСЭ, т. 47, стр. 386.

К. Ф. Гаусс
1777—1855

новых, еще количественно небольших и зачастую слабо развитых.

Теория вероятностей в XVIII в. расширила сферу своих приложений. Помимо азартных игр ее методы проникли в статистику (в частности, в демографию), страховое дело, теорию ошибок наблюдений, теорию стрельбы. Это расширение происходило в тесной связи с обогащением математических методов и результатов теории вероятностей.

Наиболее ранним теоретическим результатом в этой области было, по-видимому, доказательство Муавром (1730) локальной предельной теоремы, оценивающей асимптотически вероятность

$$P_n(t) = P\{\mu \leqslant np + t\sqrt{np(1-p)}\}$$

того, что в n независимых испытаниях, в каждом из которых p — вероятность наступления искомого события, число этих наступлений μ не превзойдет $np + t\sqrt{np(1-p)}$. Муавр доказал эту теорему для $p = \frac{1}{2}$; он вывел также необходимую для этого формулу Стирлинга:

$$s! = \sqrt{2\pi s} \cdot s^s e^{-s} e^{\theta_s},$$

где остаточный показатель θ_s удовлетворяет условию

$$|\theta_s| \leqslant \frac{1}{12s}.$$

Позднее Лаплас обобщил эту теорему для любого p $0<p<1$. Появившаяся здесь интегральная форма этой теоремы

$$P(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\frac{x^2}{2}} dx$$

и связанное с этим понятие нормального распределения вероятностей играют в дальнейшей теории вероятностей большую роль. В частности, упомянем принадлежащее Пуассону (1837) распространение теорем Муавра—Лапласа на случай обобщения закона больших чисел в формуле Бернулли для независимых испытаний, вероятность появления в которых некоторого события зависит от номера испытания. Пуассон получил при этом новый вид распределения вероятностей, известный ныне под именем закона Пуассона, и использовал его в работах по теории стрельбы.

Проблема вычисления вероятностей гипотез на основе определенных результатов некоторых наблюдений в разных аспектах рассматривалась в работах Д. Бернулли, Эйлера, Симпсона, Кондорсе и др. Важнейшим результатом здесь были формулы Бейеса, опубликованные в 1764 г. Примыкающая к этому теория ошибок наблюдений получила разработанный Лежандром, Лапласом и Гауссом метод наименьших квадратов.

Помимо указанных двух групп теоретических результатов можно отметить довольно большое число конкретных задач теоретико-вероятностного характера. Среди них: задача контроля продукции, так называемая «петербургская игра», задача Бюффона о бросании иглы и др.

На рубеже XVIII и XIX вв. теоретико-вероятностные результаты были сведены в единую систему, построенную на четко определенных основных понятиях. Выделение новой математической дисциплины — теории вероятностей — нашло яркое выражение в ряде работ Лапласа, особенно в его классической «Аналитической теории вероятностей» (1812 г., затем 1814, 1820 и 1866 гг.).

Аппарат теории вероятностей в то время, когда основным ее объектом были азартные игры, состоял из арифметических приемов, почерпнутых в особенности из комбинаторики. Вместе с обогащением методов теории вероятностей за счет привлечения предельных рассмотрений и других средств математического анализа удельный вес комбинаторных приемов стал уменьшаться. Но комбинаторика продолжала развиваться, так как ее содержание по существу не исчерпывалось приложениями к теории вероятностей.

Существование комбинаторики как научной дисциплины можно вести от работ Лейбница и Я. Бернулли. Первый из них к 1666 г. дал первое систематическое построение этой части математики в «Рассуждении о комбинаторном искусстве». Позднее (около 1700 г.) Лейбниц усовершенствовал комбинаторную символику с помощью развитой системы индексов. Я. Бернулли в сочинении «Искусство предположения» (1713) построил комбинаторику как основной для того времени аппарат решения теоретико-вероятностных задач. Здесь же он доказал важный частный случай закона больших чисел, известный как теорема Бернулли. В связи с изучением сумм вида $\sum_k k^m$ он открыл числа, названные по его имени, числами Бернулли.

Однако решение многих конкретных задач комбинато-

рики длительное время не сопровождалось усовершенствованием общей теории, вплоть до конца 70-х годов XVIII в. В это время в Германии сформировалась многочисленная математическая школа, основателем и руководителем которой был К. Ф. Гинденбург.

Прошло 40—50 лет и комбинаторная школа, исчерпав возможности имевшихся в их распоряжении немногочисленных оперативно-вычислительных методов и не преодолев противоречия между содержанием задач и громоздким формально-символическим аппаратом, распалась.

Комбинаторные методы остались в арсенале ученых как средство решения задач в различных областях математики. Новое развитие комбинаторный анализ начал получать в середине XX в. в связи с выяснившимися широкими возможностями приложения во многих практических вопросах.