ТРЕТЬЯ ГЛАВА

ТЕОРИЯ ЧИСЕЛ

Труды Эйлера

В конце XVII и начале XVIII в. внимание математиков было в основном поглощено разработкой и приложениями дифференциального и интегрального исчисления. К исследованиям по теории чисел математиков вновь привлек Л. Эйлер. П. Л. Чебышев в своей «Теории сравнений» (СПб., 1849) писал: «Эйлером положено начало всех изысканий, составляющих общую часть теории чисел. В этих изысканиях Эйлеру предшествовал Ферма; он первый начал заниматься исследованием свойств чисел в отношении их способности удовлетворять неопределенным уравнениям того или другого вида и результатом его изысканий было открытие многих общих теорем теории чисел. Но изыскания этого геометра не имели непосредственного влияния на развитие науки: его предложения остались без доказательств и без приложений. В этом состоянии открытия Ферма служили только вызовом геометров на изыскания в теории чисел. Но, несмотря на весь интерес этих изысканий, до Эйлера на них никто не вызывался. И это понятно: эти изыскания требовали не новых приложений приемов, уже известных, и новых развитий приемов, прежде употреблявшихся; эти изыскания требовали создания новых приемов, открытия новых начал, одним словом, основания новой науки. Это сделано было Эйлером»[1]. Вслед за Эйлером теорией чисел занялись Ж. Л. Лагранж, А. М. Лежандр и К. Ф. Гаусс, а за ними и другие крупнейшие математики XIX в., среди них П. Л. Чебышев, положивший начало замечательной Петербургской школе теории чисел.

Л. Эйлер доказал многие результаты своих предшественников, в частности Ферма, успешно применяя средства арифметики и алгебры и метод спуска, создал новые аналитические методы в теории чисел, поставил ряд новых важных задач.

Вклад Эйлера в теорию чисел настолько велик, что здесь нет возможности упомянуть даже об основных его результатах. Ему принадлежит свыше ста отдельных работ по теории чисел. Большинство их было объединено П. Л. Чебышевым и В. Я. Буняковским в двух томах «Собрания арифметических работ» (Commentationes arithmeticae collectae. СПб., 1849). Кроме того, вопросам теории чисел посвящены несколько глав во «Введении в анализ бесконечных» и ряд разделов «Универсальной арифметики» (1768, 1769). Наконец, вопросы теории чисел занимают важное

[1] *П. Л. Чебышев.* Полное собрание сочинений, т. I. М.—Л., 1944, стр. 10.

место в записных книжках Эйлера, хранящихся в Архиве Академии наук СССР. Особо следует отметить переписку Эйлера по вопросам теории чисел с некоторыми другими учеными, прежде всего с петербургским академиком Христианом Гольдбахом (1690—1764), автором нескольких интересных работ по анализу и весьма наблюдательным арифметиком. Хотя по математическому дарованию и эрудиции Гольдбах значительно уступал Эйлеру и математикой вообще занимался не систематически, духовный обмен с ним имел для Эйлера очень большое значение, тем более, что как раз теорией чисел в то время занимались очень немногие.

Исследование задач Ферма

Именно Гольдбах привлек внимание Эйлера к утверждению Ферма, что все числа вида $2^{2^n} + 1$ ($n = 1, 2, 3, \ldots$) — простые. Эйлер указал, что это утверждение неверно, в своей первой заметке по теории чисел «Замечания о теореме Ферма и других теоремах о простых числах» (Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus. Commentarii, (1732—1733) 1738). Оказалось, что уже число $2^{2^5} + 1$ делится на 641.

Эйлер доказал утверждение Ферма, что всякое простое число вида $4n + 1$ разлагается на сумму двух квадратов и притом единственным образом (Novi Commentarii, (1754—1755) 1760) и много других подобных теорем о представимости чисел некоторыми квадратичными формами вида $mx^2 + ny^2$. Дальнейшие исследования в этом направлении предпринял Лагранж.

Переписка с Гольдбахом послужила толчком для открытия Эйлером теоремы о том, что всякий делитель числа вида $x^2 + y^2$, где $(x, y) = 1$ есть число того же вида. Эта теорема и аналогичные ей породили впоследствии теорию делителей бинарных квадратичных форм.

В предыдущем изложении мы упомянули теорему Баше де Мезириака о представлении целого положительного числа суммой не более чем четырех целых квадратов (см. т. II, стр. 75). В Novi Commentarii, (1754—1755) 1750, Эйлер доказал, что всякое рациональное положительное число есть сумма четырех квадратов рациональных чисел, и подготовил средства для полного решения этой задач. Лагранжем (см. стр. 116). По одному замечанию Ферма Эйлер сумел воссоздать метод бесконечного спуска и доказал этим методом два случая великой теоремы Ферма: для $n = 4$ (Commentarii, (1738) 1747) и для $n = 3$ (Универсальная арифметика, т. II, 1769), сообщив о доказательстве для $n = 3$ еще в письме Гольдбаху 26 апреля 1755 г. Такой большой временно́й интервал между обоими доказательствами объясняется, по-видимому, тем, что случай $n = 3$ потребовал применения существенно новых идей. В ходе доказательства Эйлер пришел к выражению вида $a^2 + 3b^2$ (где a и b — целые числа), которое должно было равняться кубу. Эйлер разложил его на множители, положив

$$a^2 + 3b^2 = (a + b\sqrt{-3})(a - b\sqrt{-3}) = t^3.$$

Далее он, по существу, рассматривал выражения вида $a \pm b\sqrt{-3}$ как целые числа. В частности, он применил для них следующую теорему: если произведение двух взаимно простых чисел α и β равно некоторой степени z^n то $\alpha = \alpha_1^n$ и $\beta = \beta_1^n$. Эта теорема была в то время установлена

только для целых рациональных чисел, но имеет место в любом кольце с однозначным разложением на простые множители. Таким образом, здесь впервые понятие целого числа было перенесено в новую область. Правда, Эйлер не предпринял систематического исследования новых чисел — это было сделано гораздо позже, но в своем доказательстве он открыл новый путь, по которому в дальнейшем и начала развиваться высшая арифметика.

Позднее различные случаи теоремы Ферма доказали Лежандр, Э. Куммер, П. Лежен-Дирихле и др. Попытки решения этой задачи стимулировали создание теории целых алгебраических чисел в работах Дирихле, Куммера, Эрмита и других математиков XIX в. и ее разработку в трудах Дедекинда, Золотарева, Кронекера.

Отправляясь от теорем Ферма, Эйлер рассмотрел также уравнения $x^4 + y^4 = u^4 + v^4$ и $x^4 + y^4 + z^4 + u^4 = v^4$ и нашел все целые решения первого из них.

Ферма считал одной из важнейших задач теории чисел отыскание простого числа, большего, чем любое заданное. С этой задачей были связаны попытки найти многочлен, все значения которого простые числа. Однако попытки эти были обречены на неудачу. Теорему о том, что ни один многочлен с целыми коэффициентами

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n$$

($n \geqslant 1$) не может при всех целых значениях x принимать значения, равные простым числам, впервые сообщил Гольдбах в письме Эйлеру от 28 сентября 1743 г. Теорема была доказана Эйлером в 1752 г. (в письме 28 октября 1752 г.). Гольдбах указал свое доказательство этой теоремы, близкое к доказательству Эйлера, и доказательство Гольдбаха было опубликовано в статье Эйлера «Об очень больших простых числах» (De numeris primis valde magnis. Novi Commentarii, (1762—1763) 1764). В переписке и сочинениях Эйлера имеются примеры многочленов, дающих при целых значениях много простых значений.

Обобщение малой теоремы Ферма и теория степенных вычетов

С рассмотрения малой теоремы Ферма (см. т. II, стр. 74) начались исследования Эйлера по теории степенных вычетов. В заметке «Доказательство некоторых теорем о простых числах» (Theorematum quorundam ad numeros primos spectantium demonstratio. Commentarii, (1736) 1741) Эйлер привел доказательство теоремы Ферма, основанное на свойстве биномиальных коэффициентов. Другое доказательство малой теоремы Ферма Эйлер дал в работе «Теоремы об остатках, получающихся при делении степеней» (Theoremata circa residua ex divisiones potestatum relicta. Novi Commentarii, (1758—1759) 1761). Оно основано на исследовании ряда остатков (или, как теперь говорят, «вычетов»), получающихся при делении на простое число последовательных членов геометрической прогрессии $1, a, a^2, a^3, \ldots$ Эйлер показывает, что если p — простое и a — целое, не делящееся на p, то ни один из членов этой геометрической прогрессии не делится на p. При этом получается не более $p - 1$ различных остатков (остатки периодически повторяются).

Пусть k — наименьший показатель из ряда степеней $1, a, a^2, a^3, \ldots$, такой, что при делении a^k на простое число p получается в остатке единица:

$$a^k = 1 + pm \qquad (m \text{ — некоторое целое}),$$

тогда k равно $p - 1$ или является делителем числа $p - 1$. Число a, для которого $k = p - 1$, называется первообразным корнем для простого p (т. е. $a^{p-1} = 1 + pm$ и никакое a^x, где $x < p - 1$ уже не может дать при делении на p в остатке единицу). Теорема о существовании первообразного корня была по существу высказана И. Г. Ламбертом (Nova Acta Eruditorum, 1769). Несколько позднее, в работе «Доказательства, относящиеся к остаткам, происходящим от деления степеней на простые числа» (Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia. Novi Commentarii, (1773) 1774), Эйлер определил понятие первообразного корня (ввел и самый этот термин), предложил первое доказательство существования его для каждого простого числа, содержащее, однако, существенные пробелы, установил число первообразных корней и дал их важные приложения. Показав, что k делит $p - 1$, Эйлер на частном примере установил основной факт будущей теории конечных групп: порядок подгруппы есть делитель порядка группы (ср. стр. 92).

Эйлер обобщает малую теорему Ферма: если N и a взаимно просты, $\varphi(N)$ — количество чисел, взаимно простых с N и меньших N, то $a^{\varphi(N)} - 1$ всегда делится на N. Это предложение называют теоремой Эйлера, а функцию $\varphi(N)$ — функцией Эйлера. Формулу для $\varphi(N)$ при $N = p^\alpha q^\beta \ldots s^\delta$

$$\varphi(N) = p^{\alpha-1}(p-1)\,q^{\beta-1}(q-1)\ldots s^{\delta-1}(s-1)$$

Эйлер вывел в работах «Арифметические теоремы, доказанные новым методом» (Theoremata arithmetica nova methodo demonstrata. Novi Commentarii, (1758—1759) 1763) и «Размышления относительно некоторых важных свойств чисел» (Speculationes circa quasdam insignes proprietates numerorum. Acta, (1780) 1784).

Важнейший вклад в теорию чисел представляет собой открытый Эйлером квадратичный закон взаимности.

Число r называют квадратичным вычетом по модулю p, если существует такое число x, что x^2 при делении на p дает в остатке r, т. е.

$$x^2 = r + mp \qquad (m \text{ — целое}).$$

В более поздней формулировке Дирихле закон взаимности можно высказать следующим образом (Эйлер выразил его иначе): если из двух нечетных простых чисел p и q по крайней мере одно имеет вид $4n + 1$, то q будет квадратичным вычетом или невычетом p, смотря по тому, будет ли p квадратичным вычетом или невычетом q; если же оба числа имеют вид $4n + 3$, то q есть квадратичный вычет или невычет p, смотря по тому, будет ли p квадратичным невычетом или вычетом q. Пользуясь символом Лежандра $\left(\frac{r}{p}\right)$, где $\left(\frac{r}{p}\right) = +1$, если r — квадратичный вычет по модулю p, $\left(\frac{r}{p}\right) = -1$, если r — квадратичный невычет по модулю p (ср. стр. 119), закон взаимности теперь формулируют так: если p и q—нечетные простые числа, то

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

Например, если $p = 3$, $q = 5$, то $\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = -1$, если $p = 3, q = 13$, то $\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = +1$, а если $p = 3$, $q = 7$, то $\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -1$.

Первая еще неполная формулировка квадратичного закона взаимности имеется в работе Эйлера, написанной в 1744 г. и содержащей ряд теорем о делителях формы $mx^2 \pm ny^2$ (Commentarii, (1749) 1751), а развернутая формулировка — в «Замечаниях о делении квадратов на простые числа» (Observationes circa divisionem quadratorum per numeros primos), представленных им Петербургской академии в 1772 г. и опубликованных в первой части «Аналитических сочинений» (1783). Доказательства закона Эйлер не дает.

Математики долгое время не обращали внимания на работы Эйлера о квадратичном законе взаимности, к которому вновь пришел Лежандр и который затем явился предметом глубоких исследований Гаусса (см. стр. 119 и 124). Только Чебышев в 1849 г. обнаружил в трудах Эйлера эту замечательную теорему; в Западной Европе на это обратил внимание Кронекер в 1875 г.

Диофантов анализ

Решению неопределенных уравнений и систем неопределенных уравнений посвящено более 50 работ Эйлера, вторая часть «Универсальной арифметики» и большое количество записей в «Записных книжках». Эти задачи особенно привлекали внимание Ферма и других предшественников Эйлера.

Одной из важнейших задач диофантова анализа является решение в целых числах уравнения Ферма

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

В статье «О применении нового алгоритма для решения задачи Пелля» (De usu novi algorithmi in problemate Pelliano solvendo. Novi Commentarii, (1765) 1767), представленной в 1759 г., Эйлер дал полное решение уравнения Ферма (1) с помощью разложения $\sqrt{a}$ в непрерывную дробь, обнаружив при этом на частных примерах периодичность этой дроби. Одновременно он представил Петербургской академии еще одну работу на ту же тему (Novi Commentarii, (1762—1763) 1764). Наконец, он изложил решение уравнения Ферма во второй части «Универсальной арифметики» (1769), воспользовавшись для этой цели разложением формы $u^2 \pm av^2$ на иррациональные или мнимоиррациональные множители:

$$u^2 \pm av^2 = (u + v\sqrt{\mp a})(u - v\sqrt{\mp a}). \tag{2}$$

Строгого обоснования своему методу Эйлер не дал.

Эйлер рассмотрел также общее неопределенное уравнение второй степени

$$Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0, \tag{3}$$

привел его к виду

$$u^2 - av^2 = b \tag{4}$$

и связал решение уравнения (4) с решением уравнения Ферма

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

Он показал, что если x_0, y_0 — наименьшее решение уравнения (1), а u_0, v_0 — наименьшее решение уравнения (4), то другие решения u_n, v_n уравнения (4) можно получить по формуле

$$u_n + v_n\sqrt{a} = (u_0 + v_0\sqrt{a})(x_0 + y_0\sqrt{a})^n, \qquad (5)$$

где надо раскрыть скобки и приравнять в обоих частях равенства свободные члены и коэффициенты при $\sqrt{a}$. Впоследствии Лагранж показал, что формула (5) не дает, вообще говоря, всех решений уравнения (4). Мы скоро обратимся к теоретико-числовым работам этого математика.

Аналитические методы

В XVIII в. значительное развитие получили дифференциальное и интегральное исчисление и теория рядов. Эйлер принимал в их разработке самое активное участие, и неудивительно, что именно он ввел методы математического анализа в теорию чисел.

Эйлер применил аналитические методы для решения как аддитивных задач — о представлении чисел в виде суммы некоторых слагаемых, так и задач мультипликативных, связанных с разложением чисел на множители.

Ряд работ Эйлера посвящен выводу рекуррентной формулы для суммы делителей. В первой из них, «Открытии необычайного числового закона для суммы делителей чисел» (Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs. Bibliothèque impartiale, (1747) 1751), Эйлер впервые указывает рекуррентную формулу для суммы делителей числа n, которую он обозначил $\int n$, в виде

$$\int n = \int(n-1) + \int(n-2) - \int(n-5) - \int(n-7) + \ldots$$

Он получает ее сначала с помощью индукции, а потом выводит средствами математического анализа. Эйлер рассматривает бесконечное произведение

$$s = (1 - x)(1 - x^2)(1 - x^3)\ldots$$

Перемножая скобки, он приходит к представлению произведения в виде ряда

$$s = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \ldots$$

Показатели этого ряда суть пятиугольные числа, т. е. числа вида $(3n^2 - n)/2$, где n принимает значения $0, \pm1, \pm2, \pm3, \ldots$, а закон следования знаков очевиден из записи. Заметим, что функция $s = \prod_{k=1}^{\infty}(1 - x^k)$ принадлежит к числу тета-функций Якоби (ср. стр. 341).

Дифференцируя $\ln s = \sum_{k=1}^{\infty} \ln(1 - x^k)$ и умножая на $-x$, Эйлер находит

$$t = \frac{-x}{s}\frac{ds}{dx} = \frac{x}{1-x} + \frac{2x^2}{1-x^2} + \frac{3x^3}{1-x^3} + \ldots \qquad (6)$$

С другой стороны, деля

$$\frac{ds}{dx} = -1 - 2x + 5x^4 + 7x^6 - 12x^{11} - 15x^{14} + \ldots \qquad (7)$$

на s и умножая частное на $-x$, он получает

$$t = -\frac{x}{s}\frac{ds}{dx} = \frac{x + 2x^2 - 5x^5 - 7x^7 + 12x^{12} + 15x^{15} - \ldots}{1 - x - x^2 + x^5 + x^7 - \ldots}. \qquad (8)$$

Каждый член правой части (6) он раскладывает в геометрическую прогрессию

$$\begin{array}{rrrrrrrrrrl}
t = x + & x^2 + & x^3 + & x^4 + & x^5 + & x^6 + & x^7 + & x^8 + & x^9 + & x^{10} + & \ldots \\
& + 2x^2 & & + 2x^4 & & + 2x^6 & & + 2x^8 & & + 2x^{10} + & \ldots \\
& & 3x^3 & & & + 3x^6 & & & + 3x^9 & & \ldots \\
& & & + 4x^4 & & & & + 4x^8 & & & \ldots \\
& & & & + 5x^5 & & & & & + 5x^{10} + & \ldots \\
& & & & & + 6x^6 & & & & & \ldots
\end{array}$$

и складывает по столбцам одинаковые степени x. Каждая степень x встречается в ряде для t столько раз, сколько делителей имеет показатель x, так как каждый делитель показателя становится коэффициентом при той же степени x. Если объединить однородные члены, получается, что коэффициент при каждой степени x будет равен сумме всех делителей показателя этой степени:

$$t = 1 \cdot x + (1+2)x^2 + (1+3)x^3 + (1+2+4)x^4 + (1+5)x^5 + \\ + (1+2+3+6)x^6 + \ldots = \int 1x + \int 2x^2 + \int 3x^3 + \ldots \qquad (9)$$

Умножив левую и правую части равенств (8) на знаменатель, имеем

$$t(1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \ldots) - x - 2x^2 + 5x^5 + 7x^7 - \ldots = 0.$$

Наконец, подставим сюда значение t из (9)

$$\left(\int 1x + \int 2x^2 + \int 3x^3 + \ldots\right)(1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \ldots) - \\ - x - 2x^2 + 5x^5 + 7x^7 - \ldots = 0.$$

Коэффициент при x^n равен $\int n - \int(n-1) - \int(n-2) + \ldots$, откуда

$$\int n = \int(n-1) + \int(n-2) - \int(n-5) - \ldots,$$

причем сумма обрывается, когда под знаком $\int$ оказывается отрицательное число; $\int 0$ считается равным n.

Тому же вопросу посвящено еще несколько работ. В одной из них «Об удивительных свойствах пятиугольных чисел» (De mirabilibus proprietatibus numerorum pentagonalium. Acta, (1780) 1783) Эйлер доказывает равенство выражений для s в виде ряда и произведения, переносясвойства корней и коэффициентов обычных алгебраических уравнений на уравнения с бесконечным числом корней.

Большой цикл, связанный с предыдущими исследованиями, составляют работы Эйлера о разбиении чисел на слагаемые (partitio numerorum). Одной из простейших задач этого вида является издавна бытовавшая задача о взвешивании всевозможных грузов с помощью наименьшего числа гирь, приведенная Эйлером в качестве примера в 16-й главе первого тома «Введения в анализ бесконечных», специально посвященной разбиению чисел на слагаемые. Другая задача: сколькими способами данное целое число может быть разложено на сумму меньших целых чисел? — была впервые поставлена Лейбницем в 1674 г.

Задача о разбиении чисел была предложена Эйлеру в 1740 г. берлинским математиком Филиппом Ноде (1684—1745). Спрашивалось, сколькими различными способами число может быть представлено как сумма двух, трех, четырех или вообще любого количества чисел. В своем ответе Ноде Эйлер в сентябре 1740 г. впервые приводит аналитическое решение этого вопроса, опубликованное прежде всего в упомянутой 16-й главе «Введения в анализ бесконечных», а затем в одной статье 1741 г., увидевшей свет позднее (Commentarii, (1741—1743) 1751). Чтобы решить вопрос, сколькими различными способами данное число N может быть разложено на p частей, неравных между собой, Эйлер составляет произведение

$$s = (1 + xz)\,(1 + x^2z)\,(1 + x^3z)\ldots$$

и приравнивает его ряду $s = 1 + Az + Bz^2 + Cz^3 + \ldots$ Тогда

$$\begin{aligned} A &= x + x^2 + x^3 + \ldots, \\ B &= x^3 + x^4 + 2x^5 + 2x^6 + 3x^7 + 3x^8 + \ldots, \\ C &= x^6 + x^7 + 2x^8 + 2x^9 + 4x^{10} + 5x^{11} + \ldots, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Коэффициенты второго, третьего и последующих рядов показывают, сколькими различными способами показатель степени x может быть разложен соответственно на две, три и т. д. неравные части. Например, из второго ряда видно, что число 7 может быть разложено на две неравные части тремя способами (именно: $7 = 1 + 6 = 2 + 5 = 3 + 4$). Аналогично решаются и другие задачи на разложение чисел.

Во «Введении в анализ бесконечных» мы встречаем применение аналитического метода и к решению мультипликативных задач. В 15-й главе Эйлер рассматривает разложение в ряд дроби

$$\frac{1}{(1-\alpha z)\,(1-\beta z)\,(1-\gamma z)\ldots}$$

и путем формального выполнения делений (вероятно, сперва 1 на $1 - \alpha z$, затем получившегося ряда на $1 - \beta z$ и т. д.) находит

$$1 + Az + Bz^2 + Cz^3 + \ldots,$$

где A — сумма всех $\alpha, \beta, \gamma, \ldots$, B — сумма произведений пар этих чисел, C — сумма произведений троек этих чисел и т. д., не исключая одинако-

вых множителей. Если $z = 1$ и α, β, γ суть обратные величины n-х степеней всех простых чисел, то возникает тождество

$$\prod_p \frac{1}{\left(1 - \frac{1}{p^n}\right)} = \sum_{k=1}^{\infty} \frac{1}{k^n}, \tag{10}$$

где в произведении p принимает значения всех простых чисел начиная с 2, а в сумме k пробегает весь ряд натуральных чисел. Это — знаменитое тождество Эйлера, лежащее в основе всей аналитической теории чисел и впервые приведенное им в «Различных замечаниях о бесконечных рядах» (Variae observationes circa series infinitas. Commentarii, (1737) 1744). Отсюда следует новое доказательство теоремы, что простых чисел бесконечно много, так как ряд справа при $n = 1$ расходится. О сходимости применяемых им рядов и бесконечных произведений здесь Эйлер ничего не говорит.

Теперь функцию $\sum_{k=1}^{\infty} \frac{1}{k^s}$ обозначают $\zeta(s)$ и называют «дзета-функцией Римана» (см. стр. 337).

Во «Введении в анализ бесконечных» есть и другие формулы для $\zeta(s)$, среди которых такая (в современных обозначениях):

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

где $\mu(n)$ — функция, получившая впоследствии название функции Мёбиуса [1].

Заметим, что для решения аддитивных задач Эйлер использовал степенные ряды (и их выражение в виде бесконечных произведений), для мультипликативных задач — ряды, ныне называемые рядами Дирихле (и соответствующие произведения). Аналитические методы Эйлера в мультипликативных задачах были в XIX в. развиты Лежен Дирихле, в 1837 г. доказавшим с их помощью высказанную Эйлером предположительно («Аналитические сочинения», т. II, 1783) теорему о бесконечности количества простых чисел в арифметической прогрессии $ax + b$, где $(a, b) = 1$. Новая страница в истории аналитических методов была открыта Б. Риманом, который определил $\zeta(s)$ для любых комплексных s, вновь вывел основное тождество, связывающее $\zeta(s)$ и $\zeta(1 - s)$, оперируя уже в комплексной области и пользуясь аналитическим продолжением, и высказал знаменитую гипотезу о расположении нулей $\zeta(s)$ (см. стр. 338). Отправляясь от идей Римана, Ш. Ж. де ла Валле-Пуссен и Ж. Адамар в 1896 г. смогли доказать асимптотический закон распределения простых чисел, а именно сходимость $\pi(x)/\operatorname{li} x$ к 1 при $x \to \infty$, где $\pi(x)$ — это обозначение ввел Э. Ландау (1909) — обозначает число простых чисел, не превышающих x, а $\operatorname{li} x$ — интегральный логарифм $\int_2^x \frac{dx}{\ln x}$

[1] Эта функция такова: $\mu(1) = 1$; $\mu(n) = 0$, если n делится на какой-либо квадрат, больший единицы; $\mu(n) = (-1)^k$, если $n = p_1 \cdot p_2 \cdot p_3 \ldots p_k$, где все множители различные простые числа.

(ср. стр. 360). Мы упоминаем об этом потому, что еще Эйлер в письме к Гольдбаху от 28 октября 1752 г. высказал некоторые соображения о порядке роста функции $\pi(x)$. Однако начало долгой серии работ в этом направлении положил только Лежандр (см. стр. 119).

Трансцендентные числа

В рассматриваемое время были достигнуты успехи в изучении арифметической природы чисел e и π и поставлены важные проблемы теории трансцендентных чисел, решенные, впрочем, много позднее.

В иррациональности числа π математики были уверены с давних пор (см. т. I, стр. 77, 178, 198, 229). Впервые на особую природу этого числа, отличного от употребительных иррациональностей, указал, по-видимому, Валлис (1656), предвосхищая мысль о трансцендентности π. Таково же было мнение Дж. Грегори, пытавшегося доказать неалгебраичность как круговых, так и логарифмических функций (см. т. II, стр. 150—151). Вычисление π со все бо́льшим и бо́льшим числом знаков убеждало математиков, по крайней мере, в его иррациональности. Так, Д. Мечин (1706) нашел 100 десятичных знаков π, а Т. де Ланьи в «Мемуаре о квадратуре круга», представленном Парижской академии в 1717 г. («Mémoire sur la quadrature du cercle». Mém. Ac. Paris, (1719) 1721) еще более — 127 (см. стр. 331). Никакой закономерности в следовании цифр обнаружить не удавалось. В только что упомянутой работе Ланьи высказал замечательное предположение об иррациональности $\operatorname{tg} x$ при рациональном $x \neq 0$ и, наоборот, об ирралиональности дуги с рациональным тангенсом. Отсюда следовала бы иррациональность π, поскольку $\operatorname{tg}(\pi/4) = 1$. Догадка Ланьи была подтверждена полвека спустя.

Эйлер также приложил немало усилий к созданию различных эффективных приемов вычисления π, о них говорится далее (см. стр. 308). Его интересовала и теоретическая сторона проблемы квадратуры круга, и он не раз давал заключения о попытках ее точного решения, поступавшие в Петербургскую и Берлинскую академии.

В переписке Эйлера с Гольдбахом несколько раз поднимался вопрос о природе числа π. Оба полагали, что π не является рациональным числом, причем Эйлер еще не исключил возможности точного выражения π с помощью простых иррациональностей и логарифмов рациональных чисел. Во «Введении в анализ бесконечных» Эйлер прямо писал, что иррациональность π достаточно ясна. В статье, содержащей изящное геометрическое спрямление четверти круга, написанной в связи с одним построением Декарта и законченной в 1758 г. (Novi Commentarii, (1760—1761) 1763), Эйлер писал, что π следует отнести «к гораздо более высокому роду иррациональностей, которого можно достичь только посредством бесконечного повторения извлечения корней» [1].

Вероятно, он склонялся к мнению, что π трансцендентно, но все же осторожно замечал в одной статье 1775 г., что невозможность выражения π через «радикальные количества» никем еще не обнаружена (опубл. в «Аналитических сочинениях», т. II, 1785).

Первый крупный шаг в теоретическом изучении арифметической природы обоих чисел e и π сделал Иоганн Генрих Ламберт (1728—1777).

---

[1] *L. Euler.* Opera omnia, series I, t. 15, p. 1—2.

И. Г. Ламберт
(с литографии П. Р. Виньерона; городской музей в Мюлузе)

Ламберт был уроженцем Мюлуза в Эльзасе, который до Французской революции входил в Швейцарский союз. Сам Ламберт именовал себя Mulhusino-Helvetus (Мюлузо-швейцарцем). Сын бедного портного, вынужденный с ранних лет зарабатывать себе на жизнь перепиской рукописей, Ламберт, главным образом, самоучкой приобрел глубокие познания во всех областях науки и выдвинулся в ряды крупнейших ученых XVIII в. В физике он положил начало фотометрии, в астрономии вел исследования по небесной механике и высказал взгляды о развитии Вселенной, близкие к космогонической гипотезе Канта — Лапласа, в математике внес значительный вклад в теорию чисел, алгебру, анализ, теорию параллельных, учение о перспективе и т. д. Он писал и по вопросам философии. Несколько лет Ламберт работал в основанной в 1759 г. Мюнхенской академии наук, а с 1764 г.— в Берлинской академии, причем состоял членом обеих.

Иррациональность e и π Ламберт доказал в двух работах 1766 г.: в «Предварительных сведениях для ищущих квадратуру и спрямление круга» (Vorläufige Kenntnisse für die, so die Quadratur und Rectification des Circuls suchen), напечатанной во втором томе «Очерков о математике и ее применении» (Beiträge zur Gebrauche der Mathematik und deren Anwendung. Berlin, 1770), и, более подробно, в «Мемуаре о некоторых замечательных свойствах круговых и логарифмических трансцендентных коли-

честв» (Mémoire sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques, Mém. Ac. Berlin, (1761) 1768).

Отправным пунктом доказательств Ламберта явились разложения в непрерывные дроби чисел e, $(e+1)/(e-1)$ и некоторых других, данные ранее Эйлером (для e такое разложение предложил еще Коутс в 1714 г.), а также приемы преобразования в непрерывные дроби бесконечных рядов, принадлежащие тому же Эйлеру (ср. стр. 47).

На этом пути Ламберт получил представления в форме бесконечных непрерывных дробей двух функций:

$$\frac{e^x-1}{e^x+1}=\cfrac{1}{\cfrac{2}{x}+\cfrac{1}{\cfrac{6}{x}+\cfrac{1}{\cfrac{10}{x}+\cfrac{1}{\cfrac{14}{x}+\ddots}}}}$$

$$\operatorname{tg} x=\cfrac{1}{x-\cfrac{1}{\cfrac{3}{x}-\cfrac{1}{\cfrac{5}{x}-\cfrac{1}{\cfrac{7}{x}-\ddots}}}}$$

(второе можно вывести из первого, пользуясь равенством

$$\operatorname{tg} x=\frac{1}{\sqrt{-1}}\,\frac{e^{2x\sqrt{-1}}+1}{e^{2x\sqrt{-1}}-1},$$

как это сделал Лежандр).

Из того, что обе непрерывные дроби бесконечны, следует, что при рациональных x ни $\operatorname{tg} x$, ни e^x не могут быть рациональными и, в частности, иррациональность e и π. Для полной строгости рассуждениям Ламберта не хватало доказательства того, что если в бесконечной непрерывной дроби

$$\cfrac{m}{n+\cfrac{m'}{n'+\cfrac{m''}{n''+\ddots}}}$$

числа m, n, m', n' — целые положительные или отрицательные, причем дроби m/n, m'/n', . . ., начиная с некоторой, меньше единицы, то значение этой дроби — иррациональное число. Это утверждение доказал А. М. Лежандр в IV приложении к его «Началам геометрии» (Eléments de Géométrie. Paris, 1800).

Ламберт не только доказал иррациональность e и π, но и был уверен, что они, как и e^x при рациональном $x \neq 0$, не принадлежат к числу, как он выразился во второй из упомянутых статей, «радикальных иррациональных количеств», а именно иррациональных корней алгебраических уравнений. Вслед за ним и Лежандр писал: «Представляется вероятным, что число π даже не принадлежит к классу алгебраических иррациональностей, т. е. что оно не может быть корнем никакого алгебраического

уравнения с конечным числом членов, коэффициенты которого рациональны. Но эту теорему, по-видимому, очень трудно строго доказать. Мы можем только показать, что и квадрат π есть иррациональное число» [1]. В самом деле, для такого доказательства требовались более сильные методы анализа, чем существовавшие в XVIII в.

Если e^x трансцендентно при рациональном $x \neq 0$, то это значит, что натуральные логарифмы рациональных чисел, кроме единицы, трансцендентны. В таком виде эту гипотезу высказал в письме к Гольдбаху от 28 апреля 1729 г. еще Д. Бернулли: гиперболические логарифмы рациональных чисел не выражаются ни в рациональных, ни в «радикальных» числах. Несколько позже (точная дата письма неизвестна) Д. Бернулли писал, что точные квадратуры гиперболы и круга либо обе возможны, либо обе невозможны, так как «между ними существует некоторая взаимозависимость через посредство мнимых чисел» [2]. Гольдбах, со своей стороны, утверждал, что может привести бесконечное число рядов, сумма которых, по нашей терминологии, суть трансцендентные числа, и в качестве примера указал 20 октября 1729 г. число

$$\sum_{k=1}^{\infty} 10^{-2^{k-1}} = 0{,}1 + 0{,}01 + 0{,}0001 + 0{,}00000001 + \ldots$$

Эйлер во «Введении в анализ бесконечных» (1748) утверждал, что при рациональном основании логарифм любого рационального числа, не являющегося рациональной степенью основания, есть «количество трансцендентное».

Доказательства всех этих предположений о трансцендентности были даны не скоро [3]. Первый достаточный критерий трансцендентности и примеры чисел, трансцендентность которых была строго доказана, привел Ж. Лиувилль (1844, 1851) [4]. В 1873 г. Эрмит доказал трансцендентность e, а Ф. Линдеман в 1882 г.— теорему, обобщающую результат Ламберта: e^z в алгебраической степени, отличной от нуля, не может быть рациональным числом. Так как, по формуле Эйлера, $e^{\pi i} = -1$, то πi, а значит, и π трансцендентно. Из другой, более общей теоремы Линдемана вытекает следствие, обобщающее предложение Д. Бернулли: натуральный логарифм любого алгебраического числа, не равного единице, трансцендентен. А. А. Марков в 1883 г. упростил доказательства теорем Эрмита и Линдемана.

Д. Гильберт в 1900 г. включил в список поставленных им 23 актуальных проблем математики вопрос об арифметической природе чисел вида

---

[1] *Архимед, Гюйгенс, Ламберт, Лежандр.* О квадратуре круга. Перевод С. Н. Бернштейна. М. — Л., 1934, стр. 209.

[2] «Correspondance mathématique et physique de quelques célèbres géomètres du XVIII^e siècle», t. II, p. 310.

[3] Напомним теперь, что алгебраическим называют всякое число, удовлетворяющее какому-либо алгебраическому уравнению с рациональными коэффициентами. остальные числа называются трансцендентными.

[4] Лиувилль строго построил первые примеры трансцендентных чисел. Через тридцать лет, в 1874 г., Г. Кантор методами теории множеств в общем виде установил, что в то время, как множество алгебраических чисел счетно (т. е. они могут быть перенумерованы) и имеет ту же мощность, что и совокупность натуральных чисел, множество трансцендентных чисел несчетно и имеет ту же мощность, что и множество всех действительных чисел. Тем самым в некотором смысле действительные числа, как правило, являются трансцендентными.

a^b, где a — алгебраическое число, не равное нулю или единице, а b — алгебраическое и иррациональное. Эту седьмую проблему Гильберта решил до конца в 1934 г. А. О. Гельфонд, доказавший трансцендентность всего того класса чисел. Тем самым было доказано в обобщенной форме предположение Эйлера: при алгебраическом основании логарифмы алгебраических чисел трансцендентны или рациональны.

Укажем, наконец, что трансцендентность числа Гольдбаха (см. стр. 113) доказал в 1938 г. Р. О. Кузьмин.

В XX в. теория трансцендентных чисел, ростки которой появились в рассматриваемое нами время, выросла в большой отдел теории чисел со своими собственными кругом проблем и методами.

Работы Лагранжа

Лагранж посвятил вопросам теории чисел девять работ, добавления к французскому изданию «Алгебры» Эйлера (Лион, 1774) и несколько глав в «Элементарных лекциях по математике, читанных в Нормальной школе» (Leçons élémentaires sur les mathématiques données à l'École normale. Paris, 1795).

Первая работа по теории чисел «Решение одной арифметической задачи» (Solution d'un problème d'arithmétique. Miscellanea Taurinensia, 1766—1769) была опубликована в Турине. Здесь ставилась задача решения в целых числах уравнения Ферма,— Лагранж еще не знал тогда о работах Эйлера в этом направлении. Он самостоятельно решил уравнение Ферма с помощью разложения $\sqrt{a}$ в непрерывную дробь. При этом он доказал, что дробь обязательно будет периодической.

В «Решении одной арифметической задачи» и в статье «О решении неопределенных задач второй степени» (Sur la solution des problèmes indeterminés du second degré. Mém. Ac. Berlin, (1767), 1769) Лагранж дал исчерпывающее исследование решений уравнения Ферма

$$x^2 - ay^2 = 1 \tag{11}$$

и неопределенного уравнения второго порядка от двух переменных

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0 \tag{12}$$

в рациональных и целых числах. Он показал, что общее неопределенное уравнение второго порядка (12) можно всегда свести к уравнению вида

$$A = x^2 - By^2. \tag{13}$$

Таким образом, дело сводится к представлению числа A в виде

$$A = (x + y\sqrt{B})(x - y\sqrt{B}),$$

где $x + y\sqrt{B}$ — элемент поля $Q(\sqrt{B})$.

Отыскивая условия, необходимые и достаточные для разрешимости уравнения (13) в рациональных числах или, что то же, для возможности решения уравнения

$$Ar^2 = p^2 - Bq^2 \tag{14}$$

в целых числах, Лагранж пришел к рассмотрению делителей формы $z^2 - B$.

Действительно, как легко видеть, для разрешимости уравнения (14) необходимо, чтобы A было делителем формы $z^2 - B$ или $(B/t) = +1$, где t — простой делитель A. Для нахождения условий достаточности Лагранж применил алгоритм сведения уравнения (14) к уравнению того же вида

$$A_1 r^2 = p^2 - B_1 q^2,$$

но с меньшими коэффициентами, т. е. применил метод спуска; при этом A должно быть делителем $z^2 - B_1$. Повторяя тот же алгоритм, мы придем через конечное число шагов к уравнению

$$A_n r^2 = p^2 - B_n q^2,$$

где какой-либо коэффициент равен единице или полному квадрату, т. е. сведем дело либо к решению соответствующего уравнения Ферма, либо к уравнению

$$a^2 r^2 = p^2 - B_n q^2,$$

которое без труда решается общим методом.

Работа Лагранжа «О решении неопределенных задач второй степени» была написана, когда ее автор уже познакомился с трудами Эйлера об уравнении Ферма, и здесь Лагранж отмечал их недостатки. Вопросам решения в целых числах неопределенных уравнений второй степени общего вида посвящена еще одна работа Лагранжа «Новый метод для решения неопределенных задач в целых числах» (Nouvelle méthode pour resoudre les problèmes indéterminés en nombres entiers. Mém. Ac. Berlin, (1768) 1770).

Позднее в «Арифметических исследованиях» (Recherches d'arithmétique. Nouv. Mém. Ac. Berlin, (1773) 1775), исследуя вид делителей таких форм, Лагранж сделал замечательное открытие, положившее начало теории квадратичных форм.

Он обнаружил, что хотя все делители p чисел n, представимых в виде

$$n = u^2 \pm av^2, \tag{15}$$

и не могут быть, вообще говоря, записаны формой того же вида, зато допускают представление

$$p = bx^2 \pm 2cxy \pm dy^2, \tag{16}$$

где

$$\pm bd - c^2 = a.$$

Выражение $\pm bd - c^2 = a$ называется теперь, по Гауссу, дискриминантом форм (16), а форма (15) — главной формой данного дискриминанта a.

Лагранж фактически ввел понятие эквивалентности двух форм одного и того же дискриминанта (он говорил об их «тождественности»), положив, таким образом, начало теории классов форм, и доказал, что число таких классов всегда конечно. Для этого Лагранж доказал, что произвольную форму данного дискриминанта

$$bx^2 + 2cxy + dy^2,\ bd - c^2 = a, \tag{17}$$

можно преобразовать конечным числом линейных подстановок:

$$x = Lx' + My', \qquad (18)$$
$$y = lx' + my',$$

где $Lm - lM = \pm 1$, в приведенную форму того же дискриминанта, т. е. такую форму

$$px^2 + 2qxy + ry^2, \quad pr - q^2 = a, \qquad (19)$$

что

$$2|q| \leqslant |p|, \quad 2|q| \leqslant |r|.$$

Совершенно ясно, что если какое-нибудь число n представимо некоторой формой вида (17), то оно будет представимо и всеми эквивалентными ей формами. Это оправдывает гауссово наименование таких форм эквивалентными, т. е. равнозаменяемыми во всех вопросах о представлении. Таким образом, каждой форме данного дискриминанта ставится в соответствие приведенная форма. Это соответствие при данном Лагранжем способе приведения неоднозначно: одной и той же форме могут соответствовать несколько приведенных форм. Однако, как показывает Лагранж, все такие приведенные формы будут эквивалентны между собой.

Лагранж показывает далее, что существует только конечное число различных (т. е. неэквивалентных) приведенных форм данного дискриминанта.

Утверждение Лагранжа, согласно которому всякий делитель p формы $bx^2 + 2cxy + dy^2$, где $(x, y) = 1$ может быть представлен в такой же форме и с тем же дискриминантом a, в сущности означает, что p есть делитель нормы некоторой квадратичной иррациональности, зависящей от $\sqrt{-a}$. Иными словами, эта теорема утверждает, что всякий делитель нормы есть норма идеала. Из результатов этой статьи следует, что число классов идеалов конечно. Метод приложения теории делителей квадратичных форм к разложению чисел на множители был впоследствии усовершенствован П. Л. Чебышевым в «Теории сравнений» (1849).

В 1770 г. была опубликована небольшая статья Лагранжа «Доказательство одной арифметической теоремы» (Démonstration d'un théorème d'arithmétique. Nouv. Mém. Ac. Berlin, (1770) 1772). Здесь Лагранж дал полное доказательство теоремы Баше де Мезириака о четырех квадратах (см. стр. 102), которое Эйлер упростил в Nova acta eruditorum за 1773 г.

В работе «О некоторых задачах диофантова анализа» (Sur quelques problèmes de l'analyse de Diophante. Nouv. Mém. Ac. Berlin, (1777) 1779) Лагранж рассмотрел задачу Ферма об отыскании прямоугольного треугольника, у которого сумма катетов p, q и гипотенуза суть квадратные числа, т. е. $p + q = y^2$, $p^2 + q^2 = x^4$. Если положить $p - q = z$, то получается уравнение $2x^4 - y^4 = z^2$. Ферма утверждал, что наименьшие натуральные значения x, y, z, при которых p и q оба целые и положительные, суть $x = 2\,165\,017$, $y = 2\,372\,159$, $z = 1\,560\,590\,745\,759$, причем $p = 1\,061\,652\,293\,520$, $q = 4\,565\,486\,027\,761$. Для решения указанного уравнения и доказательства утверждения Ферма Лагранж применил метод, сходный с методом спуска, который характеризовал как один из самых плодотворных в теории чисел.

Арифметические вопросы затрагивались Лагранжем также в его «Лекциях по математике». Здесь говорилось о важности теории чисел для всех математических наук. В лекциях рассмотрены признаки делимости, а затем теория вычетов, где использованы результаты Эйлера по тео-

рии степенных вычетов. Здесь доказаны некоторые свойства вычетов, которые легко сформулировать как свойства сравнений. У Лагранжа не было лишь этого понятия.

Упомянем еще, что в статье Лагранжа о трехгранных пирамидах, опубликованной в 1775 г. (см. стр. 181), содержатся первые ростки будущей геометрической теории чисел.

Теорема Вильсона; проблемы Варинга и Гольдбаха

В «Алгебраических размышлениях» (1770) Варинга Лагранж нашел следующую теорему: если n какое-нибудь простое число, то число $1\cdot2\cdot3\cdot4\cdot5\ldots(n-1)+1$ всегда будет делиться на n, т. е. если разделить произведение $(n-1)!$ на простое число n, получится в остатке $n-1$ или -1. Варинг считал доказательство этой теоремы, принадлежащей, по его словам, Джону Вильсону (1741—1793), воспитаннику и некоторое время преподавателю Кембриджского университета, очень трудным. Лагранж в «Доказательстве одной новой теоремы относительно простых чисел» (Démonstration d'un théorème nouveau concernant les nombres premiers. Nouv. Mém. Ac. Berlin, (1771) 1773) привел два доказательства теоремы Вильсона. Предложение Вильсона в принципе дает возможность узнать, является ли некоторое n простым, но Лагранж указал, что этот метод ввиду быстрого роста $n!$ очень трудоемкий, и предлагал другим математикам упростить его. Лагранж доказал и другие теоремы Варинга. В 1773 г. теорему Вильсона вновь доказал Эйлер («Аналитические сочинения», т. I, 1783).

В «Алгебраических размышлениях» Варинга имеется целый ряд новых теоретико-числовых теорем, в частности высказана без доказательства знаменитая «проблема Варинга»: «Каждое целое число есть или куб или составлено из двух, трех, четырех, пяти, шести, семи, восьми или девяти кубов; есть квадрато-квадрат или составлено из двух, трех и т. д. до девятнадцати квадрато-квадратов и т. д. Кажется поэтому, что можно утверждать то же самое для любого числа величин любого измерения» [1].

Здесь же Варинг привел без доказательства утверждение, известное под именем гипотезы Гольдбаха: «Каждое четное число есть сумма двух простых чисел, и каждое нечетное число является простым или суммой трех простых чисел» [2]. В несколько ином виде эти утверждения были высказаны много ранее в переписке Гольдбаха с Эйлером, которая, однако, была впервые опубликована только в 1843 г. А именно Гольдбах сформулировал ее в письме 7 июня 1742 г. так: «Представляется, что каждое число, большее, чем 2, есть сумма трех простых чисел» [3], причем он относил к простым числам и единицу. В нескольких примерах, им указанных, четные числа были представлены также суммой двух простых. Эйлер 30 июня ответил, что, как это заметил Гольдбах еще ранее, каждое четное число есть сумма двух простых, а нечетное, в таком случае, сумма трех простых. «Но что каждое четное число есть сумма двух простых, я считаю несомненной теоремой, хотя и не могу ее доказать» [4].

---

[1] *E. Waring.* Meditationes algebraicae. Ed. III. Cantabrigae, 1782, p. 349.
[2] Там же, стр. 379.
[3] *L. Euler* und *Chr. Goldbach.* Briefwechsel, 1729—1764. Berlin, 1965, S. 104.
[4] Там же, стр. 111. В бумагах Декарта есть замечание, что всякое число есть сумма не более трех простых, но оно было опубликовано лишь в его «Oeuvres» (v. 10, Paris, 1908, p. 298).

Теперь под гипотезой Варинга понимают следующее утверждение: для любого целого k существует целое $s = s(k)$, зависящее только от k, такое, что каждое целое число N есть сумма не более s k-х степеней, т. е. для каждого k существует s, зависящее только от k, такое, что уравнение

$$N = n_1^k + n_2^k + \ldots + n_s^k$$

имеет хоть одно решение в целых неотрицательных числах.

Первое решение проблемы Варинга дал в 1909 г. Д. Гильберт, который установил существование для любого k соответствующего $s(k)$, но для самого s получил еще слишком большие значения. Оценки величины s были улучшены в 20-е годы Г. Харди и Дж. Литлвудом, которые показали, что для всех достаточно больших N число слагаемых s есть величина порядка $k \cdot 2^k$. В 1934 г. И. М. Виноградов, применив свой новый метод тригонометрических сумм, резко улучшил оценку: s есть величина порядка $k \ln k$.

Успехи в решении проблемы Гольдбаха были получены несколько позднее. В 1930 г. Л. Г. Шнирельман с помощью оригинального метода решил проблему Гольдбаха в ослабленной постановке, доказав, что всякое целое число есть сумма ограниченного числа простых чисел. Подсчетом этого числа k занимались многие ученые, до сих пор его удалось снизить до 20.

Применяя свой только что упомянутый метод, И. М. Виноградов вывел асимптотическое выражение для числа представлений нечетного $N > 0$ в виде суммы трех простых чисел. Отсюда следовало, что всякое достаточно большое нечетное число можно представить в виде суммы трех простых чисел (1937). С помощью метода Виноградова было показано также, что почти все четные числа можно представить суммой двух простых. Однако этого еще не удалось доказать для всех четных чисел, хотя бы начиная с некоторого.

«Опыт теории чисел» Лежандра

Итог работам по теории чисел в XVIII в. подвел Адриан Мари Лежандр (1752—1833), воспитанник Колледжа Мазарини и с 1775—1780 гг. преподаватель Военной школы в Париже, а с 1783 г. член Парижской академии наук. В годы Французской революции Лежандр активно участвовал в Комиссии по введению метрической системы, в частности, в измерении длины одного градуса между Дюнкерком и Барселоной для установления эталона метра, с 1795 г. стал профессором Нормальной школы, а в 1799 г. заменил на посту экзаменатора Политехнической школы Лапласа, с которым он вместе преподавал ранее в Военной школе. Для среднего образования выдающееся значение имели его уже не раз упоминавшиеся «Начала геометрии», выдержавшие множество изданий при его жизни и посмертных переработок другими авторами.

В своем творчестве Лежандр охватил многие области математики и существенно продвинул прежде всего, не считая теории чисел, теорию эллиптических интегралов, теорию потенциала (разрабатывая которую ввел шаровые функции), вариационное исчисление (вторая вариация), теорию ошибок измерений (метод наименьших квадратов). Эти исследования его мы рассмотрим в дальнейшем, а сейчас обратимся к его «Опыту теории

чисел» (Essai sur la théorie des nombres. Paris, 1798) — первому полному и последовательному изложению результатов по теории чисел, полученных как его предшественниками, так отчасти им самим. Это сочинение имело заслуженный успех и дважды переиздавалось при жизни Лежандра: в 1808 и в 1830 гг., когда оно вышло под названием «Théorie des nombres». Имеется также издание 1900 г. Во втором издании были добавлены некоторые результаты Гаусса (1801), в третьем — подробное изложение метода Гаусса для решения двучленных уравнений, доказательство Коши теоремы о многоугольных числах, доказательство последней теоремы Ферма для $n = 5$ (Лежен-Дирихле — Лежандра) и некоторые другие вещи.

Ознакомившись с «Аналитическими сочинениями» (Opuscula Analytica. Petropoli, 1783) Эйлера, Лежандр предпринял первую попытку доказать закон взаимности в статье «Исследования по неопределенному анализу» (Recherches d'analyse indeterminée. Mém. Ac. Paris, (1785) 1788). Современная формулировка закона была дана Лежандром в «Опыте теории чисел»[1]. С помощью закона взаимности Лежандр доказал ряд утверждений Эйлера и других теорем. Свой символ $\left(\frac{N}{c}\right)$ для обозначения остатка от деления $N^{\frac{c-1}{2}}$ на простое число c, равного $+1$ или -1, Лежандр ввел в первом же издании «Опыта теории чисел». Здесь «закон взаимности» (la loi de réprocité) получил свое наименование, современную символическую запись и новое доказательство, в котором Лежандр постарался восполнить пробелы, которые сам видел в предыдущем. Однако доказательство Лежандра так и осталось неполноценным, на что указал в 1801 г. Гаусс.

В книге Лежандра введен также символ $E(x)$ для обозначения целой части (entier) числа x; он использован для определения наибольшей степени данного числа m, которая содержится в $n!$

Вторым крупным вкладом Лежандра в теорию чисел было исследование функции $\pi(x)$, выражающей число простых чисел, не превосходящих x. Оценка $\pi(x)$ интересовала еще Эйлера. Во втором томе второго издания своей книги (1808) Лежандр предложил асимптотическую формулу для функции

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

Сверив результаты, полученные по этой приближенной формуле, с результатами таблиц простых чисел от 10 000 до 1 000 000, Лежандр показал, что они очень близки. Он пытался также доказать формулу с помощью интегрального исчисления. Его рассуждения не были убедительны, но интересно, что Лежандр с самого начала желал привлечь к доказательству закона распределения простых чисел и средства математического анализа.

Абель в одном письме 1823 г. назвал это предложение Лежандра самым замечательным во всей математике. Все же эта действительно замечательная формула не была строгой. Из нее следовало бы, что $\lim\limits_{x\to\infty}\left[\frac{x}{\pi(x)} - \ln(x)\right] = -1{,}08366$, но последнее неверно: в 1848 г. П. Л. Чебышев доказал, что этот предел, если он существует, есть -1. Подробно рассмотрев вопрос о приближенном выражении функции $\pi(x)$, П. Л. Чебышев установил, что среди функций вида $x/(A \ln x + B)$ только функция $x/(\ln x - 1)$ может представить $\pi(x)$ с точностью до величины порядка $x/\ln^2 x$, а еще

[1] *A. M. Legendre.* Essai sur la théorie des nombres. Paris, 1798, p. 210.

лучшие приближения дает $\mathrm{li}\, x = \int_2^x \frac{dx}{\ln x}$. О доказательстве асимптотического закона распределения простых чисел в 1896 г. мы уже упоминали (см. стр. 109).

Лежандр нестрого доказал еще несколько предложений. например, теорему о том, что всякая арифметическая прогрессия, первый член и разность которой взаимно просты, содержит бесконечное множество простых чисел. Лежандр указывает промежуток, в котором должно найтись хоть одно простое число. Теорему об арифметических прогрессиях, которую в виде предположения несколько ранее высказал Эйлер, доказал в 1837 г. Дирихле (ср. стр. 109).

Отметим еще метод определения числа членов произвольной арифметической прогрессии, не делящихся ни на какое из простых чисел, содержащихся в данной прогрессии. В частном случае получается аналитическая запись процесса решета Эратосфена — для количества чисел. остающихся в натуральном ряде после исключения всех чисел, делящихся на 2, 3, 5, 7, . . . В 1857 г. эта формула была вновь найдена Лиувиллем и Дедекиндом. Когда вышло первое издание «Опыта» Лежандра, молодой Гаусс уже подготовил к печати свой классический труд, выход которого три года спустя открыл новую эпоху в развитии теории чисел.

«Арифметические исследования» Гаусса

К концу XVIII в. относится начало деятельности Карла Фридриха Гаусса (1777—1855). Так как его творчество и по времени и по духу в большей части принадлежит XIX в., мы ограничимся лишь немногими замечаниями о жизненном пути этого великого человека, оказавшего сильное влияние на прогресс математических наук. Гаусс родился в Брауншвейге в семье водопроводчика. Впоследствии он говорил друзьям, что научился считать раньше, чем говорить. В народной школе учитель обратил внимание на математические способности маленького Гаусса, после того как тот быстро просуммировал в классе числа $1 + 2 + \ldots + 40$, заметив, что эта сумма есть $(1 + 40) + (2 + 39) + \ldots$, т. е. $41 \cdot 20$. Молодой помощник учителя М. Бартельс (1769—1836), который впоследствии был в Казани университетским профессором Н. И. Лобачевского, начал заниматься с мальчиком и, убедившись в его исключительных способностях, добился того, что герцог Брауншвейгский оказал ему материальную помощь для получения образования.

В математике Гаусс с ранних лет пошел собственным путем. Уже в 14—15 лет он занялся изучением свойств арифметически-геометрического среднего (конечно, не зная еще о роли этого понятия в будущей теории эллиптических функций [1]), простыми числами, теорией параллельных.

[1] Арифметически-геометрическим средним Гаусс назвал общий предел $M(m, n)$, к которому стремятся последовательности чисел m_k, n_k, образуемых из данных положительных чисел m, n следующим образом:

$$m_1 = \frac{m+n}{2}, \quad n_1 = \sqrt{mn}, \quad m_2 = \frac{m_1+n_1}{2}, \quad n_2 = \sqrt{m_1 n_1}$$

и т. д. В 1799 г. он установил связь между арифметико-геометрическим средним и длиной дуги лемнискаты, выражаемой некоторым эллиптическим интегралом. Через год он уже приступил к разработке теории эллиптических функций.

К. Ф. Гаусс
(с портрета Хр. А. Шварца, 1803 г.)

В 1795 г. он изобрел метод наименьших квадратов. 30 марта 1796 г. он нашел правило построения правильного 17-угольника с помощью циркуля и линейки (об этом по инициативе одного профессора даже появилось краткое сообщение в печати за подписью «Гаусса из Брауншвейга, студента математики в Гёттингене»). До того времени Гаусс еще не решил, выбрать ли себе специальностью древние языки или математику, и удачное решение этой задачи побудило Гаусса посвятить себя математике. Через 10 дней после первого замечательного открытия Гаусс нашел доказательство вновь обнаруженного им квадратичного закона взаимности. В тот же год он индуктивно открыл закон распределения простых чисел: $\pi(x) \approx \frac{x}{\ln x}$ при $x = \infty$. Обучаясь в 1795—1798 гг. в Гёттингенском университете, он посещал здесь лекции престарелого Кестнера, которые не оказали, да и не могли по своему уровню оказать на него какое-либо влияние. Впоследствии Гаусс, вспоминая о нем, говорил, что Кестнер обладал выдающимся природным остроумием во всем, даже когда говорил о математике вообще, но утрачивал его, если речь шла о более специальных математических вопросах. Зато Гаусс читал труды Ньютона, Эйлера, Лагранжа, Лежандра, а еще более черпал в глубинах своего личного гения. Большинство сделанных им в то время открытий, кроме теоретико-числовых, он опубликовал после более глубокой разработки много позднее, следуя девизу, выгравированному на его печати: pauca, sed matura (немногое, но зрелое); некоторые увидели свет только при посмертном издании его бумаг. Мы уже знаем, что в 1797 г. Гаусс оригинально доказал основную теорему алгебры, и это «Новое доказательство теоремы о том, что любая целая рациональная алгебраическая функция одного переменного может быть разложена на действительные множители первой или второй степени», опубликованное в 1799 г., явилось первой его печатной работой. Впоследствии, не вполне удовлетворенный своим первым доказательством, он предложил еще три других в 1815, 1816 и 1849 гг. (последнее уточняет доказательство 1797 г.; ср. стр. 74). «Новое доказательство теоремы...» в корректурных листах было направлено в Гельмштедтский университет профессору И. Пфаффу, и Гауссу заочно присудили докторскую степень. С 1799 г. он работал приват-доцентом университета в Брауншвейге, а с 1807 г. до конца жизни был профессором в Гёттингене и директором местной астрономической обсерватории. С именем Гаусса связаны фундаментальные исследования почти во всех основных областях математики: алгебре, дифференциальной и неевклидовой геометрии, в математическом анализе, теории функций комплексного переменного, теории вероятностей, а также в астрономии, геодезии, механике и теории магнетизма.

Работы прикладного характера занимали в его творчестве видное место и сообщили ряд стимулов его собственно математическим занятиям. Наука, говорил Гаусс, должна быть подругой практики, добавляя: подругой, но не рабыней. И, подобно Эйлеру, Гаусс был преимущественно математиком. В беседах с друзьями он называл математику царицей наук, а теорию чисел — царицей математики.

Знаменитые «Арифметические исследования» (Disquisitiones arithmeticae), которые послужили источником новых идей и одновременно моделью для арифметических теорий XIX в., находившиеся в типографии еще в 1798 г., вышли из печати в Гёттингене летом 1801 г. Хотя содержа-

ше книги было по существу новым и относилось к исследованию арифметики квадратичных полей и построению алгебры над конечным полем, форма ее оставалась еще старой. Арифметика полей алгебраических чисел изучалась без введения этих чисел, как теория квадратичных форм, а алгебра над конечным полем строилась без введения самого понятия конечного поля, как теория сравнений. Здесь же было положено начало изучению структуры конечных коммутативных групп, опять-таки без определения понятия группы (см. стр. 95). Последующие поколения математиков обращались к книге Гаусса так же, как ученые XVII в. к книгам Архимеда, чтобы уяснить себе его методы, перевести его результаты на новый язык, почерпнуть там способы конструкций и свойства новых объектов.

Остановимся вкратце на содержании «Арифметических исследований». Книга состоит из семи разделов. Первые шесть посвящены теории сравнений и теории квадратичных форм, последний раздел — исследованию уравнений деления круга (о нем см. стр. 94).

Сравнения уже применялись, по существу, в работах Эйлера, Лагранжа и Лежандра. Накопленные сведения были преобразованы Гауссом в стройную теорию, которая играет в высшей арифметике такую же роль, как теория уравнений в алгебре.

Два целых числа a и b Гаусс называет сравнимыми по модулю p, если разность $a - b$ делится на p. Он записывает это следующим образом:

$$a \equiv b \pmod{p}.$$

Легко проверить, что отношение сравнения обладает всеми свойствами отношения равенства: рефлексивностью, симметричностью и транзитивностью. Поэтому оно разбивает множество целых чисел на непересекающиеся классы сравнимых между собой чисел, которые называются классами вычетов по модулю p. Множество классов вычетов по любому модулю образуют коммутативную группу по сложению, а классы вычетов по простому модулю образуют поле. Это был первый пример конечного поля.

Теорию сравнений Гаусс развивает по аналогии с теорией алгебраических уравнений: сперва он рассматривает сравнения первой степени

$$ax + b \equiv c \pmod{p},$$

затем переходит к сравнениям вида

$$x^n \equiv A \pmod{p}$$

и развивает теорию степенных вычетов, наконец, отдельно он изучает сравнения второй степени

$$x^2 \equiv a \pmod{p},$$

которые изложены с наибольшей полнотой. Гаусс показывает, что сравнение степени n не может иметь более n корней, доказывает существование первообразного корня по любому простому модулю (т. е. такого числа a, что сравнение $a^k \equiv 1 \pmod{p}$ имеет место при $k = p - 1$ и не выполняется при $k < p - 1$), вводит понятие индекса, являющееся аналогом логарифма.

Здесь же дается первое строгое доказательство квадратичного закона взаимности, который Гаусс назвал фундаментальной теоремой. Стремясь к наиболее естественному выводу этого замечательного закона, Гаусс нашел еще семь его доказательств, из которых второе также помещено в «Арифметических исследованиях», а шесть других были опубликованы позже. Все доказательства Гаусса основываются на различных принципах. Впоследствии математики не раз возвращались к поискам «естественного» доказательства этого закона. В настоящее время существует более 40 его доказательств.

Центральное место в книге занимает теория квадратичных форм, которую Гаусс систематически развил для форм от двух переменных и исследовал также для форм от трех переменных. Следуя Лагранжу, он рассмотрел множество форм $ax^2 + 2bxy + cy^2$ одного и того же дискриминанта $D = a - b^2$ и разбил их на непересекающиеся классы эквивалентных между собой форм [1]. Для этих классов Гаусс ввел закон композиции, причем установил, по существу, что эти классы форм образуют коммутативную группу. Это было одно из первых определений закона композиции для объектов, отличных от чисел. Гаусс отмечает аналогию между композицией классов форм и умножением классов вычетов по простому модулю. Все рассуждения он проводит с максимальной степенью общности, хотя и добавляет, что границы его труда не позволяют в нем изложить теорию классов форм с надлежащей полнотой. По некоторым замечаниям Гаусса можно заключить, что он знал, что группа классов форм не всегда является циклической, но распадается в прямую сумму циклических подгрупп.

Только много позже, исследуя биквадратичные вычеты, Гаусс пришел к убеждению, что «применявшиеся до сих пор арифметические принципы ни в коем случае недостаточны для обоснования общей теории, а что эта теория с необходимостью требует в некотором смысле бесконечно расширить область высшей арифметики» («Теория биквадратичных вычетов», Theoria residuorum biquadraticorum, ч. I, 1828) [2]. Такое явное расширение области целых чисел Гаусс сделал во второй части мемуара «Теория биквадратичных вычетов» (1832), в которой он ввел целые комплексные числа как выражения вида $a + bi$, где i — корень неприводимого уравнения $x^2 + 1 = 0$, а a и b — обычные целые числа [3]. Он перенес на эти новые числа всю ту арифметическую структуру, которая была развита для целых рациональных чисел: определил простые и составные числа, ввел алгоритм Евклида, доказал однозначность разложения каждого целого числа на простые множители, построил для новых чисел теорию степенных вычетов, доказал аналог малой теоремы Ферма, ввел понятие первообразного корня и развил теорию индексов. Наконец, он сформулировал для целых комплексных чисел квадратичный закон взаимности. Таким обра-

---

[1] Гаусс называет две формы F и F' собственно эквивалентными (proprie aequivalentes), если одна из них переходит в другую при подстановке

$$x = \alpha x' + \beta y',$$
$$y = \gamma x' + \delta y',$$

где $\alpha\delta - \beta\gamma = 1$. Если $\alpha\delta - \beta\gamma = -1$, то Гаусс называет формы F и F' несобственно эквивалентными (improprie aequivalentes).

[2] *К. Ф. Гаусс.* Труды по теории чисел. Перевод В. Б. Демьянова. Редакция И. М. Виноградова, комментарии Б. Н. Делоне. М., 1959, стр. 655.

[3] В этом же мемуаре Гаусс дал геометрическую интерпретацию комплексных чисел, которая стала с тех пор общепринятой (см. стр. 65).

зом, здесь впервые арифметическая структура была оторвана от своего первоначального носителя — целых рациональных чисел — и перенесена в иную область. С помощью целых комплексных чисел Гаусс сформулировал биквадратичный закон взаимности для обыкновенных целых чисел.

Гаусс понимал, что это только начало необъятной области исследований, он писал, что для изучения кубических вычетов надо будет рассмотреть числа вида $a + b\rho$, где $\rho^3 = 1$, $\rho \neq 1$, что вскоре и было сделано Ф. Эйзенштейном. О впечатлении, которое произвела теория Гаусса, свидетельствует тот факт, что вплоть до Дедекинда алгебраические числа называли «комплексными», и это даже в том случае, если они принадлежали полю действительных чисел, как, например, $a + b\sqrt{3}$.

В XIX в. в работах П. Лежен-Дирихле, Э. Куммера, Р. Дедекинда, Е. И. Золотарева и Л. Кронекера была построена арифметика полей алгебраических чисел. При этом было уточнено само понятие целого числа из заданного поля алгебраических чисел. Однако математики встретились здесь при попытке построения арифметики с новыми трудностями: Куммер заметил, что для таких чисел не имеет места закон однозначности разложения на простые множители, если считать простыми те целые числа, которые нельзя разложить в произведение двух множителей, отличных от единиц. Для построения арифметики круговых полей он ввел в 1847 г. идеальные множители, а арифметика в любых полях была построена Дедекиндом, Золотаревым и Кронекером в 70-х годах XIX в. При этом оказалось, что вся теория квадратичных форм Гаусса эквивалентна арифметике квадратичных полей, построенной с помощью идеалов Дедекинда, идеальных множителей Золотарева или дивизоров Кронекера. Но и дальше, вплоть до работ Д. Гильберта, развитие алгебраической теории чисел следовало не только духу, но и букве Гаусса. Идеи, содержащиеся в скрытой форме в работах Гаусса, получили здесь свое полное воплощение. Исследования законов взаимности для вычетов высших степеней, начатые Гауссом и продолженные Эйзенштейном и Якоби (кубический закон), велись до наших дней Куммером, Гильбертом, Э. Артином и другими. Наиболее общую форму закона взаимности для любых полей алгебраических чисел установил И. Р. Шафаревич (1949).