Ш. Х. МИХЕЛОВИЧ,
кандидат педагогических наук

ИЗ ИСТОРИИ ТЕОРИИ ЧИСЕЛ

(ВКЛАД РУССКИХ И СОВЕТСКИХ МАТЕМАТИКОВ В РАЗВИТИЕ ТЕОРИИ ЧИСЕЛ)

Издательство «Знание»
Москва 1970

Леонард Эйлер — основоположник теории чисел как науки

Теория чисел в основном является наукой о системе обыкновенных целых чисел с присущими ей связями и законами. Целые числа составляют в большей мере как бы основу математики, а их законы обладают необыкновенной четкостью и прозрачностью, поэтому, по-видимому, К. Гаусс и назвал теорию чисел «царицей математики».

От великого Эйлера и до наших дней много славных страниц истории развития теории чисел ваполнено результатами исследований русских и советских математиков.

После отдельных теоретико-числовых результатов исследований в древности и в средние века расцвет теории чисел начинается в новое время и связан в первую очередь с именем величайшего французского математика XVII века П. Ферма, который, однако, не оставил систематического изложения своих открытий и методов.

Впервые теория чисел оформилась как наука в трудах знаменитого математика члена Петербургской Академии наук Леонарда Эйлера (1707—1783 гг.), жизнь и научная деятельность которого тесно связана с Россией, хотя родом он был из Швейцарии.

Эйлер приехал в Петербург девятнадцатилетним юношей, и с тех пор Россия стала для него второй родиной. Даже во время своего 25-летнего пребывания в Берлинской Академии (1741—1766 гг.), куда Эйлер переехал, опасаясь бироновщины, он продолжал активно сотрудничать с Петербургской Академией, печатаясь в ее трудах и участвуя в других видах ее деятельности.

Научная деятельность Эйлера изумительно богата. Несмотря на то, что он в 1735 г. ослеп на один глаз, а в 1766 г. и на другой, его научная деятельность в последние годы жизни не уменьшилась, а, пожалуй, даже возросла. Литературное наследство Эйлера составляет более 850 работ и полностью не собрано еще на сегодняшний день.

К теории чисел из трудов Эйлера относятся более 100 работ. Эйлер доказал почти все теоремы Ферма, которые последний оставил без доказательств. Кроме того, он открыл много новых законов математики.

Стремясь исследовать природу простых натуральных чисел и определить сколь угодно большое простое число, Эйлер исходил из так называемой малой теоремы Ферма, в которой говорится, что $a^{p-1}-1$ всегда делится на p, если p число простое и a не делится на p. Теорему Ферма Эйлер обобщил в двух направлениях. Во-первых, он доказал теорему, которая носит теперь его имя, о том, что $a^{\varphi(m)}-1$ делится на m, если a и m — числа взаимно простые и $\varphi(m)$ (называемая теперь функцией Эйлера) — число натуральных чисел, не превосходящих m и взаимно простых с ним.

Для простого выражения $m=p$ все натуральные числа, его не превосходящие, т. е. числа $1, 2, \ldots, p-1$, взаимно просты с p, так что $\varphi(m)=p-1$; если же m — число составное с каноническим разложением $m=P_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, то функция Эйлера вычисляется по формуле:

$$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

В первом случае теорема Эйлера совпадает с малой теоремой Ферма. Поэтому говорят также о теореме Эйлера — Ферма, которая является одной из фундаментальных в теории делимости.

Во-вторых, исходя из малой теоремы Ферма, Эйлер разработал основы так называемой теории степенных вычетов, связанной с понятием наименьшего натурального числа γ, для которого $a^{\gamma}-1$ делится на натуральное число m, если a и m числа взаимно простые. Согласно теореме Эйлера — Ферма число γ (так называемый показатель a по модулю m) не превосходит $\varphi(m)$, а при простом $m=p$ не превосходит $p-1$, но оно может быть и меньше; так, например, уже 2^3-1 делится на 7, а по теореме Ферма можно лишь утверждать, что 2^6-1 делится на 7. Если $\gamma=\varphi(m)$, то a называется первообразным корнем по модулю m. Оказывается, что показатель числа a по модулю m всегда делит $\varphi(m)$.

При помощи теории степенных вычетов Эйлер установил, что $2^{31}-1$ число простое. В то время это было наибольшее из известных простых чисел (в настоящее время наибольшим из известных простых чисел является число $2^{11213}-1$, что установлено при помощи электронных вычислительных машин). Заметим, однако, что значение теории степенных вычетов, приводящей в теории чисел к аналогу логарифма, далеко выходит за рамки указанного результата.

Много исследований Эйлер посвятил целочисленному решению неопределенных уравнений, т. е. алгебраических уравнений с целыми коэффициентами или систем таких уравнений, у которых число неизвестных больше числа уравнений. Такие уравнения называются также диофантовыми по имени греческого математика Диофанта (III в. н. э.), который впервые много ими занимался и в частных случаях мастерски их решал (в рациональных числах). В настоящее время решение неопределенных уравнений представляет собой один из важных разделов теории чисел — так называемый диофантовый анализ.

Эйлер показал, что в случае бесконечного числа решений общее уравнение второго порядка с двумя неизвестными $ax^2 + bxy + cy^2 + dx + ey + f = 0$ сводится к так называемому уравнению Пелля $x^2 - ay^2 = 1$, где a не квадратное натуральное число, и указал общий способ решения последнего.

Эйлер доказал также утверждение Ферма что уравнение $x^n + y^n = z^n$ при $n > 2$ неразрешимо в целых числах, для случаев $n = 3$ и $n = 4$. Как известно, это утверждение Ферма (так называемая «великая» теорема Ферма) в общем виде до сих пор не доказано и не опровергнуто.

В 1772 г. Эйлер доказал очень важный закон взаимности для квадратичных вычетов, при помощи которого устанавливается, что при целом a и простом p среди чисел $a + pt$, где $t = 0, \pm 1, \pm 2, \ldots$, имеются квадратные, т. е. может быть $x^2 = a + pt$, или, если воспользоваться аппаратом сравнений, разрешимо сравнение $x^2 \equiv a \ (mod\ p)$. Закон взаимности устанавливает, что если $0 < a < p$, то число a является остатком от деления некоторого квадрата на простое число p (например, x^2 при делении на 591 может дать остаток 426). Если среди чисел $a + pt$ имеются квадратные, то a называется квадратичным вычетом числа p, если же их нет, то a называется квадратичным невычетом числа p.

Эйлер, в частности, доказал следующий факт, относящийся к теории квадратичных вычетов. Если натуральное число N формы $4m + 1$ можно разложить на сумму двух квадратов единственным образом, т. е. $4m + 1 = x^2 + y^2$, и притом так, что $(x, y) = 1$ *, то N число простое. Это предположение является обратным по отношению к теореме, высказанной Ферма, а именно, что простое число вида $4m + 1$ можно разложить на сумму двух квадратов, т. е. $p = 4m + 1 = x^2 + y^2$, притом единственным образом с дополнительным условием $(x, y) = 1$.

Эйлер дал новое доказательство бесконечности числа простых чисел, применив для этого аппарат математического анализа, и положил этим начало аналитической теории чисел.

С именем Эйлера связано также возникновение нерешенной до настоящего времени полностью аддитивной проблемы (аддитивные проблемы касаются разложения целых, обычно больших, чисел на слагаемые определенного вида и выделяются в особый раздел теории чисел) — знаменитой проблемы Гольдбаха, или проблемы Гольдбаха—Эйлера. Она была поставлена в 1742 г. петербургским академиком Х. Гольдбахом в письме к Эйлеру

---

* Т. е. x и y взаимно просты.

и заключалась в утверждении, что всякое целое число, большее 5, может быть представлено в виде суммы трех простых чисел, т. е. $N = p_1 + p_2 + p_3$, $N > 5$. Эйлер в ответе выразил уверенность в справедливости теоремы, что каждое четное число, превосходящее 2, есть сумма двух простых, т. е. $2N = p_1 + p_2$, $2N > 2$.

Если расчленить утверждение Гольдбаха на два отдельных утверждения для четных и нечетных чисел, то легко заметить, что утверждение Эйлера эквивалентно утверждению Гольдбаха для четных чисел и что из каждого из них вытекает утверждение Гольдбаха для нечетных чисел, обратное же не имеет места.

Нетрудно также убедиться в том, что гипотезу Гольдбаха можно выразить так: всякое целое число, превосходящее 1, есть сумма не более трех простых чисел.

Заканчивая краткий обзор теоретико-числовых работ, следует сказать, что благодаря трудам Эйлера теория чисел получила то направление, на основании которого в дальнейшем была создана классическая теория чисел. Слова Лапласа: «Читайте, читайте Эйлера — он учитель нас всех», относятся к трудам Эйлера в области теории чисел не менее чем к другим работам этого гениального математика.

Петербургская школа теории чисел

В XIX в. весьма существенная роль в развитии теории чисел принадлежала русской математической школе, в особенности Петербургской школе теории чисел во главе со знаменитым русским математиком Пафнутием Львовичем Чебышевым (1821—1894 гг.).

Воспитанник Московского и профессор Петурбургского университетов, член Петербургской и Парижской Академий наук П. Л. Чебышев сделал много фундаментальных открытий почти во всех областях математики и механики: теории чисел, теории вероятностей, интегральном исчислении, теории приближенного представления функций, теории механизмов и др.

Для творчества Чебышева, во-первых, характерен его интерес к вопросам практики. Точка зрения Чебышева в этом отношении ярко выражена им самим в следующих словах: «Сближение теории с практикой дает самые благотворные результаты, и не одна только практика от этого выигрывает, сами науки развиваются под влиянием ее».

Другая ярко выраженная черта в творчестве Чебышева заключается в том, чтобы довести решение математической задачи до удобного способа вычисления — до «алгорифма». Обе эти точки зрения в большой мере передались и ученикам Чебышева.

Большого внимания заслуживает общественная деятельность П. Л. Чебышева, его участие в организации Московского математического общества, его деятельность в Артиллерийском ведомстве и в области народного просвещения.

Чебышев был не только выдающимся ученым, но и превосходным лектором. Его лекции, отличавшиеся простотой и ясностью изложения, а также богатством содержания, часто оживлялись ценными отступлениями, в которых Чебышев сообщал свои взгляды по затронутым темам и выяснял взаимную связь между различными вопросами математики. Чебышев отличался чутким отношением к людям, которые интересовались наукой и техникой. Известно, с каким вниманием он отнесся к С. В. Ковалевской.

Привлеченный академиком Буняковским к изданию арифметических исследований Эйлера, молодой Чебышев сразу же после переезда в Петербург в 1847 г. занялся исследованиями в области теории чисел. В итоге этих исследований появились не только его прекрасная докторская диссертация «Теория сравнений», служившая потом руководством для многих поколений учащейся молодежи, но и его знаменитые работы по вопросу о распределении простых чисел.

Вопросы распределения простых чисел 2, 3, 5, 7... в ряду натуральных чисел принадлежат к труднейшим вопросам теории чисел. Ими интересовались математики уже с древнейших времен. Еще Евклид дал в своих «Началах» доказательство бесконечности множества простых чисел, указав на то, что для каждого простого p можно найти бо́льшее, поскольку число 2,3, ..., $p + 1$, которое больше p, либо является простым числом, либо имеет простой делитель больший p, так как оно ни на одно из чисел 2, 3, ..., p не делится.

Обозначим, как это принято теперь, через $\pi(x)$ число простых чисел, не превосходящих действительное число x. Тогда теорему Евклида можно выразить следующим образом. При $x \to \infty$ $\pi(x) \to \infty$ или $\lim\limits_{x \to \infty} (x)$ — ∞ функция $\pi(x)$ имеет следующее графическое изображение (рис. 1).

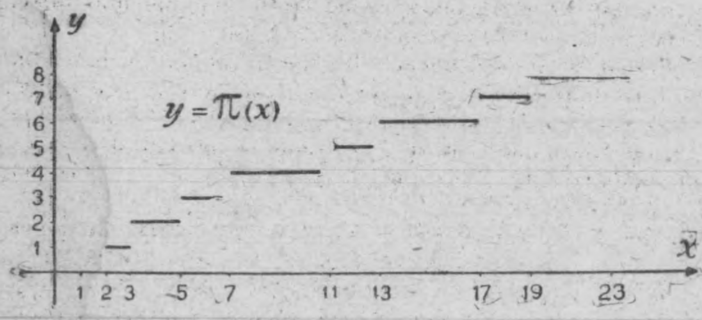

Рис. 1.

В закономерности следования простых чисел в натуральном ряду на первый взгляд неожиданным фактом является тот, что в последовательности p_1, p_2 ... всех простых чисел встречаются промежутки сколь угодно большой длины. Этот факт очень просто следует из того, что для $n > 1$ из чисел $n! + 2$, $n! + 3$, ..., $n! + n$ ни одно не является простым, так как $n! + 2$ делится на 2, $n! + 3$ — на 3 и т. д., наконец, $n! + n$ делится на n, причем во всех случаях делитель меньше делимого, т. е. является собственным.

С другой стороны, встречаются такие простые числа, как, например, 11 и 13; 17 и 19, так называемые близнецы, разность между которыми равна 2. Обнаружены весьма большие пары простых чисел близнецов p и $p + 2$, например, для $p =$ $= 8\,004\,119$, 10 006 427, 1 000 000 009 649 и даже для 1 000 000 000 149 341 (наибольшей из известных пар), однако вопрос о бесконечности числа «близнецов» является до сих пор нерешенным.

Таким образом, оказывается, что длина ступеней в графическом изображении $\pi(x)$ меняется от 2 до любой величины. Этот факт как бы предопределяет чрезвычайную трудность в исследовании закона распределения простых чисел. И действительно, после Евклида сколько-нибудь крупных результатов в развитии теории простых чисел достиг лишь Эйлер, который, как уже упоминалось, дал аналитическое доказательство бесконечности числа простых чисел. При этом Эйлер исходил из рассмотрения введенной им функции $\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \sum_1^\infty \frac{1}{n^s}$, где $S > 1$. В настоящее время эту функцию называют «дзета-функцией».

Указанный ряд при $S > 1$ сходится. Эйлер нашел замечательное тождество, играющее очень важную роль в теории простых чисел, а именно $\sum_1^\infty \frac{1}{n^s} = \prod \frac{1}{1 - 1/p^s}$, где произведение распространяется по всем простым числам, а сумма — по всем натуральным числам. Если S стремится к единице, левая часть равенства беспредельно растет (получается гармонический ряд $\sum \frac{1}{n}$), следовательно, бесконечно увеличивается и правая часть, так что простых чисел должно быть бесконечно много.

Эйлер доказал также, что ряд величин, обратных простым числам, т. е. ряд $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots = \sum \frac{1}{p}$, является расходящимся.

Факт расхождения ряда $\sum \frac{1}{p}$ более сильное явление, чем расхождение гармонического ряда $\sum \frac{1}{n}$ (ибо в последнем речь идет лишь о части его членов), и дает некоторую характеристику роста простых чисел. Он показывает, что ряд простых чисел ведет себя в некотором отношении так же, как весь натуральный ряд, в противоположность, например, ряду полных квадратов $1^2, 2^2, \ldots$, обратные величины которых образуют сходящийся ряд $\sum \frac{1}{n^2}$. Поэтому можно сказать, что плотность распределения простых чисел в натуральном ряду выше, чем полных квадратов.

Изучая таблицы простых чисел, легко заметить, что в среднем простые числа встречаются все реже и реже, точнее говоря, отношение $\frac{\pi(x)}{x}$, так называемая «средняя плотность» простых чисел в отрезке от 1 до x, все время убывает (примеры: $\frac{\pi(10)}{10} = \frac{4}{10}$, $\frac{\pi(100)}{100} = \frac{25}{100}$). Эйлер впервые, хотя и не совсем строго, доказал, что при $x \to \infty$ $\frac{\pi(x)}{x} \to 0$, или $\lim\limits_{x\to\infty} \frac{\pi x}{x} = 0$.

Отмеченные факты о распределении простых чисел все же дают лишь смутное представление об этом сложнейшем вопросе теории чисел. Исследуя таблицы простых чисел, Лежандр и Гаусс нашли эмпирические формулы для числа простых чисел $\pi(x)$, а именно: Лежандр, что $\pi(x) \approx \frac{x}{\ln x - B}$, где B — некоторое постоянное число, равное 1,08366, а Гаусс, что $\pi(x) \approx$ $\approx \int\limits_2^x \frac{dt}{\ln t}$ ($\int\limits_2^x \frac{dt}{\ln t}$, так называемый интегральный логарифм, не выражается в элементарных функциях). Это были замечательные формулы, но поскольку они были установлены эмпирическим путем, то о поведении функции $\pi(x)$ за пределами известной тогда таблицы простых чисел (таблица простых чисел к тому времени была составлена до числа 400 000) ничего нельзя было сказать.

Естественно, что ответ на вопрос о поведении функции $\pi(x)$ за пределами какой бы то ни было таблицы можно было получить только теоретическими исследованиями. И вот такими теоретическими исследованиями занялся молодой Чебышев. Исключительно остроумными средствами он достиг таких результатов, которые сразу выдвинули его в число крупнейших математиков мира.

Результаты Чебышева по указанному вопросу изложены в двух трудах о простых числах: «Об определении числа простых чисел, не превосходящих данной величины» (1849 г.) и «О простых числах» (1852 г.). В первой работе Чебышев (пользуясь функцией $\zeta(S)$ для действительных значений S) доказал, что ступени графика $\pi(x)$ бесчисленное множество раз входят в кривую полосу около графика $y = x\int\limits_2^x \frac{dt}{\ln t}$ (рис. 2), образованную графиками функций

$$y_1 = \int\limits_2^x \frac{dt}{\ln t} - \frac{\alpha x}{\ln^n x} \quad \text{и} \quad y_2 = \int\limits_2^x \frac{dt}{\ln t} + \frac{\alpha x}{\ln^n x},$$

где $n > 0$ сколь угодно велико и $\alpha > 0$ сколь угодно мало (эта полоса сначала узкая, в дальнейшем все расширяется).

При помощи указанной теоремы Чебышев установил, что эмпирическая формула Лежандра при $x \to \infty$ не может быть точной,

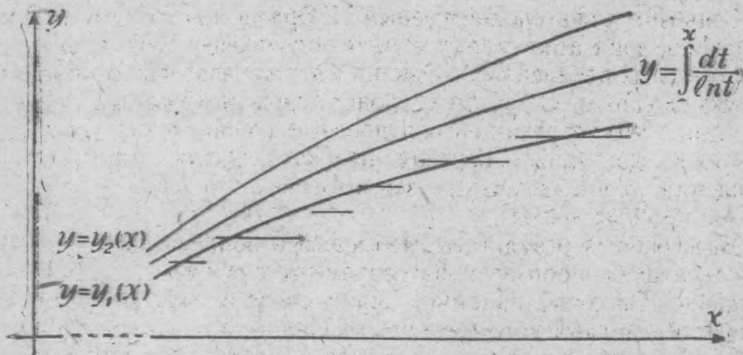

Рис. 2.

что более точной константой в указанной формуле является $B = 1$, и далее, что если предел отношения $\pi(x) : \frac{x}{\ln x}$ при $x \to \infty$ существует, то он должен быть равен 1.

В своей второй работе Чебышев доказал, что для достаточно больших значений x выполняются неравенства $0{,}92129 < \frac{\pi(x)}{\frac{x}{\ln x}} < 1{,}10555$, известные теперь под названием неравенств Чебышева.

Из них, между прочим, вытекает теорема Эйлера о том, что $\frac{\pi(x)}{x} \to 0$, когда $x \to \infty$. В самом деле, на основании правой части неравенства можно записать, что $\frac{\pi(x)}{x} < \frac{1{,}1}{\ln x}$, откуда и следует упомянутый факт, так как при $x \to \infty$ $\frac{1{,}1}{\ln x} \to 0$. Из неравенств Чебышева вытекает также то, что для $n > 3$ между n и $2n - 2$ всегда имеется простое число. Последний факт, принятый французским математиком Бертраном в качестве аксиомы, явился поводом для написания работы Чебышевым, но ее результаты гораздо глубже и значительнее.

Результаты Чебышева явились важной вехой в теоретическом обосновании асимптотического (или основного) закона распределения простых чисел, который гласит: предел отношения $\pi(x) : \frac{x}{\ln x}$ существует и равен единице, когда $x \to \infty$, т. е. $\lim\limits_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$.

Существование указанного предела было доказано лишь 50 лет спустя французским математиком Адамаром и бельгийским математиком Валле-Пуссеном, которые при этом воспользовались глубокими исследованиями немецкого математика Римана относительно дзета-функции для комплексных значений S.

Необходимо отметить, что в 1949 г. норвежский математик А. Сельберг и венгерский ученый П. Эрдеш нашли для него элементарное доказательство (т. е. не использующее теорию функций комплексных переменных). Однако и это доказательство является весьма сложным. С другой стороны, очень интересным является тот факт, что теоретико-вероятностные соображения дают возможность доступным образом передать общую картину рассуждений для обоснования асимптотического закона распределения простых чисел[1].

Выдающиеся результаты Чебышева в вопросе распределения простых чисел произвели на современников очень сильное впечатление. Об этом, например, ярко свидетельствуют слова выдающегося английского математика Сильвестра, который назвал Чебышева «победителем простых чисел» и предлагал для дальнейших успехов теории чисел ждать, пока родится некто настолько же превосходящий Чебышева своей проницательностью и вдумчивостью, насколько Чебышев превосходил этими умственными качествами обыкновенных людей; или слова выдающегося немецкого математика Э. Ландау, который в своей специальной работе, посвященной распределению простых чисел, в 1909 г. писал: «Первый после Евклида, кто пошел правильным путем для решения проблемы о простых числах и достиг важных результатов, был Чебышев». Общая же оценка научного творчества Чебышева ярко выражена в письме французского математика Эрмита в связи с присуждением Чебышеву в 1890 г. президентом Франции ордена Почетного легиона: «... Вы являетесь гордостью науки в России, одним из первых геометров Европы, одним из величайших геометров всех времен».

Гениальными работами Чебышева по теории чисел начинается Петербургская школа теории чисел. Наиболее выдающиеся представители школы — А. Н. Коркин (1837—1908 гг.), Е. И. Золотарев (1847—1878 гг.), А. А. Марков (1856—1922 гг.) и Г. Ф. Вороной (1868—1908 гг.) — нашли новые методы и направления в теории чисел. Они произвели глубокие исследования, касающиеся квадратичных форм от двух и более переменных.

[1] См. например, Я. Б. Зельдович, А. Д. Мышкис. Элементы прикладной математики. М., «Наука», 1965, гл. XIII, § 8 «О распределении простых чисел».

По сей день их работы остаются предметом внимательного изучения (квадратичными формами, например, от двух переменных, являются однородные многочлены второй степени $ax^2 + bxy + cy^2$, где a, b, c целые числа; их теория связана с решением неопределенных уравнений второй степени).

Г. Ф. Вороной сделал, кроме того, важные открытия в геометрии чисел и некоторыми своими работами стимулировал развитие современной аналитической теории чисел. Заметим, что в геометрии чисел, одном из важных разделов теории чисел, применяются так называемые «пространственные решетки», или системы целочисленных точек, имеющие в качестве координат в заданной декартовой системе координат целые числа. Эта теория имеет большое значение в геометрии и в кристаллографии. В теории чисел она связана с теорией квадратичных форм.

Работы А. А. Маркова имеют важное значение для решения задачи о приближении действительного числа рациональной дробью, относящейся к особому разделу теории чисел под названием «диофантовы приближения». В этот раздел входит также теория трансцендентных чисел, которая занимается исследованием арифметической природы разных классов иррациональных чисел относительно их принадлежности к алгебраическим иррациональностям или к трансцендентным числам, т. е. к таким числам, которые являются корнями уравнения вида $a_0x^n + a_1x^{n-1} + \ldots + a_n = 0$, где $a_0, a_1, \ldots, a_n$ целые числа, или к таким, которые уравнениям такого вида не удовлетворяют, как, например, число π.

Труды Е. И. Золотарева по теории алгебраических чисел оказались в этой области исключительными по своей глубине.

Советская школа теории чисел

Достойными продолжателями замечательных традиций Петербургской школы теории чисел являются советские ученые во главе с академиком Иваном Матвеевичем Виноградовым.

Академик Виноградов родился в 1891 г. В 1914 г. он окончил Петербургский университет и посвятил свою научную деятельность теории чисел. После написания своей первой работы в 1915 г. он был оставлен при университете для подготовки к профессорскому званию. Несколько лет Иван Матвеевич проработал в Перми. В 1920 г. он был избран профессором Политехнического института в Петрограде, а с 1925 г. профессором Ленинградского университета. Появляются фундаментальные работы Ивана Матвеевича, и в 1929 г. он избирается действительным членом Академии наук, а с 1932 г. Виноградов — директор Математического института им. В. А. Стеклова Академии наук СССР.

Следуя традициям Петербургской школы, И. М. Виноградов посвятил себя решению труднейших задач теории чисел, в том числе решению проблем Варинга и Гольдбаха — Эйлера.

Проблема Гольдбаха — Эйлера была поставлена еще в 1742 г., и в течение почти двух столетий попытки решить ее оставались безуспешными.

Проблема Варинга, которую выдвинул английский математик Э. Варинг в 1770 г., заключается в следующем: для любого целого числа $n > 2$ существует такое натуральное $r = r(n)$, что всякое натуральное число N можно представить в виде:

$$N = x_1^n + x_2^n + \cdots + x_r^n, \quad x_i \geqslant 0, \tag{1}$$

т. е. как сумму r целых неотрицательных (или не более чем r целых положительных) n — x степеней. Надо обратить внимание на то, что число слагаемых зависит только от показателя степени n и не зависит от представляемого числа N. В противном случае утверждение теоремы становится совершенно тривиальным, так как любое натуральное число N можно, например, выразить как сумму N единиц и вместе с тем как сумму n — x степеней единицы, поскольку $1 = 1^n$.

С другой стороны, нетрудно понять, что проблему Варинга в принципе (т. е. как теорему существования) достаточно решить для всех достаточно больших чисел N, так как если для представления натуральных $N > N_0$ (т. е. достаточно больших N) в формуле (1) достаточно r слагаемых, то для любого N потребуется не более чем r' таких слагаемых, где r' не превосходит наибольшее из чисел r и N_0. В самом деле, любое натуральное число $N \leqslant N_0$ можно, во всяком случае, представить как сумму N_{n-x} степеней единицы.

Заметим, однако, что вопрос о том, каково наименьшее значение для числа r слагаемых в формуле (1), является, конечно, в проблеме Варинга наиболее интересным. Если речь идет о представлении любого N, то оно обозначается через $g(n)$; если о достаточно больших N, то через $G(n)$.

Еще в XVIII в. частный случай проблемы Варинга для $n = 2$ был решен Лагранжем. Для этого частного случая теорема Лагранжа формулируется так: всякое натуральное число представляется в виде суммы не более четырех квадратов, т. е. $g(2) = 4$. Например, $27 = 4^2 + 3^2 + 1^2 + 1^2$, $250 = 14^2 + 7^2 + 2^2 + 1^2$.

Теорема Лагранжа доказывается элементарно. В дальнейшем разными математиками были даны доказательства также для $n = 3, 4, 5, 6, 7, 8, 10$. Однако в общем виде проблема оставалась нерешенной до начала XX в. Первое общее доказательство дал немецкий математик Д. Гильберт в 1909 г., но это доказательство очень сложно и громоздко, а значение верхней границы для $G(n)$, как было показано позже, излишне велико.

В проблемах Варинга и Гольдбаха, а также в других аддитивных задачах И. М. Виноградов исходит из интеграла:

$$I = \int_0^1 e^{2\pi i m \alpha} d\alpha,$$

где m — любое целое число.

Если $m = 0$, то $I = \int_0^1 d\alpha = 1$, если же $m \neq 0$, то

$$I = \int_0^1 e^{2\pi i m \alpha} d\alpha = \frac{1}{2\pi i m} \left[e^{2\pi i m \alpha}\right]_0^1 = \frac{1}{2\pi i m} \left(e^{2\pi i m} - e^0\right) = 0,$$

так как $e^{2\pi i m} = \cos 2\pi m + i \sin 2\pi m = 1$.

Рассмотрим применение этого интеграла к решению проблемы Варинга. Предварительно заметим, что если целое число N представлено в виде $N = x_1^n + x_2^n + \ldots + x_r^n$ с целыми положительными x_i, то $x_i^n < N$, а $x_i < \sqrt[n]{N}$.

Если наибольшее целое число, не превосходящее $\sqrt[n]{N}$, обозначим через P, то $x_i \leqslant P$, поскольку x_i является целым числом.

Пусть теперь дано некоторое целое число $N > 0$ и пусть x_1, x_2, ..., x_r какие-либо r положительных целых чисел, удовлетворяющих условию $x_i \leqslant P$.

Возьмем $m = (x_1^n + x_2^n + \ldots + x_r^n) - N$ и подставим это число в интеграл I. Всякий раз, когда $N = x_1^n + x_2^n + \ldots + x_r^n$, m обращается в нуль и интеграл I принимает значение 1, в остальных случаях, т. е. когда $N \neq x_1^n + x_2^n + \ldots + x_r^n$, $m \neq 0$ и интеграл равен нулю. Поэтому суммируя указанный интеграл по всем x_1, x_2, ..., x_r, принимающим независимо друг от друга значения 1, 2, ..., P, мы получим столько единиц, сколько имеется различных представлений числа N в виде суммы r слагаемых n-х степеней целых положительных чисел (при этом, очевидно, представления, отличающиеся порядком следования чисел x_i, считаются различными).

Обозначая через $\Upsilon(N)$ число таких представлений, мы можем утверждать, что

$$\Upsilon(N) = \sum_{x_1=1}^{P} \cdots \sum_{x_r=1}^{P} \int_0^1 e^{2\pi i \alpha \left(x_1^n + x_2^n + \cdots + x_n^n - N\right)} d\alpha.$$

Так как сумма нескольких интегралов, взятых в одинаковых пределах, равна интегралу от суммы подынтегральных выражений, то из предыдущего равенства следует:

$$\Upsilon(N)=\int\limits_0^1\sum_{x_1=1}^{P}\cdots\sum_{x_r=1}^{P}e^{2\pi i\alpha\,(x_1^n+\cdots+x_r^n-N)}d\alpha;$$

$$\Upsilon(N)=\int\limits_0^1\sum_{x_1=1}^{P}\cdots\sum_{x_r=1}^{P}(e^{2\pi i\alpha x_1^n}\cdots e^{2\pi i\alpha x_r^n}e^{-2\pi i\alpha N})\,d\alpha.$$

Из слагаемых подынтегрального выражения можно вынести за общую скобку сомножитель $e^{-2\pi i\alpha N}$. В скобке останется произведение

$$\sum_{x_1=1}^{P}e^{2\pi i\alpha x_1^n}\cdots\sum_{x_r=1}^{P}e^{2\pi i\alpha x_r^n}.$$

Но

$$\sum_{x_1=1}^{P}e^{2\pi i\alpha x_1^n}=\cdots=\sum_{x_r=1}^{P}e^{2\pi i\alpha x_r^n}\sum_{x=1}^{P}e^{2\pi i\alpha x^n}.$$

Поэтому, обозначая

$$L_\alpha=\sum_{x=1}^{P}e^{2\pi i\alpha x^n},$$

можно написать

$$\Upsilon(N)=\int\limits_0^1 L_\alpha^r e^{-2\pi i\alpha N}d\alpha.$$

Для решения проблемы Варинга надо, очевидно, при любом данном n установить существование такого $G(n)$, чтобы при $r\geqslant G(n)$ для достаточно больших N $\Upsilon(N)$ было положительным.

В гипотезе Гольдбаха для нечетных чисел утверждается, что любое нечетное число $N\geqslant 9$ есть сумма трех нечетных простых чисел: $N=p_1+p_2+p_3$, где p_1, p_2 и p_3 — нечетные простые числа.

Рассуждая таким же образом, как при рассмотрении проблемы Варинга, мы легко найдем, что число $I(N)$ представлений нечетного числа N в виде суммы трех нечетных простых чисел выразится через

$$I(N)=\sum_{p_1\leqslant N}\sum_{p_2\leqslant N}\sum_{p_3\leqslant N}\int\limits_0^1 e^{2\pi i\,(p_1+p_2+p_3-N)\,\alpha}\,d\alpha,$$

где суммирование ведется по нечетным простым числам, не превосходящим число N.

Кроме того, можно записать

$$I(N)=\int_0^1 \sum_{p_1\leqslant N}\sum_{p_2\leqslant N}\sum_{p_3\leqslant N} e^{2\pi i(p_1+p_2+p_3-N)\alpha}\,d\alpha,$$

$$I(N)=\int_0^1\Bigl(\sum_{p_1\leqslant N} e^{2\pi i p_1\alpha}\sum_{p_2\leqslant N} e^{2\pi i p_2\alpha}\sum_{p_3\leqslant N} e^{2\pi i p_3\alpha}\Bigr)e^{-2\pi i N\alpha}\,d\alpha,$$

$$I(N)=\int_0^1\Bigl(\sum_{p\leqslant N} e^{2\pi i p\alpha}\Bigr)^3\cdot e^{-2\pi i N\alpha}\,d\alpha,$$

или

$$I(N)=\int_0^1 T_\alpha^3 e^{-2\pi i N\alpha}\,d\alpha,$$

где

$$T_\alpha=\sum_{p\leqslant N} e^{2\pi i p\alpha}.$$

Проблема Гольдбаха для нечетных чисел будет решена, если удастся доказать, что для любого нечетного числа $N\geqslant 9$ число $I(N)>0$. Практически важно доказать это для достаточно больших N.

Как в проблеме Варинга, так и в проблеме Гольдбаха наиболее трудным вопросом является оценка сумм L_α и T_α. Эти суммы являются частными случаями сумм вида $\sum\limits_{A<x<B} e^{2\pi i f(x)}$, где $f(x)$ — некоторая действительная функция от x и суммирование распространяется на все целые числа некоторого интервала $(A—B)$, или же на какую-либо часть этих целых чисел, например простые числа.

Такие суммы называются тригонометрическими суммами. Оценка их является чрезвычайно важным вопросом в аналитической теории чисел.

Впервые тригонометрическими суммами интересовался К. Ф. Гаусс. Он изучил суммы вида

$$\sum_{x=0}^{q-1} e^{2\pi i\frac{ax^2}{q}},\ \text{где } (a,q)=1,$$

получившие впоследствии название «суммы Гаусса».

Первый общий метод оценки сумм вида

$$\sum_{x=1}^{P} e^{2\pi i f(x)},\ f(x)=\alpha_n x^n+\alpha_{n-1}x^{n-1}+\cdots\alpha_1 x+\alpha_0$$

(где α_n, α_{n-1}, ..., α_0 — заданные действительные числа, причем хотя бы одно из них иррациональное) дал Герман Вейль в 1914 г., поэтому они носят название «суммы Вейля». Оценки, получаемые по методу Вейля, зависят от приближений посредством рациональных дробей к старшему коэффициенту многочлена $f(x)$.

Хотя оценка Вейля лишь немного лучше тривиальной (тривиальной является оценка $\left|\sum_{x=1}^{p} e^{2\pi i f(x)}\right| \leqslant p$; это неравенство заведомо имеет место, так как модуль $e^{2\pi i f(x)}$ при действительных значениях $f(x)$ равен единице, а модуль суммы нескольких слагаемых не превосходит суммы модулей этих слагаемых), однако и она уже ведет к замечательным приложениям.

Использовав ее, английские математики Г. Харди и Дж. Литлвуд создали в начале 20-х годов нашего столетия первый мощный аналитический метод для решения аддитивных задач теории чисел. Этим методом им удалось, в частности, дать более совершенное, чем Гильберту, доказательство теоремы Варинга. Они снизили также верхнюю границу для $G(n)$.

В отношении проблемы Гольдбаха Харди и Литлвуд получили лишь условный результат.

Существенное развитие теория тригонометрических сумм получила в работах И. М. Виноградова начиная с 1934 г. Характерной чертой этих работ является освобождение от условия, чтобы суммирование проводилось по всем натуральным числам некоторого отрезка подряд.

В отношении проблемы Варинга (которой И. М. Виноградов начал заниматься с 1924 г.) новый метод позволил резко снизить верхнюю границу для $G(n)$. И. М. Виноградов нашел оценку $G(n) < n(3\ln n + 11)$, а в 1959 г. улучшил свой результат и показал, что $G(n) < n\ln n\,(2 + \varepsilon(n)$, где $\varepsilon(n) \to 0$ при $n \to \infty$. Методом И. М. Виноградова получены также наилучшие значения для $g(n)$.

Необходимо также подчеркнуть, что в работах И. М. Виноградова проблема Варинга получила обозримое решение.

Еще более усовершенствовав свой метод, И. М. Виноградов в 1937 г. доказал, что для всякого достаточно большого нечетного положительного числа N $(N > N_0)$ число $J(N)$ представлений в виде суммы трех простых чисел, больших нуля, а это значит что такие представления возможны. И. М. Виноградов нашел также приближенное значение для $I(N)$. Относительно числа N_0 К. Г. Бороздкин показал, что $N_0 \leqslant e^{e^{16,038}}$.

Таким образом, И. М. Виноградовым была, наконец, в принципе решена знаменитая проблема Гольдбаха для нечетных чисел.

Метод И. М. Виноградова был также применен (и применяется) для решения многих других задач.

И. М. Виноградов исследовал проблему распределения дробных долей многочлена с действительными коэффициентами, нашел общий закон распределения степенных вычетов и невычетов, им получены весьма точные формулы для количества целых точек в областях на плоскости и в пространстве.

Характеризуя силу нового метода для оценки тригонометрических сумм, можно сказать, что результаты исследований Виноградова в рассматриваемом круге вопросов примерно равны результатам всех работ западных ученых, а в отдельных вопросах (проблема Варинга, проблема Гольдбаха) далеко их превосходят.

Новый метод оценки тригонометрических сумм принес академику Виноградову мировую славу. Иван Матвеевич почетный член многих наших и зарубежных научных обществ; в 1942 г. он был избран членом Лондонского королевского общества, в 1946 г.— членом Парижской академии наук, Академии наук США и других академий. Академик Виноградов — лауреат Государственной премии и Герой Социалистического Труда.

Метод, развитый Виноградовым, успешно развивается и применяется как советскими, так и зарубежными математиками. С его помощью получены наилучшие оценки добавочного члена

$$R(x) = \pi(x) - \int_2^x \frac{dt}{\ln t}$$

в асимптотическом законе распределения простых чисел. Сюда относятся результаты исследований Н. Г. Чудакова (в 1936 г.), Е. Титчмарша, Н. М. Коробова и самого И. М. Виноградова, который в 1958 г. доказал, что

$$|R(x)| < c_1 x e^{-c_2 (\ln x)^{\mu}},$$

где c_1 и c_2 положительные постоянные, а $\mu = \frac{3}{5} + \varepsilon$.

Интересно отметить, что значение $R(x)$ тесно связано со свойствами дзета-функции $\zeta(S)$ для комплексных значений $S = \sigma + it$. Для таких значений эту функцию исследовал известный немецкий математик Б. Риман, и поэтому ее называют также дзета-функцией Римана.

Нетривиальные, т. е. комплексные, нули дзета-функции (под нулями функции комплексного переменного понимают точки, в которых она обращается в нуль) находятся в полосе $0 < \sigma < 1$, которую называют критической. Риман высказал предположения, что все нетривиальные нули дзета-функции расположены на прямой $\sigma = \frac{1}{2}$. Эта гипотеза Римана до сих пор не доказана, но и не опровергнута. В случае ее справедливости мы имели бы «идеальную» оценку $R(x) < c_1 \sqrt{x}$, что соответствует значениям $\mu = 1$ и $c_2 = \frac{1}{2}$.

Используя метод Виноградова, Чудакову удалось значительно уменьшить те границы, в пределах которых можно утверждать наличие хотя бы одного простого числа. До этого немецким математиком Хейльброном в 1933 г. было установлено, что в последовательности 1^{250}, 2^{250}, 3^{250}, ..., n^{250}, $(n+1)^{250}$, ..., начиная с некоторого $n = n_0$, между двумя ее соседними членами лежит еще хотя бы одно простое число. Чудакову удалось заменить эту последовательность более тесной 1^4, 2^4, 3^4, ..., n^4, $(n+1)^4$..., имеющей тем не менее аналогичное свойство[1].

В 1938 г. Н. Г. Чудаков доказал, что почти все четные числа можно представить в виде суммы двух простых. Это значит: если $\nu(x)$ число тех четных чисел $\leqslant x$, которые нельзя представить как сумму двух простых, то $\lim\limits_{x\to\infty} \frac{\nu(x)}{x} = 0$. Результат Чудакова явился существенным вкладом в решение проблемы Гольдбаха для четных чисел.

Метод Виноградова получил успешное применение в исследовании важных классов систем целочисленных уравнений (К. К. Марджанишвили), в метрических проблемах диофантовых приближений (В. Г. Спринджук), в вопросах распределения дробных долей показательной функции $\{\alpha g^x\}$ и значений арифметических функций, например, значений функции Эйлера (А. Г. Постников) и др.

Значение метода Виноградова не ограничивается одной теорией чисел. Он имеет также применение, выходящее за пределы области теории чисел, например, в теории функций, теории вероятностей и приближенном анализе для вычисления кратных интегралов (Н. М. Коробов).

К крупнейшим достижениям советской школы теории чисел, имеющим фундаментальное значение, следует также отнести открытия, сделанные молодым советским математиком Л. Г. Шнирельманом (1905—1938 гг.). Еще мальчиком 12 лет Лев Генрихович уже самостоятельно исследовал теорию алгебраических уравнений, а в 16 лет стал студентом Московского университета, который блестяще закончил за два с половиной года. В 24 года Лев Генрихович был профессором, а в 1933 г. его избрали членом-корреспондентом Академии наук СССР.

В 1930 г. Шнирельман открыл новый метод, имеющий очень важное значение в аддитивной теории чисел, так называемый метод сложения числовых последовательностей.

При помощи этого метода Шнирельман доказал, что всякое натуральное число $N > 1$ есть сумма ограниченного, не зависящего от N, числа простых чисел.

---

[1] Заметим, что впоследствии английскому математику А. Е. Ингаму в 1937 г. удалось уточнить этот результат, а именно заменить четвертые степени кубами. Из результатов Ингама следует даже, что число простых чисел между n^3 и $(n+1)^3$ стремится вместе с n к бесконечности.

Наименьшее натуральное число S (s), такое, что всякое достаточно большое натуральное число (всякое натуральное число $N > 1$) представимо в виде суммы не более S (s) простых, называют теперь постоянной (абсолютной постоянной) Шнирельмана.

Элементарным методом было установлено, что $S \leqslant 67$ (Д. Риччи, 1937), в 1950 г. указанная верхняя грань была снижена до 20 (Х. Шапиро и Ж. Варга), а в 1958 г. до 18 (Ин Вен Лин). Комбинируя элементарные и аналитические методы, Н. И. Климов и его ученики доказали (1968), что для достаточно больших четных чисел $S \leqslant 10$, а для достаточно больших нечетных чисел $S \leqslant 9$.

Что касается абсолютной константы Шнирельмана, то элементарным методом пока лишь установлено, что $S \leqslant 6 \cdot 10^9$ (Шептицкая — Климов).

Метод Шнирельмана заключается в следующем. Пусть дано некоторое число начинающихся с нуля возрастающих последовательностей целых чисел:

$$a_0, a_1, a_2, \cdots, a_m, \cdots \qquad (A);$$

$$b_0, b_1, b_2, \cdots, b_m, \cdots \qquad (B);$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$c_0, c_1, c_2, \cdots, c_m, \cdots \qquad (C),$$

где

$$a_0 = b_0 = \cdots = c_0 = 0.$$

Выберем по одному числу из каждой последовательности и сложим между собой эти числа. Совокупность всех полученных таким образом чисел, в которой равные между собой будем считать только по одному разу, можно расположить в виде некоторой новой возрастающей последовательности $n_0, n_1, n_2, \ldots, n_m, \ldots$ (N), где $n_0 = 0$.

Последнюю последовательность мы назовем суммой данных последовательностей $A, B, \ldots, C$

$$N = A + B + \cdots + C.$$

Последовательность N состоит из всех чисел вида

$$a_i + b_j + \cdots + c_l$$

и содержит, в частности, все члены данных последовательностей (чтобы их получить, нужно складывать члены данной последовательности с нулевыми членами остальных последовательностей).

Обозначив через P последовательность 0, 2, 3, 5, 7, 11, 13... (P), состоящую из нуля и всех простых чисел, можно гипотезу Гольдбаха выразить следующим образом: сумма $P + P + P$

содержит все натуральные числа, превосходящие единицу. В самом деле, последовательность $P+P+P$ состоит из сумм вида $0+0+0$, $0+0+p_1$, $0+p_1+p_2$, $p_1+p_2+p_3$, т. е. из сумм не более трех простых чисел. Если она содержит все натуральные числа больше единицы, то это значит, что всякое натуральное число больше единицы можно представить в виде суммы не более, чем трех простых чисел, а это как раз и утверждается в гипотезе Гольдбаха.

Если сумма k одинаковых последовательностей A охватывает все натуральные числа, то последовательность A называется базисом (натурального ряда) порядка k (она будет также базисом порядка $k_1>k$).

Говорят также о базисе k-го порядка для достаточно больших чисел, если сумма k одинаковых последовательностей A охватывает все достаточно большие числа.

Не всякая последовательность является базисом. Так, например, последовательность четных чисел 0, 2, 4... не является базисом какого-либо порядка, так как при сложении чисел этой последовательности нельзя получить ни одного нечетного числа. Не является также базисом ранее упомянутая последовательность P, так как при сложении ее чисел нельзя получить 1.

Л. Г. Шнирельман ввел понятие плотности последовательности. Пусть $A(n)$ обозначает количество натуральных чисел последовательности (A), не превосходящих n (при этом подсчете $a_0=0$ не считается). Тогда под плотностью α этой последовательности понимают нижнюю грань отношения $\frac{A(n)}{n}$ (т. е. наибольшее число, которое не превосходит ни одного из значений этого отношения). Таким образом, $A(n)\geqslant \alpha n$ для любого $n\geqslant 1$ и $0\leqslant\alpha\leqslant 1$. Например, последовательность, состоящая из нуля и арифметической прогрессии с первым членом 1 и разностью d, имеет плотность $1/d$.

Очевидно, плотность последовательности может принимать только неотрицательные значения и не может быть больше 1.

Если $a_1>1$ (т. е. если последовательность A не содержит единицы), то $\alpha=0$; если плотность последовательности равна 1, то последовательность содержит все натуральные числа.

Л. Г. Шнирельман показал, что плотность суммы любых двух числовых последовательностей A и B с плотностями α и соответственно β не меньше, чем $\alpha+\beta-\alpha\beta$. Другими словами, если мы через γ обозначим плотность суммы $C=A+B$, то

$$\gamma\geqslant\alpha+\beta-\alpha\beta, \tag{2}$$

что можно заменить соотношением:

$$1-\gamma\leqslant 1-\alpha-\beta+\alpha\beta,$$

или

$$1-\gamma\leqslant(1-\alpha)(1-\beta), \tag{3}$$

распространимое по индукции на любое конечное число последовательностей.

При помощи предыдущей теоремы Шнирельман доказал следующую основную теорему: всякая последовательность положительной плотности есть базис натурального ряда. Другими словами, если для некоторой числовой последовательности A $\alpha > 0$, то сумма достаточного количества последовательностей A охватывает весь натуральный ряд.

Для доказательства допустим, что γ — плотность последовательности C, суммы k последовательностей A плотности α. Тогда согласно (3) $1-\gamma \leqslant (1-\alpha)^k$.

Для достаточно большого k правая часть станет меньше $\frac{1}{2}$ и вместе с тем $\gamma > \frac{1}{2}$. Из этого следует, что на любом сегменте $[1, n]$ расположено $r > \frac{n}{2}$ членов c: $c_1, c_2, \ldots, c_r$.

Если к ним присоединить нуль и числа $n-c_1$, $n-c_2$, ..., $n-c_r$, то получится всего $2r+1 > n+1$ чисел, принадлежащих отрезку $[0, n]$. Поэтому (по принципу Дирихле[1]) среди них должны быть равные, т. е. $n-c_i = c_j$, откуда $n = c_i + c_j$.

Другими словами, любое натуральное число n можно получить как сумму двух чисел из C, а это значит, что A есть базис натурального ряда (притом порядка $\leqslant 2k$), что и требовалось доказать.

Основную теорему Шнирельман постарался применить к решению проблемы Гольдбаха. Сделать это непосредственно не было возможности, так как плотность последовательности P′ 0, 1, 2, 3, 5, 7, 11, 13 ... (P′), состоящей из нуля, единицы и всех простых чисел, имеет плотность, равную нулю, поскольку $\frac{\pi(x)}{x} \to 0$, когда $x \to \infty$. Однако Шнирельману удалось доказать знаменитую теорему о том, что последовательность $P' + P'$ имеет положительную плотность.

Вместе с тем оказывается, что $P' + P'$, а следовательно, и P' является базисом натурального ряда. Из этого уже нетрудно заключить, что всякое натуральное число N, кроме 1, есть сумма ограниченного, не зависящего от N числа простых чисел.

Метод Шнирельмана, таким образом, позволил решить проблемы Гольдбаха в упрощенной формулировке. Это был первый существенный сдвиг в почти 200 лет казавшейся неприступной проблеме. Для своего времени результат Шнирельмана был фундаментальным и вызвал величайший интерес в математическом мире. Крупнейший специалист по теории чисел Э. Ландау писал: «Работа Л. Г. Шнирельмана содержит одно из величай-

---

[1] При размещении $n+1$ предмета в n ящиках по крайней мере в одном из них окажутся два или больше предметов.

ших достижений в теории чисел, до которого мне удалось дожить».

Исследования с помощью метода Шнирельмана выделились в самостоятельное и весьма плодотворное направление теории чисел.

Большое значение для развития теории чисел имеют работы выдающегося ленинградского математика — академика Юрия Владимировича Линника (род. в 1915 г. на Украине в городе Белая Церковь). Неодолимый интерес к математике заставил Ю. В. Линника после двух лет занятий на физическом факультете Ленинградского университета перейти на математический факультет, который он окончил в 1938 г. Представленная им в 1940 г. кандидатская диссертация сразу же была принята как докторская. С 1944 г. Ю. В. Линник — профессор Ленинградского университета, с 1953 г.— член-корреспондент АН СССР, а с 1964 г.— действительный член АН СССР. В 1947 г. Ю. В. Линнику присуждена Государственная премия, а в 1970 г.— Ленинская премия.

Ю. В. Линник работает над трудными задачами, его методы имеют яркий новаторский характер и обычно далеко выходят за пределы их первоначального применения.

Оригинальным аналитико-алгебраическим методом в теории чисел Ю. В. Линник решил проблему представления чисел тернарными (т. е. зависящими от трех переменных) квадратичными формами, которая долгое время не поддавалась усилиям крупнейших специалистов. Эти исследования привели Ю. В. Линника к непревзойденному до настоящего времени результату — всякое достаточно большое целое число можно представить суммой семи неотрицательных кубов, и к глубоким результатам о распределении целых точек на сфере и двуполостном гиперболоиде.

Методом Шнирельмана Ю. В. Линник в 1943 г. дал новое элементарное решение проблемы Варинга, в основном доказав, что для любого натурального n последовательность $0, 1^n, 2^n, \ldots$ $\ldots, k^n \ldots$ представляет собой базис натурального ряда.

Существенный вклад Ю. В. Линник внес в теорию L-функций Дирихле, которые представляют собой обобщение дзета-функции $\zeta(s)$ и для распределения простых чисел в арифметической прогрессии играют такую же роль, как функция $\zeta(s)$ для распределения простых чисел в натуральном ряде. L-функции Дирихле имеют вид

$$L(S, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^S},$$

где $S = \sigma + it$, а $\chi(n)$ — характер модуля k.

Характером $\chi(n)$ в теории чисел называют числовую функцию, определенную для всех целых n и удовлетворяющую следующим условиям:

1) $\chi(n) \neq 0$, т. е. не равна тождественно нулю, это значит, что существуют значения $\chi(n)$, отличные от нуля;

2) $\chi(mn) = \chi(m)\chi(n)$ для всех m и n;

3) существует такое целое число k (период), что $\chi(n+k) = \chi(n)$.

Если k наименьший из положительных периодов, то он называется основным модулем, а характер с основным модулем k обозначается $\chi(n, k)$.

Характером является, например, единичная функция $\chi(n) = 1$, т. е. функция, тождественно равная единице, а также так называемый главный характер по модулю k, который определяется условиями:

$$\chi(n, k) = \begin{cases} 0 \text{ при } (n, k) > 1 \\ 1 \text{ при } (n, k) = 1 \end{cases}$$

Относительно функции $L(s, \chi)$ для не главного характера английские математики Харди и Литлвуд высказали предположение, что ее критические нули так же, как и в случае дзета-функции $\zeta(s)$, лежат на прямой $\sigma = \frac{1}{2}$. Это предположение носит название расширенной гипотезы Римана. Если она справедлива, то из нее вытекали бы многие свойства о простых числах в арифметической прогрессии. Принимая ее, были получены некоторые условные результаты.

В период 1944—1952 гг. Ю. В. Линник разработал новое направление в теории L-функций — теорию L-функций в среднем, опирающуюся на то, что в среднем $L(s, \chi)$ данного модуля имеет мало нулей вблизи прямой $\sigma = 1$.

Для развития этого направления Ю. В. Линник создал также новый метод элементарной теории чисел, названный им «большим решетом». Этот метод, углубляющий метод эрастофенова решета, дает возможность высеивать последовательности с помощью простых чисел с возрастающим значением выбрасываемых вычетов.

Значение метода Ю. В. Линника в теории L-функций заключается в том, что во многих задачах теории чисел он может заменить расширенную гипотезу Римана. Так много лет назад была поставлена проблема о наименьшем простом числе в арифметической прогрессии $kx + l$, т. е. в прогрессии $l, l + k, l + 2k, \ldots$, где k и l числа взаимно простые. Ее можно было бы решить, если была бы верна расширенная гипотеза Римана. Но проблема состояла в том, как обойти эту гипотезу, которая и до сегодняшнего дня еще не доказана.

В 1944 г. Ю. В. Линник дал качественное решение этой проблемы. Он доказал, что в такой прогрессии (при $0 < l < k$) содержится простое число $p < k^c$, где c — абсолютная (т. е. не зависящая от k) константа.

Заметим, что в 1958 г. китайский математик Пан Чен-тонг, пользуясь методом Линника, показал, что $c \leqslant 5448$, а в 1965 г. Чен Ин-рун доказал, что $c \leqslant 777$.

В 1946 г. Ю. В. Линник дал при помощи своего метода новое доказательство теоремы Гольдбаха — Виноградова о представлении достаточно большого нечетного числа суммой трех простых. Вместе с тем было показано, что и здесь расширенную гипотезу Римана, которую Харди и Литлвуд применили для условного доказательства этой теоремы, можно обойти.

Венгерский математик А. Реньи, работавший под руководством Ю. В. Линника, в 1948 г. доказал, что всякое большое четное число можно представить в виде суммы простого числа и произведения не более k простых чисел. Ученик Линника А. И. Виноградов доказал, что каждое достаточно большое четное число является суммой двух целых, каждое из которых содержит не более трех множителей. Наилучший результат в этом отношении получен А. А. Бухштабом в 1965 г. Он показал, что каждое достаточно большое четное число может быть представлено суммой простого числа и произведения не более трех простых чисел.

Развивая метод Линника, А. И. Виноградов получил важные результаты в исследованиях по замене расширенной гипотезы Римана теоремами типа большого решета.

Синтезируя теоретико-числовые и теоретико-вероятностные соображения, Ю. В. Линник развил в 1957—1961 гг. новый метод аналитической теории чисел, названный автором дисперсионным. Этим методом им была, в частности, решена классическая проблема Харди — Литлвуда о представлении каждого достаточно большого целого числа в виде суммы простого числа и двух квадратов целых чисел, т. е. в виде $N = p + k^2 + l^2$.

Мы коснулись работ академика Ю. В. Линника только в области теории чисел. Почти столько же работ ученого принадлежит теории вероятностей.

Методы Ю. В. Линника пользуются мировой известностью и широко применяются не только у нас, но и за рубежом.

Очень важную роль в теории трансцендентных чисел играет аналитический метод, созданный членом-корреспондентом Академии наук СССР А. О. Гельфондом (1906—1968 гг.).

Александр Осипович родился в 1906 г. в Петербурге. В 1927 г. он закончил Московский государственный университет. С 1931 г. А. О. Гельфонд — профессор в Московском государственном университете, с 1933 г. работает в Математическом институте Академии наук СССР, а с 1939 г. членом-корреспондентом Академии наук СССР. Основное направление научной деятельности А. О. Гельфонда — аналитическая теория чисел и теория интерполирования и приближения аналитических функций комплексных переменных.

Исследования по вопросу об арифметической природе заданных чисел, в особенности выяснение того, являются ли эти числа алгебраическими или трансцендентными, принадлежат к труднейшим задачам современной математики. Только лишь в 1873 г. французский математик Ш. Эрмит доказал трансцендентность e, а в 1882 г. немецкий математик Ф. Линдеман — трансцендентность числа π.

После результатов, полученных Эрмитом и Линдеманом, долгое время не удавалось добиться новых значительных успехов в рассматриваемой области.

На международном математическом конгрессе в 1900 г. Д. Гильберт в качестве одной из 23 актуальных математических проблем выдвинул задачу (проблема № 7) исследовать, являются ли трансцендентными числа вида α^β, где α и β — алгебраические числа, причем α отлично от 0 и 1, а β — иррационально (проблема трансцендентности чисел вида α^β была впервые в частной форме поставлена Эйлером), и, в частности, является ли трансцендентным число $2^{\sqrt{2}}$.

Несмотря на усилия многих ученых, эта проблема долгое время не поддавалась решению. Только в 1929 г. А. О. Гельфонду удалось найти частное решение. Углубив свой метод введением в него новых идей, он дал в 1934 г. полное ее решение и доказал, что все числа, о которых идет речь в этой проблеме, являются трансцендентными.

Решение классической проблемы Гильберта принесло автору мировую славу.

Из результата А. О. Гельфонда непосредственно следует, что трансцендентными будут, например, все десятичные логарифмы рациональных чисел, если сами они не являются рациональными числами. Действительно, если бы $\lg r$, где r — рациональное число, было алгебраически иррациональным, то число $10^{\lg r}$ согласно результату А. О. Гельфонда должно было бы быть трансцендентным, между тем $10^{\lg r} = r$ — число рациональное.

В 1940 г. А. О. Гельфонд дал новое приложение своего метода и получил глубокие теоремы из теории диофантовых уравнений, например, если α, β, γ — алгебраические числа (не все являющиеся алгебраическими единицами, а $\gamma \neq 2^n$, где n — целое рациональное число), то диофантово уравнение $\alpha^x + \beta^y = \gamma^z$ имеет лишь конечное число решений в целых рациональных числах x, y, z.

А. О. Гельфонд выяснил, и это весьма интересно, что вопросы приближения функции целочисленными полиномами связаны с вопросами распределения простых чисел.

В последние десятилетия А. О. Гельфонд, все более совершенствуя свои прежние методы, получил возможность указать на ряд новых классов трансцендентных чисел. Метод Гельфонда успешно используется также другими авторами, как советскими, так и зарубежными.

Очень важных результатов добился ученик А. О. Гельфонда А. Б. Шидловский, который исследовал вопрос трансцендентности и алгебраической независимости значений функций, являющихся решением некоторых линейных дифференциальных уравнений.

Заметим, что комплексные числа u и v называются алгебраическими независимыми, если нет такого многочлена от двух переменных $P(x, y) \not\equiv 0$ (тождественно не равного нулю) с алгебраическими коэффициентами, для которого $P(u, v) = 0$. В противном случае u и v называются алгебраически зависимыми. Это понятие можно распространить на n чисел. При $n = 1$ определение переходит в определение трансцендентности числа.

Вопросы алгебраической независимости решаются с большим трудом. Так, например, до сих пор проблема алгебраической независимости чисел e и π остается без решения.

В области алгебраической теории чисел и ее приложений к диофантову анализу в 20—40-е годы важные результаты были получены членами-корреспондентами АН СССР Б. Н. Делоне (род. 1890 г.), Н. Г. Чеботаревым (1894—1947 гг.), Д. К. Фаддеевым (род. 1907 г.).

Н. Г. Чеботарев дал глубокое обобщение известной теоремы Дирихле о бесконечности простых чисел в арифметической прогрессии.

Б. Н. Делоне доказал, что кубическое уравнение Пелля $ax^3 + y^3 = 1$ (где a — целое число) может иметь, кроме тривиального решения (0,1), не более одного решения в целых числах. Он показал также, что для каждого заданного значения a можно установить, существует ли нетривиальное решение и как найти его, и доказал также, что уравнение $ax^3 + bx^2y + cxy^2 + dy^3 = 1$ имеет не более 5, а иногда 5 решений в целых числах, и указал алгоритм решения.

До работ Б. Н. Делоне было лишь известно — это доказал норвежский математик А. Туэ в 1909 г.,— что неопределенное уравнение $a_0x^n + a_1x^{n-1} \cdot y + \ldots + a_ny^n = c$ (где $a_0, a_1, \ldots, a_n$, c — целые и многочлен $a_0t^n + a_1^{n-1} + \ldots + a_n$ не приводим в поле рациональных чисел) имеет только конечное число целых решений при $n \geqslant 3$. Однако метод А. Туэ не позволял найти сами решения, он не давал даже ответа на вопрос, существуют ли вообще у данного уравнения решения.

Ученик Б. Н. Делоне Д. К. Фаддеев развил метод своего учителя и получил новые результаты. Он, в частности, обнаружил более широкий класс уравнений третьей степени, чем уравнения Пелля, допускающих эффективное решение.

Начиная с конца 40-х годов блестящих успехов в алгебраической теории чисел добился другой ученик Б. Н. Делоне — член-корреспондент АН СССР лауреат Ленинской премии Игорь Ростиславович Шафаревич (род. в 1923 г.).

Необыкновенные способности И. Р. Шафаревича проявились рано. В 14 лет он закончил курс математики средней школы, в 16 лет — Московский университет, а к 22 годам им была уже подготовлена докторская диссертация. В 1949 г. И. Р. Шафаревич получил фундаментальный результат в области теории алгебраических чисел, а именно он открыл и доказал общий закон взаимности в области теории алгебраических чисел.

Чтобы дать представление об общем законе взаимности Шафаревича, отметим, во-первых, что при помощи квадратичного закона взаимности для нечетных простых чисел можно не только по данному a и простому p определить, является ли a квадратическим вычетом числа p или нет, но и решить более сложную обратную задачу о том, как найти те простые числа p, для которых заданное число a является квадратическим вычетом числа p.

Для случая $a = -1$ при помощи указанного закона устанавливается, что минус единица является квадратическим вычетом всех простых чисел вида $4m + 1$ и квадратическим невычетом всех простых чисел вида $4m + 3$.

Значимость этого факта вытекает из следующего. Как известно, простыми числами называются числа 2, 3..., которые не имеют собственных делителей (т. е. делителей, кроме 1 и самого числа). При этом речь идет о целых рациональных делителях.

Оказывается, что имеет смысл расширить поле рациональных чисел, присоединяя к нему иррациональное число $\sqrt{a}$, где a — целое рациональное. Тогда получается множество чисел вида $x + y\sqrt{a}$, где x и y — рациональные числа, также образующие поле, так называемое квадратичное поле $R(\sqrt{a})$.

Таким расширением является, например, поле комплексных чисел $a + bi$. Множество чисел $a + bi$, где a и b — целые рациональные числа, играют в этом поле такую же роль, как целые числа в поле рациональных чисел. Они образуют кольцо, которое носит название гауссова кольца целых комплексных чисел, поскольку Гаусс первый исследовал его.

В $R(\sqrt{-1})$ простое число 29 уже не является «простым», оно разложимо на множители: $29 = (5 + 2i)\cdot(5 - 2i)$, притом однозначно, если не обращать внимания на порядок следования сомножителей и множителей «единиц», т. е. $1, -1, i, -i$.

Но не всякое обычное простое число разложимо в $R(\sqrt{-1})$, так, например, 31 так разложить нельзя. Оказывается, что из простых чисел p в $R(\sqrt{-1})$ разложимы в указанном смысле только простые числа вида $4m + 1$ (а простые числа вида $4m + 3$ неразложимы), т. е. как раз те, для которых 21 является квадратическим вычетом.

Вообще: только те простые числа p, по которым a является квадратическим вычетом, разлагаются в квадратичном поле $R(\sqrt{a})$, другие p — нет. Но вопрос квадратичной вычетности решается законом взаимности. Таким образом, квадратичный закон взаимности показывает, какова зависимость арифметики квадратичного поля от арифметически рационального поля, так как законы разложимости определяют всю арифметику. Как раз в этом фундаментальность закона взаимности.

Насколько важным является вопрос разложимости в $R(\sqrt{a})$, видно из следующего примера, относящегося к $R(\sqrt{-1})$. Так как число минус единица является квадратическим вычетом для всех p вида $4m+1$ и квадратическим невычетом для всех p вида $4m+3$, то первые, и только они, всегда представимы формой x^2+y^2, притом еще единственным образом и с условием $(x, y)=1$. Это связано с тем, что из $p=(x+y\sqrt{-1})\cdot(x-$ $-y\sqrt{-1})$ следует $p=x^2+y^2$ и наоборот.

Так, с помощью арифметической теории алгебраических чисел очень просто доказываются знаменитые теоремы Ферма и Эйлера относительно простых чисел p вида $4m+1$.

Вопросы, аналогичные тем, которые мы только что рассмотрели, возникают при переходах к более сложным полям. Несмотря на большие усилия виднейших ученых (Гаусса, Эйнштейна, Куммера, Гильберта и др.), в течение 150 лет эти вопросы удалось решить только для разных частных случаев. Общий закон взаимности Шафаревича решает указанную проблему в наиболее общем виде: он устанавливает, как разлагаются на простые множители в поле K простые множители поля k, т. е. зависимость арифметики поля K от арифметики поля k, где k — произвольное поле алгебраических чисел m-й степени, а K — его расширение, полученное присоединением к нему $\sqrt[n]{\alpha}$, где α число поля k.

И. Р. Шафаревич решил также другую знаменитую алгебраическую задачу, известную под названием обратной задачи Галуа для разрешимых групп.

В последние годы И. Р. Шафаревич решил третью важнейшую для теории алгебраических чисел задачу о том, является ли любое поле алгебраических чисел подполем одноклассного поля алгебраических чисел. Оказалось, что нет. Этим решена в отрицательном смысле так называемая «проблема башни», поставленная Гильбертом. Работы И. Р. Шафаревича получили международное признание и выдвинули молодого советского ученого в ряды выдающихся математиков современности.

Больших успехов в алгебраической теории чисел добился также ученик И. Р. Шафаревича, лауреат Ленинской премии Юрий Иванович Манин (род. в 1938 г.).

Около 50 лет назад английский математик Морделл высказал предположение («гипотеза Морделла»), которую можно сформулировать так: уравнение $f(x, y)=0$, где $f(x, y)$ — многочлен степени >3, достаточно общего характера, имеет лишь конечное число рациональных решений. Использовав созданный им новый метод «дифференциальных операторов», Ю. И. Манин доказал функциональный аналог этой гипотезы, т. е. ее обобщение для случая, когда коэффициенты и неизвестные являются некоторыми рациональными или алгебраическими функциями.

Результат Ю. И. Манина произвел на математиков всего мира большое впечатление.

* * *

Перечень славных достижений русских и советских математиков в развитии теории чисел можно было бы продолжить. Можно было бы остановиться на теоретико-числовых работах А. Я. Хинчина (1894—1959 гг.), касающихся диофантовых приближений — решения неравенств в целых числах, и связанных с теорией вероятности, на фундаментальных результатах И. П. Кубилюса и его учеников в вероятностной теории чисел; на работах Б. Н. Делоне и Б. А. Венкова (род. 1900 г.) в геометрии чисел и многих других исследованиях.

Однако, на наш взгляд, и перечисленные достижения уже свидетельствуют о выдающемся вкладе русских и советских математиков в развитие теории чисел.

СОДЕРЖАНИЕ

Стр.

Леонард Эйлер — основоположник теории чисел как науки 3

Петербургская школа теории чисел 6

Советская школа теории чисел 12

Шефтель Хенехович МИХЕЛОВИЧ

ИЗ ИСТОРИИ ТЕОРИИ ЧИСЕЛ

Редакторы *Е. А. Авсиевич, Р. Г. Базурин*

Обложка *В. А. Яковлева*

Художественный редактор *В. Н. Конюхов*

Технический редактор *Е. М. Лопухова*

Корректор *Г. К. Храпова*

А 04775. Сдано в набор 15/V 1970 г. Подписано к печати 12/VI 1970 г. Формат бумаги 60×90/16. Бумага типографская № 3. Бум. л. 1,0. Печ. л. 2,0. Уч.-изд. л. 1,67. Тираж 40 700 экз. Издательство «Знание». Москва, Центр, Новая пл., д. 3/4. Набрано во 2-й типографии изд-ва «Наука». Заказ 573. Отпечатано в типографии изд-ва «Знание». Москва, Центр, Новая пл., д. 3/4, Заказ 1498.

Цена 6 коп.

ДОРОГИЕ ТОВАРИЩИ!

Всем интересующимся точными науками издательство «Знание» предлагает книги естественно-научного факультета.

В 1970 году выйдут:

Алякринский Б. С. **О талантах и способностях.** (Психологические очерки).

Горстко А. Б. **Поиски правильных решений** (О принципах рациональной деятельности человека).

Игнациус Г. И. **Теория поля** (Математический анализ функций нескольких переменных).

Нигматулин И. Н. **Современные ядерные реакторы.**

Для того, чтобы получить указанные книги, вам необходимо обратиться в ближайший книжный магазин и сделать заказ по тематическому плану издательства «Знание» на 1970 год, № 162, 163, 164, 166.

ИЗДАТЕЛЬСТВО «ЗНАНИЕ»