I. R. Shafarevich, Euler's Investigations on Number Theory, *Math. Ed.*, 2007, Issue 3, 2–12

Исследования Эйлера по теории чисел

И. Р. Шафаревич

Этот год — год 300-летнего юбилея Леонарда Эйлера (4 (15) апреля 1707, Базель — 7 (18) сентября 1783, Санкт-Петербург). Наш журнал планирует ряд публикаций, посвященных великому ученому. Предлагаем вниманию читателей статью Игоря Ростиславовича Шафаревича, посвященную трудам Эйлера по теории чисел.

Эйлер родился в 1707 г. в Швейцарии, но провел большую часть своей активной научной жизни в России.

Этими обстоятельствами объясняется то, что в этом году отмечается 300-летие его рождения и, что в России эта дата привлекает особое внимание.

Эйлер был одним из самых широких математиков, когда-либо живших на Земле. Его математические исследования относятся к анализу, дифференциальной геометрии, теории чисел, теории приближенных вычислений и другим вопросам математики, а так же и к приложениям математики в физике и небесной механике и даже математическим проблемам, возникающим в технических областях, например, в баллистике или кораблестроении. Полное собрание его сочинений занимает более 70-и томов. Из них теории чисел посвящены лишь 4.

Однако, в этих работах не только содержатся фундаментальные идеи, определившие дальнейшее развитие теории чисел, но и основополагающие открытия в других областях, сделанные Эйлером в связи с вопросами теории чисел.

В ту эпоху, когда жил Эйлер (то есть, в XVIII веке), блистательные успехи анализа сделали его самой популярной частью математики. Некоторые ученые, целиком посвятившие себя анализу и близким областям, не чувствовали, видимо, принципиальной значительности вопросов "о числах", как тогда говорили (чего нельзя сказать как о математике XVII века, так и более поздней XIX и XX веков). Тем более удивительно, что теоретико-числовые исследования Эйлера продолжались в течении приблизительно 50-ти лет. Причем он неоднократно (возможно, полемизируя с некоторыми высказываниями современных ему математиков) выражал свое мнение, что он не чувствует необходимости оправдываться в том, что потратил столько времени и усилий на эти вопросы. Так, он писал: "Высший Анализ столь многим обязан Диофантову методу (то есть, определенному разделу теории числе), что мы не имеем права им пренебрегать". Кроме того, Эйлер, видимо, ясно чувствовал эстетическую привлекательность вопросов теории чисел. Он не раз пишет об "очень красивых" и "божественных" (he??liche) закономерностях, которые он открыл или лишь предвидел.

Особенностью работы Эйлера в математике (не только в теории числе), было то, что он исключительно долго держал памяти интересовавшие его некогда вопросы. Иногда он через 10 лет возвращался к доказательству, которое было неполным, чтобы заменить его более убедительным (или более ясным) рассуждениям. Поэтому дальше я изложу некоторые из основных его результатов в теории чисел (конечно, не все — их было слишком много) не в хронологическом порядке, а группируя их по их идейному содержанию. Начну же с коротких биографических данных. Практически все мое изложение заимствовано из прекрасной книги покойного А.Вейля по истории теории чисел ("От Хаммураби до Лежандра") — фактически это сокращенный пересказ главы этой книги, посвященной Эйлеру. Я очень надеюсь, что книга будет некогда переведена на русский язык. Она будет полезна всем, интересующимся математикой и доставит им громадное удовольствие — книга читается как роман.

1. Биографические сведения

Вся математическая жизнь Эйлера связана с Российской Академией Наук. Организация Академии Наук в Петербурге была задумана Петром I (Петром Великим) в конце его жизни. Начало ее деятельности приходится на царствование Екатерины I. Тогда молодой Эйлер и был приглашен в Петербург. Когда он прибыл в Петербург, ему еще не было 20-ти лет. Вскоре он был зачислен в число сотрудников академии, сначала в низшем звании "адъюнкта". В Петербурге он женился. Там же перенес тяжелую болезнь, в результате которой потерял правый глаз — на некоторых портретах мы видим Эйлера с повязкой на правом глазе.

В 1740 г. в связи со смертью императрицы Анны Иоанновны, в России разразился политический кризис и жизнь здесь стала неспокойной. Но тогда же в Берлине на прусский престол взошел Фридрих II (Фридрих Великий). Дорожа своим прозвищем "Король — философ", он, конечно, решил основать в Берлине Академию Наук, куда пригласил и Эйлера. Эйлер последовал этому приглашению и был даже назначен президентом Берлинской академии. Он прожил в Берлине 24 года. Однако, никакого разрыва с Петербургской академией не произошло. Эйлер числился это время почетным иностранным членом нашей академии и опубликовал в ее изданиях более 100 работ (а В Берлине — 127).

Постепенно отношения между Эйлером и Фридрихом Великим (который, видимо, вообще обладал капризными и тяжелым характером), становились все прохладнее. Тем временем русский престол заняла Екатерина II (Екатерина Великая), стремившаяся вообще продолжить начинания Петра Великого. Это относилось и к академии наук, туда она пригласила вернуться Эйлера. После переговоров, продолжающихся 3 года, Эйлер вернулся в Петербург в 1766 г. Там он и работал до самой смерти в 1783 г.

Еще в Берлине у Эйлера стал развиваться катаракт на левом (неповрежденном) глазе. В России он перенес операцию, которая прошла успешно, но в глаз была занесена инфекция. В результате Эйлер стал терять зрение и в конце концов почти полностью его лишился. Это, однако, не сказалось на его математическом творчестве. Многие свои работы и книга в тот период он диктовал сотрудникам и ученика, в которых у него не было недостатка. За это время им было написано несколько сот работ.

Теперь я перехожу к описанию некоторых направления размышлений Эйлера в теории чисел.

II. Использование свойств делимости алгебраических чисел

В большой степени исследования Эйлера по теории чисел были связаны с развитием традиции, идущей от Ферма. Речь шла как о воссоздании доказательств некоторых утверждений Ферма (части самим Ферма не приводившихся), так и об исследовании вопросов, лишь поставленных Ферма.

В частности, одним из толчков к теоретико-числовым исследованиям Эйлера послужило весьма популярное утверждение Ферма о том, что уравнение

$$x^n + y^n = z^n \tag{1}$$

при $n > 2$ не имеет решений, в целых числах x, y и z, которые все отличны от 0. Один раз Ферма написал, что располагает доказательством этого утверждения (замечание на полях книги Диофанта). В других же случаях, говоря о близких вопросах, он больше никогда такого утверждения не делал. Поэтому мне кажется весьма правдоподобной мысль, высказанная в уже упоминавшейся книге А.Вейля — что Ферма таким доказательством и не располагал. Случай $n = 4$ может быть без труда разобран на основании соображений, которыми Ферма владел и весьма вероятно, что в момент чтения книга Диофанта он думал, что тот же метод может быть применен и в общем случае.

Эйлер нашел несколько доказательств утверждения Ферма в случае $n = 3$. Многие исследователи предполагают, что Ферма обладал доказательством этого факта, где он заменял разложение на множители равносильными формулами. В основе всех этих доказательств лежит (иногда искусно спрятанная за элементарными по виду рассуждениями) совершенно новая идея:

разложения многочлена на множители с иррациональными коэффициентами. В результате вопрос сводится к простым утверждениям относительно разложения на множители некоторых иррациональных чисел. Этим Эйлер положил начало громадной новой области, арифметике алгебраических чисел.

Мы изложим вариант доказательства Эйлера, эквивалентной приводимым им рассуждениям, но более ярко выделяющий описанную выше идею. В применении к уравнению (1) в случае $n = 3$ можно переписать его в виде

$$y^3 = z^3 - x^3$$

и разложить правую часть на множители:

$$z^3 - x^3 = (z - x)(z - \rho x)(z - \rho^2 x) \tag{2}$$

где $\rho = \frac{-1+\sqrt{-3}}{2}$ комплексное число, удовлетворяющие условию $\rho^3 = 1$ (другими такими числами являются $\frac{-1-\sqrt{-3}}{2}$ оба встречаются в правой части соотношения (2)).

Мы видим совершенно новый подход к нашей проблеме, требующий, однако рассмотрения нового типа чисел. Это будут все комплексные числа, которые можно представить в виде $m+n\rho$, где m и n целые рациональные числа. Совокупность всех таких числе обозначал через R. Легко убедиться, что сумма и разность двух чисел из R, содержится в R. Но верно и гораздо более поразительное свойство: произведение двух чисел из R, содержится в R. Это следует из того что $\rho^2 + \rho + 1 = 0$ (как легко проверить) и если $\alpha = a + b\rho$, $\beta = m + n\rho$, то $\alpha\beta = m + (an + bm)\rho + bn\rho^2 = am - bn + (an + bm - bn)\rho$. Таким образом, числа совокупности R похожи на целые рациональные числа и для них можно поставить аналогичная вопросы: о разложении числа на простые множители, единственности такого разложения и т.д. ....

Это вопросы разной степени трудности то, что разложение на простые (далее на разложимые) множители возможно убедится не трудно. Проще всего для этого воспользоваться выражением $N(a+b\rho) = |a+b\rho|^2 = a^2+ab+b^2$. Из теперь хорошо известных свойств комплексных чисел, следует, что $N(\alpha\beta) = N(\alpha)N(\beta)$, где α и β — два произвольные числа нашей совокупности R. Так как $N(\alpha)$ положительное целое рациональное число, то если бы число α не было простым, а имело делитель β, $\alpha = \beta\gamma$, где γ другое число нашей совокупности то мы имели бы разложение $N(\alpha) = N(\beta)N(\gamma)$. Продолжая так (если β не простое) мы прийдем к числу, для которого $N(\xi) = 1$. Легко проверить, что таких чисел всего шесть: ± 1, $\pm\rho$ и $\pm\rho^2$. Здесь мы встречаемся с первым отличием совокупности R от совокупности целых рациональных чисел. Указанные 6 чисел являются единственными в нашей совокупности для которых обратное тоже число из R. (Среди целых рациональных чисел такими являются только ± 1). Такие числа называют обратными в R. Очевидно, что и понятие делителя и простого числа в R имеет смысл раз????лировать только "с точностью до обратимых множителей". Предшествующее рассуждение и является доказательством того, что любое число из R является произведением простых чисел — с точностью до обратимого множителя, конечно.

Дальше мысль Эйлера шла, очевидно, примерно так:

Рассмотрим тот случай, когда сомножители в правой части равенства (2) взаимно просты (случай, когда это не так, может быть рассмотрен вполне элементарно). Тогда произведение взаимно простых чисел является кубом. *Ясно*, пишет Эйлер, что это возможно только, когда каждый из них является кубом. Тогда мы можем записать $z - x\rho = (p - q\rho)^3$ и $z - x = k^3$, а отсюда элементарными преобразованиями не трудно найти решение x_1, y_1, z_1 уравнения (1) с меньшими, но отличными от 0 значениями (например, $0 < z_1 < z$). Мы пропускаем эти элементарные преобразования, которые можно, например, прочесть в книге Р.О.Кузьмина и Д.К.Фаддеева "Алгебра и арифметика комплексных чисел".

Но самым интересным — и важным для будущего математика — является утверждение, сформулированное Эйлером как *очевидное*. На самом деле, оно является действительно очевидным, только если для совокупности R доказана однозначность разложения на простые множители (разумеется, с точностью до множителей, обратимых в R).

По-видимому, Эйлер не задумывался над вопросами однозначности разложения на простые множители, так как он подобные высказывания делал и для других выражений, которые приводят к другой области R', для которой разложение на простые множители не единственно. Он, например, рассматривает вопрос о решении в целых числах уравнения $x^2 + Ay^2 = z^4$ для некоторого условия A для этого пользуемся разложения $x^2 + Ay^2 = (x + y\sqrt{-A})(x - y\sqrt{-A})$. Как он утверждает, отсюда следует, что $x + y\sqrt{-A} = (p - qR - A)^\lambda$ с некоторыми целыми p и q. Это рассуждение приводит к рассмотрению совокупности R', состоящей из чисел вида $x + y\sqrt{-A}$ при любых целых рациональных числах x и y. Утверждение, которое делает Эйлер, было бы верно, если бы разложение на простые множители в совокупности R' было единственным. Это, однако, не всегда так. Например, при $A = 5$ мы имеем:

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

и все числа в этом равенстве — простое (в совокупности чисел вида $x + y\sqrt{-5}$), как нетрудно проверить, так что мы имеем два разных разложения на простые множители.

Эйлер явно понимал общематематическую значимость сделанного им шага. Например, в книге "Алгебра" он пишет: "Этот метод тем более замечателен, что он исходит из тории иррациональных чисел, которая иначе была бы бесполезной в Диофантовом анализе".

Одновременно такие же идеи были открыты французским математиком Лагранжем. В письме ему Эйлер пишет: "Я восхищен Вашим методом введения иррациональных и даже мнимых чисел в этом разделе анализа, который имеет дело только с целыми числами. Я уже несколько лет пользуюсь этой идеей. Я разработал это направление детально, показав, что для решения уравнения $x^2 + ny^2 = (p^2 + nq^2)^\lambda$ достаточно решить $x + y\sqrt{-n} = (p + q\sqrt{-n})^\lambda$.

К счастью для Эйлера, разложение на простые множители все же однозначно в той совокупности чисел R, которая нужна для доказательства предположения Ферма при $n = 3$. В не очень явном виде он сам это раньше доказал. С современной точки зрения однозначность разложения на простые множители в этой совокупности R следует, как и для целых рациональных чисел, из алгоритма Евклида — для R он дает остаток δ, для которого $N(\delta) < N(\beta)$ в представлении $\alpha = \beta\gamma + \delta$. Доказательство можно прочесть в цитированной выше книге Кузьмина и Фаддеева.

Эти вопросы были прояснены более поздними математиками. Но работы Эйлера впервые показали интересные исследования вопросов делимости внутри некоторых естественно возникающих совокупностей комплексных чисел, которые теперь называются "кольцами целых алгебраических чисел".

На этом мы расстанемся с работами Эйлера, связанными с арифметикой алгебраических чисел. Но интересно все же сказать еще несколько слов о гипотезе Ферма, связанной с уравнением (1). Судьба этого вопроса удивительна. В течение многих лет (и веков) им занимались выдающиеся математики, следуя по пути, намеченному Эйлером. Именно, для произвольного n выражение $z^n - x^n$ тоже можно разложить на множители: $z^n - x^n = (z - n)(z - \xi_1 x)...(z - \xi_{n-1} x)$, где 1, $\xi_1, \ldots, \xi_{n-1}$ — это различные корни многочлена $t^n - 1$: "корни из единицы". Очень скоро было замечено, что достаточно доказать предположение Ферма для простого значения n.

С числами ξ_i можно тоже связать некоторую совокупность чисел $\bar{R}$ и утверждение, высказанное Ферма было бы доказанным, если бы в этой совокупности разложения на простые множители было однозначно. Для небольших простых значений n это и было доказано. Так "Теорему Ферма" доказал Ламэ для $n = 5$. В таком же направлении двигались Коши, по-видимому — Дирихле — Куммер и другие. Куммер исследовал сам феномен неоднозначности разложения на простые множители и показал, что эта однозначность вообще говоря не имеет места, но восстанавливается, если к числам совокупности $\bar{R}$ добавить некоторые объекты, названные им "идеальными числами", а теперь называемые "Эйвизорами". Это дало возможность доказать предположение Ферма и для таких значения n, для которых разложение на простые множители в множестве $\bar{R}$ неоднозначно. Сам Куммер сделал это для простых $n \leq 100$ (другие математики — для любых $n \leq 5500$).

Так эта область развивалась много лет в одном и том же направлении. Еще в начале XX в. Гильберт считал вопрос Ферма — одним из самых насущных в теории чисел. Но вот в самом конце XX в. (1985 г.) вопрос был перенесен в совершенно другую область. Немецкий математик

Фрей заметил, что отрицательный ответ на вопрос Ферма привел бы к странным явлениям, плохо согласующимся с гипотезами, которые обсуждались (и хорошо подтверждались численным экспериментом) в казалось бы не связанной с этим вопросом области теории чисел так называемой "теории эллиптических кривых" с рациональными коэффициентами. Наконец, была указана и точная гипотеза, к тому времени не доказанная, но очень популярная — из которой утверждение Ферма вытекало бы. Это так называемая "гипотеза Таниямы–Вейля". Ее не трудно было бы и сформулировать, но вряд ли ее формулировка много пояснит неспециалисту. Наиболее поразительно, что она имеет дело с объектами, весьма далекими от первоначальной постановки вопроса Ферма.

Вскоре после того, как такая зависимость была установлена, гипотезу Таниямы Вейля (с небольшими ограничениями, достаточными для доказательства "Теоремы Ферма") доказали Уайлс и Тэйлор (в 1995 г.). Так была доказана и гипотеза Ферма.

Этот путь доказательства кажется мне поразительным, так как он в принципе отличен от того, которым пытались идти до того. Неужели интуиция обманула таких математиков как Эйлер, Коши, Куммер, Гильберт и многие другие? Быть может, дальнейшие исследования прольют свет на этот вопрос.

III. Исследование конечных алгебраических систем

Эйлер, собственно, создал основной аппарат теории чисел (работающий вплоть до наших дней): теорию сравнений по модулю целого числа m. Как известно, если считать эквивалентными два целых числа, если их разность делится на m, то целые числа распадутся на m множеств, сейчас называемых "классами вычетов". Сложение и умножение целых чисел переносится на классы вычетов, которые образуют "конечное кольцо" $\mathbb{Z}/m$ и многие свойства чисел сейчас формулируются как свойства этого кольца. Такая точка зрения восходит к Эйлеру. То, что сейчас называется "модулем", он называет "Демтелем" и обозначает d. Сам класс вычетов имеет у Эйлера особое название — "вид" (specio). Более того, он подчеркивает, что то или иное свойство относится к "виду", а не к его отдельным элементам. В частности, от исследует деление в кольце $\mathbb{Z}/d$. В частности, он доказывает существование частного α/β для двух "видов", из которых β должен состоять из чисел, взаимно простых с "делителем" d. При этом он подчеркивает, что речь не идет о делении чисел: частное $\gamma = \alpha/\beta$ определяется соотношением $\gamma\beta = \alpha$ в кольце $\mathbb{Z}/d$.

Начал Эйлер с восстановления доказательства теоремы, доказанной Ферма: если числа p простое, а a не делится на p, то $a^{p-1} - 1$ делится на p (сначала не зная, что ее доказал Ферма, позже ссылаясь на него). С современной точки зрения речь идет об определении порядка группы отличных от 0 элементов *поля* $\mathbb{Z}/p$ (сейчас она обычно обозначается $\mathbb{F}_p^*$). Для произвольного d Эйлер исследует соответствующую группу (элементов на которые возможно деление) в кольце $\mathbb{Z}/d$ при произвольном d. Ее порядок равен числу целых чисел, меньших d и взаимно простых с d. Сейчас это число обозначается $\varphi(d)$ "φ называется *функцией Эйлера*". (Сам Эйлер использовал обозначение πn). Известная "теорема Эйлера" утверждает, что если число a взаимно просто с "делителем" d, то $a^{\varphi(d)} - 1$ делится на d. Если d-простое число p, то это утверждение превращается в теорему Ферма, так как тогда $\varphi(p) = p - 1$. Сейчас это утверждение рассматривается как частный случай соотношения

$$g^{|G|} = e \tag{3}$$

для любого элемента g конечной группы G. Здесь $|G|$ обозначает число элементов в G, а e — ее единичный элемент. В большем числе доказательств, которые Эйлер нашел для своей теоремы, то, которое было опубликовано позже других, носит именно теоретико-групповой характер и сейчас может быть дословно приведено как доказательство соотношении (3) для произвольной конечной коммутативной группы.

Для случая, когда "делитель" d является простым числом. Эйлер исследует так же группу (конечно — это более поздний термин) по умножению отличных от 0 элементов этого поля. Основной результат заключается в том, что она циклическая. Элементарно это можно выразить так, что существует такое целое число g, что его степени g^k дают все возможные остатки

(кроме равного 0) при делении на p. Такое число g называется в теории чисел "первообразными корню? по модулю p", а показатели, которые мы обозначали через k — "индексами" соответствующих остатков. Умножение классов сводится тогда к сложению индексов, играющих в этом случае роль, аналогичную логарифмам.

Рассуждение Эйлера по сути чисто теоретико-групповое. Оно сейчас приводится, когда доказывается, что в любом поле K корни степени m из 1 образуют циклическую группу. (В случае $K = \mathbb{F}_p$, согласно теореме Ферма, $m = p - 1$).

В связи с этими и близкими исследованиями Эйлер доказывает что любой многочлен $f(x)$ с коэффициентами из $\mathbb{F}_p$ не может иметь в $\mathbb{F}_p$ больше корней, чем его степень. По существо, Эйлер обращает внимание на то, что в этом случае пригодно рассуждение, предложенное Декартом для аналогичного факта и числовых коэффициентов, в предшествующем веке (Эйлер приводит рассуждение только для нужного ему случая, когда $f(x) = x^n - 1$, то оно от этого предположения не зависит).

В других ситуациях Эйлер сталкивается со случаем, когда коэффициенты многочлена $f(x)$ принадлежат полю $\mathbb{F}_p$, но сам он в этом множестве корней не имеет. В этом случае он спокойно рассуждает об эти корнях, называя их, однако, "мнимыми" или "несуществующими". В этой связи А.Вейль делает, в уже не раз цитированной книге интересное замечание, с которым я хотел бы читателей познакомить.

Известно, что в анализе одно из основных достижений Эйлера состоит в рассмотрении многих важнейших функций — таких, как e^x, $\sin x$, $\cos x$ — для комплексных значений аргумента. Только тогда можно было хотя бы сформулировать поразительные соотношения, открытые и доказанные Эйлером. Например, знаменитое "тождество Эйлера":

$$e^{ix} = \cos x + i \sin x$$

В этих случаях Эйлеру было достаточно задать функцию степенным рядом, а потом заметить, что ряд сходится и для некоторых (часто — любых) комплексных значений аргумента.

Таким образом, он понимал, какая пропасть новых фактов возникает при рассмотрении уже знакомых функций в новой области. В приведенных примерах это распространение было столь естественно, что Эйлер даже его специально не оговаривал. Но вот, например, при его новом доказательстве того, что каждый многочлен с вещественными коэффициентами имеет вещественный или комплексный корень (тогда это называлось "основной теоремой алгебры") дело обстояло сложнее — и понимание этого затрудняло многих более поздних математиков. Эйлер считает, что многочлен $f(x)$ с вещественными коэффициентами имеет такие-то корни $\alpha_1, \ldots, \alpha_n$ и различается в произведение: $c(x-\alpha_1)...(x-\alpha_n)$, после этого доказывает, что корни являются комплексными числами, то есть могут быть представлены в виде $a+b\sqrt{-1}$. На первый взгляд здесь — очевидный прочный круг. Но для Эйлера существование корня у многочлена представляется само собой разумеющимся — и тут он находится на уровне более позднего развития математики (XX в.). Именно, для этого рассуждения нам достаточно построить какое-то поле K, в котором многочлен имеет n корней — а это можно сделать часто алгебраическим методами. Суть же рассуждения Эйлера заключается в доказательстве того, что эти корни можно представлять в виде $a + b\sqrt{-1}$. Именно такое доказательство (восходящее к Эйлеру) содержится во многих современных алгебраических трактатов (например, Ван дер Вардена).

И в переписке Эйлер ссылается на то, что постепенное расширение понятия числа обычно связано с тем, чтобы ранее не разрешимые уравнения имели решения. Надо только, чтобы подобное расширение приводило к области, где имеют место обычные законы алгебры и не приводило к противоречиям — и в качестве проверки этого Эйлер (здесь — в отличие от более современных взглядов) готов опереться на математическую практику.

Теперь я могу привести мысль, высказанную А.Вейлем по поводу теоретико-числовых работ Эйлера. В некоторых работах Эйлер рассматривает многочлены $f(x)$ с коэффициентами в поле $\mathbb{F}_p$, причем уравнение $f(x) = 0$ может иметь решение с $\mathbb{F}_a \in \mathbb{F}_p$, а может и не иметь. В первом случае Эйлер называет этот корень "вещественным", а во втором он все равно предполагает его существование, сам корень называет "так сказать, мнимым". Сейчас известно, что такие корни действительно существуют и содержатся в различных конечных полях, содержащих поле $\mathbb{F}_p$. И

Вейль предполагает, что в этих работах Эйлер делает первые шаги в теории конечных полей. Не даром долгое время конечные поля называемые "полями мнимостей Галуа".

IV. Разбиения на слагаемые

Эйлер положил начало большому разделу теории чисел с таким названием. Речь идет о числе представлений произвольного натурального числа n в виде суммы слагаемых специального типа например, различных натуральных или нечетных, но не обязательно различных и т.д. Причем разбиения, отличающиеся порядком слагаемых, не различаются. Например, равенства $6 = 1+5 = 1+2+3 = 2+4$ являются разбиениями на различные слагаемые, а $6 = 1+5 = 1+1+1+3 = 3+3$ разбиениями на нечетные, не обязательно различные слагаемые. Замечателен метод предложенный Эйлером. Для любого натурального числа n обозначим через a_n число разбиений числа n на слагаемые изучаемого типа. Мы получаем бесконечную последовательность чисел: a_1, a_2, a_2, ..., a_n .... Эйлер предлагает рассматривать их как коэффициенты некоторого степенного ряда, то есть рассмотреть ряд $1 + a_1x + a_2x^2 + ... + a_nx^n + ...$ Вполне может сказаться, что такая бесконечная сумма не имеет смысла ни для какого значения x, то есть наш ряд не сходится. Тем не менее, обычные правила действий над многочленами переносятся на такие образования. Чтобы подчеркнуть, что ряд не рассматривается как функция x, дающая какое-то значение для некоторых значений x, такие ряды сейчас называют §формальными степенными рядами".

Эйлер обнаружил, что оперирование с такими рядами приводит к нетривиальным утверждениям о числах разбитий на слагаемые того или иного вида. Особенно важно, что при некоторых условиях можно образовать и бесконечные суммы и произведения таких рядов. Например, бесконечное произведения таких рядов. Например, бесконечное произведение

$$(1 + u_1(x))(1 + u_2(x))...(1 + u_n(x))...$$

можно представить как формальный степенной ряд раскрывая по очереди скобы, если степенные ряды $u_i(x)$ начинаются со все бо?льших степеней x.

Я приведу только один пример результатов, которые Эйлер получил таким образом. Например, если представить бесконечное произведение $(1 + x)(1 + x^2)...(1 + x^n)...$ в виде степенного ряда $1 + a_1x + a_2x^2 + ... + a_nx^n + ...$, то его коэффициент a_n показывает, сколькими способами можно представить n в виде различных натуральных слагаемых ведь член x^n

Получается, когда мы берем (или не берем) член x из первой скобки, x^2 из второй и т.д.

Немного сложнее записать число разбиений на слагаемые, которые не предполагаются различными. Для этого заметим, что имеет место равенство

$$\frac{1}{1-u(x)} = 1 + u(x) + u(x)^2 + ... + u(x)^n + ...$$

где $u(x)$ — степенной ряд без свободного члена. Это равенство доказывается точно так же, как формула для бесконечной геометрической прогрессии. В частности,

$$\frac{1}{1-x} = 1 + x + x^2 + ... + x^n + ..., \quad \frac{1}{1-x^2} = 1 + x^2 + x^4 + ... + x^{2n} + ...$$

а значит, если записать выражение

$$\frac{1}{(1-x)(1-x^2)...(1-x^n)...}$$

в виде степенного ряда $1 + a_1x + a_2x^2 + ... + a_nx^n + ...$, то a_n будет равно числу разбиений n на слагаемые, не обязательно различные. Проверяется это тем же рассуждением, каким мы раньше пользовались. Действительно если в каком-то разбиении числа n входит числа 1 k_1 раз, 2 k_2 раза и т.д., то есть, если $n = k_1 + 2k_2 + ... + nk_n + ...$ то умножая член x^{k_1} из первой скобки на x^{2k_2} — из второй и т.д., мы получим x^n столько раз, сколько существует подобных разбиений. Можно видоизменить то же рассуждение, если нас интересуют разбиение только на нечетные слагаемые. Тогда соответствующий ряд запишется в виде

$$\frac{1}{(1-x)(1-x^3)...(1-x^5)...} \tag{4}$$

В частности, Эйлер исходит из очевидного тождества

$$(1+x)(1+x^2)(1+x^3)... = \frac{1-x^2}{1-x}\cdot\frac{1-x^4}{1-x^2}\cdot\frac{1-x^6}{1-x^3}\cdot\frac{1-x^8}{1-x^4}...$$

При этом каждый множитель $1-x^n$ в знаменателе при четном n сокращается с таким же множителем в числителе и в результате остается в точности произведение (4). Отсюда как бы "из ничего" вытекает теорема: число разбиений натурального числа на различные слагаемые, равно числу его разбиений на нечетные слагаемые (но не обязательно различные). Для $n = 6$ утверждение проверено в начале этого раздела.

Эйлер нашел способ вывести много аналогичных соотношений более сложным путем, рассматривая ряды, содержащие кроме x и другую неизвестную. Я не буду на этом более подробно останавливаться, так как вопрос изложен в моей книге "Избранные главы алгебры", а глава, ему посвященная напечатана в номере 3-4 этого же журнала за 1998 г. Интересно все же отметить, что в связи с подобными вопросами Эйлер столкнулся с любопытным во многих отношениях произведением $(1-x)(1-x^2)(1-x^3)...(1-x^n)$ и нашел для него красивое разложение в степенной ряд. Характерен способ, которым Эйлер нашел свой результат: он вычислил (указанным выше способом) представление этого произведения до 51-й (!) степени включительно. На этом основании он высказал общее предположение, но писал, что "это примечательное наблюдение я не могу еще доказать с геометрической строгостью". Доказательство своей гипотезы он действительно нашел но, немного меньше, чем 10 лет спустя.

Интересно отметить связь всего этого круга вопросов с утверждением Ферма, интересовавшим Эйлера почти всю его жизнь: что каждое натуральное число есть сумма четырех квадратов целых чисел. Это утверждение было доказано Лагранжем еще при жизни Эйлера. Эйлер нашел другое, более простое доказательство и в связи с этим заметил, что самым естественным было бы доказательство того, что возведя в 4-ю степень ряд §, мы получил ряд, в котором все коэффициенты отличны от 0. Именно это и доказал Якоби но уже в следующем веке, получив так же и формулу для числа таких представлений. А ряд, написанный Эйлером, лишь тривиальными слагаемым и множителем отмечается от "тэта-функции" излюбленного объекта исследований Якоби. Интересно заметить, что таким же путем, что и Эйлер, шли в XX в. Харди и Литтльвуд, исследуя разбиения на более сложные слагаемые (например, простые). Однако, теперь они рассматривали ряд как функцию комплексного переменного x. В несколько завуалированной форме та же идея используется и в методе И.Л.Виноградова (в частности, при доказательстве того, что всякое достаточно большое нечетное число равно сумме трех простых чисел).

V. Суммы степеней натуральных чисел

Многие математики предшественники Эйлера занимались суммами степеней последовательных натуральных чисел, то есть суммами

$$S_n(k) = 1^k + 2^k + ... + (n-1)^k \tag{5}$$

Для этих сумм были открыты красивые формулы, связанные с интересной последовательностью чисел, которые Эйлер назвал "Бернуллиевыми числами". Естественно возникала мысль найти нелогичные выражения и для случая отрицательных значений k — тем более, что если $k = -s$ и $s > 1$, то сумма в формуле (5) сохраняет смысл, если ее распространить на все натуральные числа. Сейчас получающееся выражение обозначается через $\xi(n)$:

$$\xi(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + ... + \frac{1}{n^s} + ... \tag{6}$$

и, ряд в правой части сходится при $s > 1$, как очень легко проверить. Мы пользуемся обозначением $\xi(s)$ для этой суммы, введенной Ременом через 100 лет после работ Эйлера. Но как найти

его значения? Например, чему равно $\xi(s)$, если $s = m$ — натуральное число. Простейший случай значение $\xi(q)$ интриговал тогда многих математиков. Например, Яков Бернулли писал, что, как он доказал, это число весьма близко к 1". Эйлер нашел значение $\xi(q)$ с 20 десятичными знаками, а потом и точное значение. Как писал Эйлер, оно "оказалось связанным с квадратурой круга". А именно, Эйлер привел рассуждения в пользу того, что $\xi(q) = \frac{\pi^2}{6}$. Тогда он был еще совсем молод (ему не было 30-ти лет) и этот результат, сообщенной им в письмах ряду математиков, сразу стал знаменит.

Поразителен тот путь, которым Эйлер пришел к своему результату. По-существу, Эйлер пользуется тем, что известно разложение в ряд функции $\sin x$ и решения уравнения $\sin x = u$ они равны $\alpha_n = n\pi$ при целом n. Он предполагает, что ввиду этого функция $\sin x$ может быть представлена как произведение

$$\prod_{n\neq 0}\left(1 - \frac{x}{\alpha_n}\right) \tag{7}$$

Тогда, рассуждая так, "как будто" имеем дело с многочленом, легко найти (он ссылается на формулы Ньютона), зная коэффициенты и корни, сумму квадратов его "корней". Это рассуждение вызвало ряд сомнений у его современников. Поразительно, что основные возражения были связаны не со смелым переносом на степенные ряды утверждений, относящихся к многочленам (хотя, с точки зрения современной теории аналитических функций то разложения функции $\sin x$ в произведение, которое предполагает верным Эйлер, связано с порядком роста ($\sin z$) при $|z| \to \infty$). Основной вопрос заключался в том почему рассматриваемая функция (например, $\sin x$), кроме "видимых" вещественных корней не имеет других мнимых"? Эйлер сам понимал, что это далеко не очевидно, хотя ссылаясь на совпадение его ответа с приближенным вычислением, писал: "поэтому я не колеблясь опубликовал этот результат, считая его безусловно верным".

Те же рассуждения, несколько усложненные, привели Эйлера к формулам для значения $\xi(n)$ для любого *четного* n: $\xi(n) = r_n\pi^n$, где r_n некоторые рациональные числа, определенным образом связанные с числами Бернулли. Характер значения $\xi(n)$ при $n > 1$ и *нечетном* не ясен до сих пор. Единственный известный результат — доказательство того, что $\xi(3)$ иррационально (в 1978 г.). Сейчас доказано, что $\xi(n)$ иррационально для бесконечного числа нечетных чисел n, но конкретно можно утверждать, что это верно лишь для $n = 3$.

Проведение более убедительного доказательства своих формул заняло у Эйлера более 10 лет! Он нашел многочлены степени n, стремящиеся к $\sin x$ при $n \to \infty$ и, разлагая их на множители, обосновал разложение (7) для $\sin x$. Как он пишет, это доказывает, что рассматриваемые им функции "не имеют других корней, кроме видимых действительных".

VI. Аналитическая теория чисел

Так называется раздел теории числе, где некоторые свойства целых чисел доказываются при помощи привлечения методов анализа. В конце IV раздела мы указали некоторые такие результаты, восходящие к идеям Эйлера. Но большинство таких результатов относится к функции (5) впервые рассмотренной Эйлером. Им же были указаны некоторые свойства этой функции, игравшие впоследствии основную роль в ее исследованиях и приложениях.

Прежде всего, речь идет о так называемом функциональном уравнении для ξ-функции". Так называется соотношение, имеющее вид:

$$\xi(1-s) = 2(2\pi)^{-s}\cos\frac{\pi s}{2}\cdot\Gamma(s-1)\xi(s) \tag{8}$$

Это соотношение кажется парадоксальным, если вспомнить, что $\xi(s)$ Эйлер определял рядом (5), который сходится лишь при $s > 1$, то время как аналогичный ряд, если в нем поставить $1 - s$, то время как аналогичный ряд, если в нем поставить $1 - s$ вместо s, расходится во всех возможных смыслах этого понятия. Но подобные соображения мало слушали Эйлера. Дальше я расскажу о пути, на котором Эйлер пришел к соотношению (8), чтобы читатели могли почувствовать стиль рассуждений.

Прежде всего. Эйлер установил соотношения (8) для тех значения s. для которых значение $\xi(s)$, а значит и всего выражения в провой части равенства (8) было ему известно — а именно, когда n — натуральное и четное число. Но это не снимает вопроса о сходимости — в данном случае, сходимости ряда $\xi(1-s)$. Чтобы можно было хоть в каком-то смысле сопоставлять ряды для $\xi(s)$ и $\xi(1-s)$, Эйлер вводит дополнительный параметр x и рассматривает ряды (для целого $s=n$) $1+4x+\frac{1}{2^m}x^2+\frac{1}{3^m}x^3+\ldots$, которые как легко показать, сходятся при $|x|<1$ и могут быть даже (в этой области значений x) представлены рациональной функцией от x и для них он устанавливает соотношение, которое при $x=1$ приводит к уравнению (8). (Надо предупредить читателей, что Эйлер рассматривает не ряд (5) для $\xi(s)$, ряд, задающий функцию, отличающегося от $\xi(s)$ некоторым тривиальным множителем — я пропускаю этот переход, чтобы не вводить лишних обозначений). Эйлер переходит от целых значений к произвольным в работе под названием "Замечания о красивой связи между рядами, связанными с прямым и обратными степенями". Это очень интересное и возможно. Еще не переосмысленное более поздними математиками исследование. Эйлера вообще привлекала задача построения аналитических функций $f(z)$, для которых значения в целых точках, то есть $f(n)$ совпадают с некоторой естественной последовательностью целых чисел. Конечно, функция $f(z)$ не определена тем. что известны ее значения $f(n)$ (например. $f(n)=0$ если $f(z)=\sin\pi z$), но для некоторых значений $f(n)$ Эйлер строит "естественное" продолжение $f(z)$. Так, он построил и изучил ту функцию, которую позже (по предложению Лежандра) стали обозначать $\Gamma(z)$ и для которой $\Gamma(n+1)=n!$. Именно она и входит в уравнение (8). А в первоначальном уравнении для натуральных четных значений n стояло $\left(\frac{n}{2}\right)!$ Кроме того, в уравнение входил некий множитель, равный $(-1)^{n/2}$, который Эйлер для любого s интерпретирует как $\cos\frac{\pi s}{2}$. Возможно, что Эйлер и сам считал, что в то эпоху его утверждение строилось на догадке. Во всяком случае, он говорит иногда о своих утверждениях как о "предположениях" и проверяет для некоторых значений s, а так же показывает. что тем же способом можно вычислить значения других рядов, в то время уже найденные иными методами. Но сейчас естественно напрашивается вопрос — не скрывается ли за "догадками" Эйлера некоторая теорема с точной постановкой вопроса и точным доказательством?

Кроме функционального уравнения (8) Эйлер нашел ряд других свойств функции $\xi(s)$. В частности, тождество, сейчас называемое "тождеством Эйлера", выражающее в аналитическом виде однозначность разложения целого числа в произведение простых чисел. Эйлер написал его только для натуральных значений s, но оно верно для любого $s>1$:

$$\xi(s)=\prod_p \frac{1}{1-\frac{1}{p^s}}, \tag{9}$$

где произведение в правой части распространено на все простые числа p. Эйлер исследовал и поведение $\xi(s)$ при $s\to 1$ и вывел из тождества (9). что ряд $\sum\frac{1}{p}$, распространенный на все простые числа, расходится. Это, конечно, дает совершенно новое доказательство бесконечности числа простых чисел, что подробнее изложено в моей уже цитированной книге (и напечатано в первом номере за 1998 г. этого журнала). Эйлер пишет так же, что порядок роста сумм ряда $\sum\frac{1}{p}$ равен логарифму порядка роста частных сумм гармонического ряда. Так как для последних сумм Эйлер знал, что они растут как $\ln N$, то для сумм $\sum\frac{1}{p}$ он получает порядок роста $\ln\ln N$ (где — обозначает натуральный логарифм).

Эйлер рассматривает так же ряды (сходящиеся, но не абсолютно). аналогичные $\xi(1)$, но распространенные на числа вида $4n+1$, $4n-1$, $3n+1$ или $3n-1$. Он находит их значения и указывает, что таким образом получается доказательство бесконечности числа простых чисел в этих арифметических прогрессиях. Ряды, которые он рассматривает, в теперешней терминологии — это L-ряды с характерами Дирихле. Именно таким путем Дирихле и доказал, уже в XIX в., бесконечность числа простых чисел, содержащихся в арифметической прогрессии вида $an+b$, если a и b взаимно просты.

Этот сжатый обзор не только не включает все работы Эйлера по теории чисел, но и далеко не все его важнейшие исследования в этой области. Все же, я надеюсь, что читатели по нему смогут почувствовать поразительные черты научного творчества Эйлера. Такие главные черты,

как мне кажется, две:

1) Это необычайная смелость, с которой Эйлер опирается на аналогии, частные случаи и т.д. для того, чтобы сформулировать свое видение математического мира. Он отнюдь не пренебрегает логическим выводом своих результатов. В частности, по поводу найденного им функционального уравнения для ξ-функции, он пишет: "надо надеяться, что усилия для искания безупречного (perfaite) доказательства будут более успешными, так как несомненно, что это прольет свет на множество аналогичных исследований". Здесь чувствуется и то, что именно Эйлер ценил в "безупречном" доказательстве: не принудительную констатацию верности факта, но большее понимание всей области. Однако сам факт он страшился "увидеть" каким-то образом и для этого "видения" логическое рассуждение было таким же приемом, как аналогия, частные случаи и т.д. Пожалуй, самое удивительное — это то, как часто "видение" Эйлера не только подтверждалось логическим доказательством, но и оказывалось плодотворным для дальнейшего развития области. Рискну высказать предположение, что общим знаменателем его приемов исследования было некоторое эстетическое чувство, которое он отражал, говоря о "божественных" закономерностях.

2) Вторая черта, типичная для работ Эйлера — это необычайная широта его математических интересов. При этом он, видимо, все время держал в голове области, которыми когда-либо занимался и легко использовал идеи и приемы, возникшие в одной области в другой, по видимости, с ней не связанной. Так что работы Эйлера часто трудно поддаются классификации про них не легко сказать, к какой области они относятся: анализу, алгебре или теории чисел. Короче говоря, он воспринимал всю математику как одно поле исследования.

Не удивительно, что влияние Эйлера на развитие математики было колоссальным. Части (как, например, с выводом функционального уравнения для ξ-функции) его исследования много позже повторялись математиками, не имевшими представления о его достижениях, и только еще позже математики, интересующиеся так же историей своей науки, обращали внимание на то, насколько Эйлер опередил свое время. Но еще чаще его идеи воспринимались и продолжались его более молодыми современниками и последователями (например, Лагранжем или Гауссом). Как пишет в своей книге Вейль "ни один математик никогда не достигал такого положения неоспариваемого лидерства во всех ветвях математики". Его старый учитель Иоганн Бернулли назвал его "первым математиком" "mathematicorum princeps". Этот термин в другие эпохи применялся и к другим математикам например, к Гауссу. Но впервые так был назван Эйлер.

Шафаревич Игорь Ростиславович,
Академик РАН, профессор,
доктор физ.-мат. наук.