КОРОЛЬ МАТЕМАТИКОВ

Не считать ничего сделанным, если еще кое-что осталось сделать.
Гаусс

В 1854 г. здоровье тайного советника Гаусса, как его именовали коллеги по Геттингенскому университету, решительно ухудшилось. Не могло быть и речи о продолжавшихся в течение двадцати лет ежедневных прогулках от Обсерватории до Литературного музея. Профессора, приближавшегося к восьмидесятилетнему рубежу, удалось уговорить обратиться к врачу! Летом ему стало лучше и он даже присутствовал на открытии железной дороги Ганновер — Геттинген. В январе 1855 г. Гаусс соглашается позировать художнику Геземану для медальона. По заказу Ганноверского двора уже после смерти ученого в феврале 1855 г. по этому медальону была изготовлена медаль. На медали под барельефом Гаусса было написано: Mathematicorum princeps (Король математиков). История всякого настоящего короля должна начинаться с детства, овеянного легендами. Гаусс в этом смысле не был исключением.

1. Дебют Гаусса

«Упорство, с которым Гаусс следовал по избранному им пути, бурный юношеский натиск, с которым он каждый раз, не взирая ни на что, преодолевал самые крутые подъемы, ведущие к цели, все эти трудные испытания закаляли его силы и делали его способным, после победы над препятствиями, уже устраненными другими, неудержимо идти вперед, опережая их. К этой хвале творческой самодеятельности я должен присоединить другое: похвалу юности. Я этим хочу сказать только то, что развитие математического гения подчиняется тем же законам, что

Молодой Гаусс (1803 г.)

и развитие всякой другой творческой способности. Для гениально одаренной личности годы юности, период, когда только что завершается процесс физического роста, являются эпохой великих, в изобилии сменяющих друг друга откровений; именно в эти годы гениально одаренный дух создает те новые, ему одному принадлежащие ценности, которые им будут впоследствии преподнесены миру» (Ф. Клейн).

Брауншвейг, 1777 – 1795. Гаусс не получил свой титул по наследству, хотя его отец Гергард Дидерих не был вовсе чужд математике. Мастер на все руки, прежде всего фонтанный мастер, но также и садовник, как его отец, Гергард Дидерих был известен своими успехами в счетном ремесле. Его услугами пользовались купцы во время ярмарок в Брауншвейге и даже Лейпциге, а еще он имел постоянный заработок в самой большой похоронной кассе Брауншвейга (место, которое он передал по наследству сыну от первого брака Георгу — отставному солдату).

Карл Фридрих родился 30 апреля 1777 г. в доме № 1550, что стоял на канале Венденгребене в Брауншвейге. По мнению биографов, он унаследовал от родных отца крепкое здоровье, а от родных матери яркий интеллект. Ближе других был к будущему ученому дядя Фридерихс — искусный ткач, в котором, по словам племянника, «погиб прирожденный гений». Гаусс говорил о себе, что он «умел считать раньше, чем говорить». Самая ранняя математическая легенда о нем утверждает, что в три года он следил за расчетами отца с каменщиками-поденщиками и неожиданно поправил отца, причем оказался прав.

В 7 лет Карл Фридрих поступил в Екатерининскую народную школу. Поскольку считать там начинали с третьего класса, первые два года на маленького Гаусса внимания не обращали. В третий класс ученики обычно попадали в 10-летнем возрасте и учились там до конфирмации (15 лет). Учителю Бюттнеру приходилось заниматься одновременно с детьми разного возраста и разной подготовки. Поэтому он давал обычно части учеников длинные задания на вычисление, с тем чтобы иметь возможность беседовать с другими учениками. Однажды группе учеников, среди которых был Гаусс, было предложено просуммировать натуральные числа от 1 до 100. (Разные источники называют разные числа!) По мере выполнения задания ученики должны были класть на стол учителя свои грифельные доски. Порядок досок учитывался при выставлении оценок. 10-летний Гаусс положил свою доску, едва Бюттнер кончил диктовать задание. К всеобщему удивлению, лишь у него ответ был правилен. Секрет был прост: пока диктовалось задание, Гаусс успел переоткрыть формулу для суммы арифметической прогрессии! Слава о чудо-ребенке распространилась по маленькому Брауншвейгу.

В школе, где учился Гаусс, помощником учителя, основной обязанностью которого было чинить перья младшим ученикам, работал некто Бартельс, интересовавшийся математикой и имевший несколько математических книг. Гаусс и Бартельс начинают заниматься вместе; они знакомятся с биномом Ньютона, бесконечными рядами . . .

Как тесен мир! Через некоторое время Бартельс получит кафедру чистой математики в Казанском университете и будет учить математике Лобачевского.

В 1788 г. Гаусс переходит в гимназию. Впрочем, в ней не учат математике. Здесь изучают классические языки. Гаусс с удовольствием занимается языками и делает такие успехи, что даже не знает, кем он хочет стать — математиком или филологом. О Гауссе узнают при дворе. В 1791 г. его представляют Карлу Вильгельму Фердинанду — герцогу Брауншвейгскому. Мальчик бывает во дворце и развлекает придворных искусством счета. Благодаря покровительству герцога Гаусс смог в октябре 1795 г. поступить в Геттингенский университет. Первое время он слушает лекции по филологии и почти не посещает лекций по математике. Но это не означает, что он не занимается математикой. Приведем слова

Феликса Клейна, замечательного математика, глубокого исследователя научного творчества Гаусса: «Естественный интерес, какое-то, я сказал бы, детское любопытство приводит впервые мальчика независимо от каких-либо внешних влияний к математическим вопросам. Первое, что его привлекает, это чистое искусство счета. Он беспрестанно считает с прямо-таки непреоборимым упорством и неутомимым прилежанием. Благодаря этим постоянным упражнениям в действиях над числами, например, над десятичными дробями с невероятным числом знаков, он не только достигает изумительной виртуозности в технике счета, которой он отличался всю свою жизнь, но его память овладевает таким колоссальным числовым материалом, он приобретает такой богатый опыт и такую широту кругозора в области чисел, каким навряд ли обладал кто-либо до или после него. Путем наблюдений над своими числами, стало быть, индуктивным, «экспериментальным» путем он уже рано постигает общие соотношения и законы. Этот метод, стоящий в резком противоречии с современными навыками математического исследования, был, однако, довольно распространен в XVIII столетии и встречается, например, также у Эйлера ... Все эти ранние, придуманные только для собственного удовольствия забавы ума являются подходами к значительной, лишь позже осознанной цели. В том-то именно и заключается подсознательная мудрость гения, что он уже при первых пробах сил, полуиграя, еще не сознавая всего значения своих действий, попадает, так сказать, своей киркой как раз в ту породу, которая в глубине своей таит золотоносную жилу. Но вот наступает 1795 год, о котором мы имеем более точные показания ... С еще большей силой, чем до сих пор (все еще до геттингенского периода), его охватывает страстный интерес к целым числам. Незнакомый с какой бы то ни было литературой, он должен был все создавать себе сам. И здесь он вновь проявляет себя как незаурядный вычислитель, пролагающий пути в неизвестное. Гаусс составляет большие таблицы простых чисел, квадратичных вычетов и невычетов, выражает дроби $1/p$ от $p = 1$ до $p = 1000$ десятичными дробями, доводя эти вычисления до полного периода, что в иных случаях требовало несколько сотен десятичных знаков. При составлении последней таблицы Гаусс задался целью изучить зависимость периода от знаменателя p.

Кто из современных исследователей пошел бы этим странным путем, чтобы получить новую теорему! Гаусса же привел к цели именно этот путь, по которому он шел с неимоверной энергией. (Он сам утверждал, что отличается от других людей только своим прилежанием.) Осенью 1795 г. Гаусс переезжает в Геттинген и прямо-таки проглатывает впервые попавшуюся в его руки литературу: Эйлера и Лагранжа».

Открытие, которого ждали две тысячи лет. 1 июня 1796 г. в газете «Jenenser Intelligenzblatt» появилась заметка следующего содержания:

«Всякому начинающему геометру известно, что можно геометрически (т. е. циркулем и линейкой) строить разные правильные многоугольники, а именно: треугольник, пятиугольник, пятнадцатиугольник и те, которые получаются из каждого из них путем последовательного удвоения числа его сторон. Это было известно во времена Евклида, и, как кажется, с тех пор было распространено убеждение, что дальше область элементарной геометрии не распространяется: по крайней мере, я не знаю удачной попытки распространить ее в эту сторону.

Тем более кажется мне заслуживающим внимания открытие, что, кроме этих правильных многоугольников, может быть геометрически построено множество других, например семнадцатиугольник».

Под заметкой стоит подпись: К. Ф. Гаусс из Брауншвейга, студент-математик в Геттингене.

Это первое сообщение об открытии Гаусса. Прежде чем подробно рассказывать о нем, освежим в памяти то, что «известно всякому начинающему геометру».

О построениях циркулем и линейкой. Предполагается заданным отрезок единичной длины. Тогда при помощи циркуля и линейки можно строить новые отрезки, длины которых получаются из длин имеющихся отрезков при помощи операций: сложения, вычитания, умножения, деления и извлечения квадратного корня.

Последовательно проводя эти операции, при помощи циркуля и линейки можно построить любой отрезок, длина которого выражается через единицу конечным числом операций сложения, вычитания, умножения, деления и извлечения квадратного корня. Такие числа называются квадратичными иррационально-

стями. Можно доказать, что никакие другие отрезки построить при помощи циркуля и линейки нельзя.

Задача о построении правильного n-угольника, как легко понять, эквивалентна задаче о делении окружности радиуса 1 на n равных частей. Хорды дуг, на которые делится окружность, являются сторонами правильного n-угольника, и длина каждой из них равна $2\sin(\pi/n)$. Следовательно, *при тех n, для которых $\sin(\pi/n)$ является квадратичной иррациональностью, можно построить правильные n-угольники циркулем и линейкой. Этому условию удовлетворяют, например, значения* $n = 3, 4, 5, 6, 10$. Для $n = 3, 4, 6$ это хорошо известно.

Покажем, что $\sin(\pi/10)$ — квадратичная иррациональность. Рассмотрим равнобедренный треугольник ABC, угол при вершине B которого равен $\pi/5 = 36°$, длина AB равна 1; пусть AD — биссектриса угла A. Тогда $x = AC = AD = BD = 2\sin(\pi/10)$. Имеем

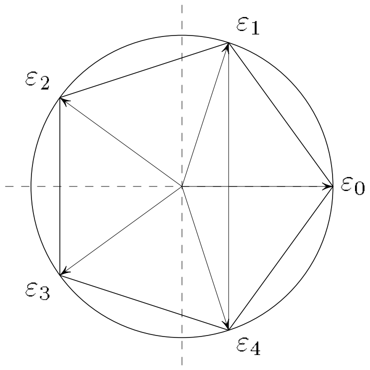
$$\frac{BD}{DC} = \frac{AB}{AC}; \qquad \frac{x}{1-x} = \frac{1}{x}, \quad x = \frac{\sqrt{5}-1}{2}.$$

Это число является квадратичной иррациональностью; тем самым мы можем построить сторону правильного 10-угольника.

Далее, из возможности деления окружности на p_1p_2 равных частей следует, конечно, возможность ее деления на p_1 равных частей (в частности, можно построить правильный пятиугольник). Обратное утверждение, вообще говоря, неверно. Укажем два частных случая, когда оно все же справедливо.

1) Из возможности деления окружности на p равных частей следует возможность деления на $2^k p$ равных частей для любого k. Это следует из возможности деления любого угла пополам при помощи циркуля и линейки.

2) Если мы умеем делить окружность на p_1 равных частей и p_2 равных частей, где p_1 и p_2 взаимно просты (например, p_1, p_2 — различные простые числа), то окружность можно разделить на p_1p_2 равных частей. Это следует из того, что наибольшая общая мера углов $2\pi/p_1$ и $2\pi/p_2$ равна $2\pi/p_1p_2$, а наибольшую общую меру двух соизмеримых углов можно найти циркулем и линейкой. В частности, $2\pi/15 = \frac{1}{2}(2\pi/3 - 2\pi/5)$, откуда следует возможность построения правильного 15-угольника.



Несколько слов о комплексных числах. Нам нужно знать про комплексные числа совсем немного: операции над ними и геометрическую интерпретацию. Напомним, что комплексному числу $z = a + ib$ ставится в соответствие точка с координатами (a, b) и вектор с концом в этой точке и с началом в $(0, 0)$. Длина вектора $z = a + ib$ называется *модулем* данного числа z. Комплексное число z можно записать в тригонометрической форме: $z = a + ib = r(\cos\varphi + i\sin\varphi)$; угол φ называется аргументом числа z.

Сложению комплексных чисел соответствует сложение векторов; при умножении модули перемножаются, а аргументы складываются. Отсюда следует, что существует ровно n корней уравнения $z^n = 1$; обычно их обозначают через

$$\varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}; \qquad k = 0, 1, \ldots, n-1. \tag{17}$$

Легко показать, что концы векторов ε_k являются вершинами правильного n-угольника. Если мы докажем, что ε_k — квадратичные иррациональности (т. е. что этим свойством обладают их вещественные и мнимые части), то тем самым мы покажем, что правильный n-угольник можно построить при помощи циркуля и линейки.

Правильные n-угольники и корни из единицы. Преобразуем уравнение $z^n = 1$:

$$z^n - 1 = (z-1)(z^{n-1} + z^{n-2} + \ldots + z + 1) = 0.$$

Получим два уравнения: $z = 1$ и

$$z^{n-1} + z^{n-2} + \ldots + z + 1 = 0. \tag{18}$$

Уравнение (18) имеет своими корнями ε_k при $1 \leqslant k \leqslant n-1$. В дальнейшем мы будем иметь дело с уравнением (18).

При $n = 3$ получаем уравнение $z^2 + z + 1 = 0$. Его корни: $\varepsilon_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\varepsilon_2 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. При $n = 5$ дело обстоит сложнее, так как мы получаем уравнение четвертой степени

$$z^4 + z^3 + z^2 + 1 = 0, \tag{19}$$

имеющее четыре корня ε_1, ε_2, ε_3, ε_4. Хотя и существует формула Феррари для решения общего уравнения 4-й степени, пользоваться ею практически невозможно. В нашем случае помогает специальный вид уравнения (19). Чтобы решить его, разделим сначала уравнение (19) на z^2. Получим

$$z^2 + \frac{1}{z^2} + z + \frac{1}{z} + 1 = 0$$

или

$$\left(z + \frac{1}{z}\right)^2 + \left(z + \frac{1}{z}\right) - 1 = 0.$$

Сделаем подстановку $w = z + \frac{1}{z}$:

$$w^2 + w - 1 = 0. \tag{20}$$

Отсюда

$$w_{1,2} = \frac{1 \pm \sqrt{5}}{2}$$

Далее можно найти и ε_k из уравнений

$$z + \frac{1}{z} = w_1, \quad z + \frac{1}{z} = w_2, \tag{21}$$

но нам это не нужно; для построения достаточно знать, что удвоенная вещественная часть ε_1 равна

$$2\cos(2\pi/5) = \varepsilon_1 + \varepsilon_4 = \varepsilon_1 + \frac{1}{\varepsilon_1} = w_1 = \frac{1 + \sqrt{5}}{2}.$$

Из того, что w_1 — квадратичная иррациональность, следует, что ε_1 и ε_4 представляют собой квадратичные иррациональности. Для ε_2 и ε_3 рассуждаем в точности так же.

Итак, для $n=5$ решение нашей задачи удалось свести к последовательному решению двух квадратных уравнений: сначала решается уравнение (20), корнями которого являются суммы $\varepsilon_1+\varepsilon_4$ и $\varepsilon_2+\varepsilon_3$ симметричных корней уравнения (19), а затем из уравнений (21) находятся и сами корни уравнения (19).

Именно таким путем Гауссу удалось осуществить построение правильного 17-угольника: здесь тоже выделяются группы корней, суммы которых находятся последовательно из квадратных уравнений. Но как искать эти «хорошие» группы? Гаусс находит удивительный путь ответить на этот вопрос...

Построение правильного 17-угольника. «30 марта 1796 года наступает для него (Гаусса) день творческого крещения... Гаусс уже занимался с некоторого времени группировкой корней из единицы на основании своей теории «первообразных» корней. И вот однажды утром, проснувшись, он внезапно ясно и отчетливо осознал, что из его теории вытекает построение семнадцатиугольника... Это событие явилось поворотным пунктом жизни Гаусса. Он принимает решение посвятить себя не филологии, а исключительно математике» (Ф. Клейн).

Остановимся подробнее на пути, по которому двигался Гаусс. Одна из математических игр юного Гаусса состояла в следующем. Он делил 1 на различные простые числа p, выписывая последовательно десятичные знаки, с нетерпением ожидая, когда они начнут повторяться. Иногда приходилось ждать долго. Для $p=97$ повторение начиналось с 97-го знака, при $p=337$ период равен 336. Но Гаусса не смущали длинные прямолинейные вычисления, он входил при их помощи в таинственный мир чисел. Гаусс не поленился рассмотреть все $p<1000$ (ср. приведенное выше высказывание Клейна).

Известно, что Гаусс не сразу попытался доказать периодичность получающейся дроби в общем случае ($p\neq 2,5$). Но, вероятно, доказательство не затруднило его. В самом деле, достаточно лишь заметить, что следить надо не за знаками частного, а за остатками! Знаки начинают повторяться после того, как на предыдущем шагу остаток равнялся 1 (почему?). Значит, надо найти такое k, что 10^k-1 делится на p. Так как имеется лишь конечное число возможных остатков (они заключены между 1 и $p-1$), для каких-то $k_1 > k_2$ числа 10^{k_1}, 10^{k_2} при делении на p дадут одинаковые остатки. Но тогда $10^{k_1-k_2} - 1$ делится на p (почему?).

Несколько труднее показать, что в качестве k всегда можно взять $p-1$, т. е. $10^{p-1} - 1$ при $p \neq 2, 5$ всегда делится на p. Это частный случай теоремы, носящий название малой теоремы Ферма. Когда Ферма (1601 – 1655) открыл ее, он писал, что его «озарило ярким светом». Теперь ее переоткрыл юный Гаусс. Он всегда будет ценить это утверждение: «Эта теорема $\langle \ldots \rangle$ заслуживает величайшего внимания как вследствие ее изящества, так и ввиду ее выдающейся пользы». Гаусса интересует наименьшее k, для которого $10^k - 1$ делится на p. Такое k всегда является делителем $p-1$. Иногда оно совпадает с $p-1$ (например, для $p = 7, 17, 19, 23, 29, 97, 337$). До сих пор неизвестно, конечно или бесконечно число таких p. Гаусс заменяет 10 на любое число a и интересуется, когда $a^{k-1} - 1$ не делится на p при $k < p-1$ (предполагается, что a не делится на p). Такие a принято называть *первообразными корнями для p*. Условие того, что a — первообразный корень, равносильно тому, что среди остатков от деления $1, a, a^2, \ldots, a^{p-2}$ на p встречаются все ненулевые остатки $1, 2, \ldots, p-1$ (почему?). Гаусс не знал тогда, что первообразными корнями интересовался уже Эйлер (1707 — 1783), который предполагал (но не смог доказать), что для каждого простого числа существует хотя бы один первообразный корень. Первое доказательство гипотезы Эйлера дал Лежандр (1752 — 1833); очень изящное доказательство дал Гаусс. Но это было позднее, а пока Гаусс манипулировал с конкретными примерами. Он знал, например, что для $p = 17$ число 3 является первообразным корнем. В приводимой ниже таблице в первой строке стоят значения k, а под ними остатки от деления 3^k на 17. Обратите внимание, что второй строке встречаются все остатки от 1 до 16, что и означает первообразность 3 для 17.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Эти вычисления и легли в основу группировки корней уравнения

$$z^{16} + z^{15} + z^{14} + \ldots + z + 1 \qquad (22)$$

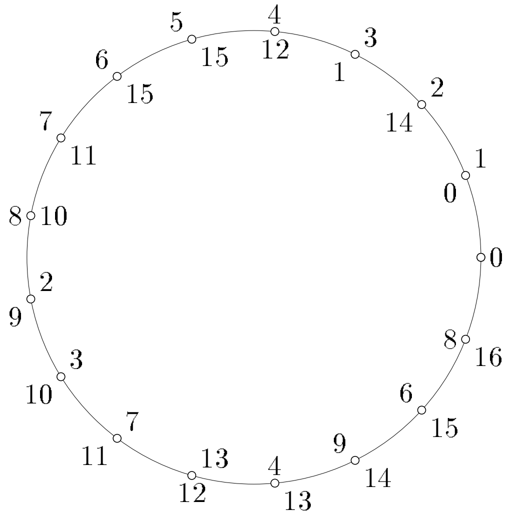


Рис. 32.

(с тем, чтобы свести решение его к цепочке квадратных уравнений). Идея Гаусса состоит в том, что надо перейти к другой нумерации корней. Присвоим корню ε_k новый номер l (обозначается $\varepsilon_{[l]}$), если 3^l при делении на 17 дает остаток k. При переходе от одной нумерации к другой можно пользоваться таблицей, находя k во второй строке, а соответствующее l над ним в первой строке, но удобнее пользоваться рисунком, где по внешней стороне окружности написаны старые номера, а по внутренней — новые. Именно эта нумерация позволила Гауссу, разбивая корни (22) на группы, свести решение (22) к цепочке квадратных уравнений.

Именно, на первом шагу берутся $\sigma_{2,0}$, $\sigma_{2,1}$ — соответственно суммы корней $\varepsilon_{[l]}$ с четными и нечетными l (в каждой сумме по 8 корней). Эти суммы оказываются корнями квадратного уравнения с целочисленными коэффициентами. Далее, берутся суммы $\sigma_{4,0}$, $\sigma_{4,1}$, $\sigma_{4,2}$, $\sigma_{4,3}$ четверок корней $\varepsilon_{[l]}$, у которых l при делении на 4 дает фиксированный остаток. Показывается, что эти величины являются корнями квадратных уравнений, у которых коэффициенты арифметически выражаются через $\sigma_{2,0}$, $\sigma_{2,1}$. Наконец, образуются суммы $\sigma_{8,i}$ пар корней $\varepsilon_{[l]}$, у которых l при делении на

8 дает остаток i. Для них выписываются квадратные уравнения с коэффициентами, просто выражающимися через $\sigma_{4,j}$. Имеем: $\sigma_{8,0} = 2\cos(2\pi/17)$ и из квадратичной иррациональности $\sigma_{8,0}$ следует возможность построения правильного 17-угольника циркулем и линейкой. Поучительно записать разбиение корней на группы в старой нумерации. Согласитесь, что в таком виде угадать разбиение невозможно! Теперь реализуем только что описанный путь.

Подробные вычисления. Мы докажем квадратичную иррациональность корней 17-й степени из единицы. Отметим, что $\varepsilon_k\varepsilon_l = \varepsilon_{k+l}$ (если $k+l > 17$, то $k+l$ заменяется остатком от его деления на 17), $\varepsilon_k = (\varepsilon_1)^k$. Прежде всего заметим, что

$$\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_{16} = \varepsilon_{[0]} + \varepsilon_{[1]} + \ldots + \varepsilon_{[15]} = -1.$$

(В этом можно убедиться, например, рассматривая это выражение как сумму геометрической прогрессии.)

Обозначим через $\sigma_{m,r}$ сумму $\varepsilon_{[k]}$ с теми k, которые дают остаток r при делении на m. Получаем

$$\sigma_{2,0} = \varepsilon_{[0]} + \varepsilon_{[2]} + \varepsilon_{[4]} + \ldots + \varepsilon_{[14]};$$
$$\sigma_{2,1} = \varepsilon_{[1]} + \varepsilon_{[3]} + \varepsilon_{[5]} + \ldots + \varepsilon_{[15]}.$$

Ясно, что

$$\sigma_{2,0} + \sigma_{2,1} = \varepsilon_{[0]} + \varepsilon_{[1]} + \ldots + \varepsilon_{[15]} = -1.$$

Можно показать, что

$$\sigma_{2,0} \cdot \sigma_{2,1} = 4(\varepsilon_{[0]} + \varepsilon_{[1]} + \ldots + \varepsilon_{[15]}).[1]$$

Теперь, воспользовавшись теоремой Виета, мы можем составить квадратное уравнение, корнями которого будут $\sigma_{2,0}$ и $\sigma_{2,1}$:

$$x^2 + x - 4 = 0, \quad x_{1,2} = \frac{-1 \pm \sqrt{17}}{2}.$$

[1]В этом можно убедиться, проводя непосредственные перемножения и учитывая, что $\varepsilon_k \cdot \varepsilon_l = \varepsilon_{k+l}$, причем удобно пользоваться рисунком на с. 320. Однако ниже будет указан способ избежать этих утомительных выкладок.

Чтобы различить корни, опять воспользуемся рисунком на с. 320. В каждую из сумм корни входят вместе со своими сопряженными. Ясно, что $\sigma_{2,0} > \sigma_{2,1}$ (в первом случае нужно сложить и удвоить вещественные части корней ε_1, ε_2, ε_4, ε_8, во втором — ε_3, ε_5, ε_6, ε_7). Итак,

$$\sigma_{2,0} = \frac{\sqrt{17}-1}{2}, \quad \sigma_{2,1} = \frac{-\sqrt{17}-1}{2}.$$

Рассмотрим суммы четверок корней:

$$\begin{aligned}\sigma_{4,0} &= \varepsilon_{[0]} + \varepsilon_{[4]} + \varepsilon_{[8]} + \varepsilon_{[12]},\\ \sigma_{4,1} &= \varepsilon_{[1]} + \varepsilon_{[5]} + \varepsilon_{[9]} + \varepsilon_{[13]},\\ \sigma_{4,2} &= \varepsilon_{[2]} + \varepsilon_{[6]} + \varepsilon_{[10]} + \varepsilon_{[14]},\\ \sigma_{4,3} &= \varepsilon_{[3]} + \varepsilon_{[7]} + \varepsilon_{[11]} + \varepsilon_{[15]}.\end{aligned}$$

Имеем: $\sigma_{4,0} + \sigma_{4,2} = \sigma_{2,0}$; $\sigma_{4,1} + \sigma_{4,3} = \sigma_{2,1}$. Можно показать далее, что $\sigma_{4,0} \cdot \sigma_{4,2} = \sigma_{2,0} + \sigma_{2,1} = -1$, а значит, $\sigma_{4,0}$, $\sigma_{4,2}$ — корни уравнения $x^2 - \sigma_{2,0}x - 1 = 0$. Решая это уравнение и учитывая, что $\sigma_{4,0} > \sigma_{4,2}$ (см. рис. на с. 320), получаем после несложных преобразований

$$\begin{aligned}\sigma_{4,0} &= \frac{1}{4}\left(\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}}\,\right),\\ \sigma_{4,2} &= \frac{1}{4}\left(\sqrt{17} - 1 - \sqrt{34 - 2\sqrt{17}}\,\right).\end{aligned}$$

Аналогично показывается, что

$$\begin{aligned}\sigma_{4,1} &= \frac{1}{4}\left(-\sqrt{17} - 1 + \sqrt{34 + 2\sqrt{17}}\,\right),\\ \sigma_{4,3} &= \frac{1}{4}\left(-\sqrt{17} - 1 - \sqrt{34 + 2\sqrt{17}}\,\right).\end{aligned}$$

Переходим к заключительному этапу. Положим

$$\begin{aligned}\sigma_{8,0} &= \varepsilon_{[0]} + \varepsilon_{[8]} = \varepsilon_1 + \varepsilon_{16},\\ \sigma_{8,4} &= \varepsilon_{[4]} + \varepsilon_{[12]} = \varepsilon_4 + \varepsilon_{13}.\end{aligned}$$

Можно было бы рассмотреть еще шесть такого рода выражений, но нам они не потребуются, так как достаточно доказать квадратичную иррациональность $\sigma_{8,0} = 2\cos(2\pi/17)$, что уже позволяет построить правильный 17-угольник. Имеем $\sigma_{8,0}+\sigma_{8,4} = \sigma_{4,0}$, $\sigma_{8,0}\cdot\sigma_{8,4} = \sigma_{4,1}$; из рисунка видно, что $\sigma_{8,0} > \sigma_{8,4}$, а потому $\sigma_{8,0}$ — бо́льший корень уравнения $x^2 - \sigma_{4,0} + \sigma_{4,1} = 0$, т. е.

$$\begin{aligned}\sigma_{8,0} = 2\cos(2\pi/17) = \frac{1}{2}\Big(\sigma_{4,0} + \sqrt{\sigma_{4,0}^2 - 4\sigma_{4,1}}\ \Big) = \\ = \frac{1}{8}\left(\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}}\ \right) + \\ + \frac{1}{4}\sqrt{17 + 3\sqrt{17} - \sqrt{170 + 38\sqrt{17}}}.\end{aligned}$$

Мы несколько преобразовали непосредственно получаемое выражение для $\sqrt{\sigma_{4,0}^2 - 4\sigma_{4,1}}$, однако не будем утомлять читателя воспроизведением этих простых выкладок.

Пользуясь полученной формулой для $\cos(2\pi/17)$, построение правильного 17-угольника можно выполнить при помощи элементарных правил построения выражений, являющихся квадратичными иррациональностями. Разумеется, получится весьма громоздкая процедура. В настоящее время известны довольно компактные способы построения. Один из них будет приведен (без доказательства) в приложении. В одном отношении формула для $\cos(2\pi/17)$ не оставляет сомнения. Прийти к ней в рамках традиционных геометрических идей времени Евклида невозможно. Решение Гаусса принадлежало другой эпохе в математике. Отметим, что наиболее содержательное утверждение — принципиальная возможность построения правильного 17-угольника. Сама процедура построения не столь существенна. Для доказательства возможности построения было достаточно убедиться, что на каждом шаге возникали квадратные уравнения с коэффициентами-квадратичными иррациональностями, не выписывая точных выражений (это становится особенно существенным при переходе к большим показателям).

В рассказанном решении уравнения (22) остался совершенно невыясненным вопрос о том, почему оказалось удачным разбиение корней, использующее нумерацию $\varepsilon_{[l]}$, как можно было догадаться положить ее в основу решения? Сейчас мы, по существу, еще раз повторим решение, обнажив ключевую идею — исследование симметрий в множестве корней.

Симметрии в множестве корней уравнения (22). Прежде всего, задача о корнях из единицы тесно связана с арифметикой остатков от деления на n (по модулю n). Действительно, если $\varepsilon^n = 1$, то ε^k — также корень n-й степени из единицы, причем число ε^k зависит только от остатка от деления k на n. Положим $\varepsilon = \varepsilon_1$ (см. формулу (17)); тогда ε_k есть просто ε в степени k, поэтому $\varepsilon_k \cdot \varepsilon_l = \varepsilon_{k+l}$, где сумма берется по модулю n (остаток от деления на n); в частности, $\varepsilon_k \cdot \varepsilon_{n-k} = \varepsilon_0 = 1$.

Задача 1. Если p — простое число и δ — любой комплексный корень p-й степени из единицы, то множество δ^k, $k = 0, 1, \ldots, p-1$, содержит все корни p-й степени из единицы.

Указание. Нужно доказать, что в этом случае для всякого $0 < m < p$ среди остатков от деления чисел km, $k = 0, 1, \ldots, p-1$ на p содержатся все числа $0, 1, \ldots, p-1$.

Обозначим через T_k следующее преобразование (возведение в степень k): $T_k\varepsilon_l = (\varepsilon_l)^k = \varepsilon_{lk}$.

Задача 2. Докажите, что если $n = p$ — простое число, то каждое из преобразований T_k $(k = 1, 2, \ldots, p-1)$ осуществляет взаимно однозначное отображение множества корней на себя (т. е. множество $\{T_k\varepsilon_0, T_k\varepsilon_1, \ldots, T_k\varepsilon_{p-1}\}$ совпадает с множеством всех корней $\{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{p-1}\}$).

Задача 1 показывает, что для всякого $1 \leqslant l \leqslant p-1$ множество $\{T_k\varepsilon_0, T_k\varepsilon_1, \ldots, T_k\varepsilon_{p-1}\}$ совпадает с множеством всех корней. Из задач 1 и 2 следует такой вывод: *составим таблицу, в которой на пересечении k-й строки и l-го столбца стоит $T_k\varepsilon_l$, $1 \leqslant k, l \leqslant p-1$; тогда в каждой строке и каждом столбце стоят все корни $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{p-1}$ в некотором порядке без повторений.* Отметим, что $T_{p-1}\varepsilon_l = \varepsilon_{-l} = (\varepsilon_l)^{-1}$. Тем, кто знает определение группы, советуем проверить, что преобразования T_k образуют группу относительно умножения $T_k \cdot T_l = T_{kl}$.

Далее мы рассматриваем случай $p = 17$. Будем говорить, что множество корней M инвариантно относительно преобразования T_k, если $T_k\varepsilon_l \in M$ для всех $\varepsilon_l \in M$. Относительно всех преобразований T_k инвариантно лишь множество всех корней $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{16}\}$.

Кардинальная догадка заключается в том, что *группа корней тем «лучше», чем большее число преобразований оставляет эту группу инвариантной.*

Введем для T_k еще одну нумерацию $T_{[l]}$, как это было сделано для ε_k: $T_{[l]} = T_k$, $k = 3^l$. В новых обозначениях $T_{[k]}\varepsilon_{[l]} = \varepsilon_{[k+l]}$, $T_{[m]}(T_{[k]}\varepsilon_{[l]}) = T_{[m+k]}\varepsilon_{[l]}$ (сумму в квадратных скобках надо брать по модулю 16).

Читатель, конечно, обнаружит аналогию с переходом к логарифмам, что не удивительно, так как $\varepsilon_{[l]} = \varepsilon_{3^l}$.

Задача 3. Доказать, что если некоторое множество корней инвариантно относительно некоторого $T_{[k]}$, где k нечетно, то это множество инвариантно относительно всех преобразований $T_{[m]}$, т. е. если оно не пусто, то совпадает с множеством всех корней.

Указание. Достаточно показать, что если k нечетно, то существует такое m, что km дает при делении на 16 остаток 1.

С другой стороны, имеются две группы корней, инвариантные относительно всех $T_{[k]}$ с четными k: корни $\varepsilon_{[l]}$ с четными l и корни с нечетными l. Их суммы мы обозначили через $\sigma_{2,0}$, $\sigma_{2,1}$.

Ясно, что $\sigma_{2,0} + \sigma_{2,1} = -1$. Исследуем $\sigma_{2,0} \cdot \sigma_{2,1}$. Это произведение является суммой попарных произведений $\varepsilon_{[k]}\varepsilon_{[l]}$, где k — четное, l — нечетное, каждое из которых является некоторым корнем $\varepsilon_{[m]}$, а всего — 64 слагаемых. Мы покажем, что среди них каждый из корней $\varepsilon_{[0]}, \varepsilon_{[1]}, \ldots, \varepsilon_{[15]}$ встречается одинаковое число раз (четыре раза), а в результате $\sigma_{2,0} \cdot \sigma_{2,1} = -4$. Воспользуемся тем, что преобразования T_k сохраняют группы корней при k четном и переводят их одна в другую при k нечетном. Каждое слагаемое в $\sigma_{2,0} \cdot \sigma_{2,1}$ однозначно представимо в виде $\varepsilon_{[m]}\varepsilon_{[m+r]}$, где $0 \leqslant m \leqslant 15$, $r = 1, 3, 5, 7$ (докажите!). Сгруппируем слагаемые с одинаковыми r. Полученные суммы будут иметь вид

$$\begin{aligned}
\varepsilon_{[0]}\varepsilon_{[r]} + \varepsilon_{[1]}\varepsilon_{[r+1]} + \varepsilon_{[2]}\varepsilon_{[r+2]} + \ldots + \varepsilon_{[15]}\varepsilon_{[r+15]} &= \\
= T_{[0]}(\varepsilon_{[0]}\varepsilon_{[r]}) + T_{[1]}(\varepsilon_{[0]}\varepsilon_{[r]}) + \ldots + T_{[15]}(\varepsilon_{[0]}\varepsilon_{[r]}) &= \\
= T_{[0]}\varepsilon_{[r]} + T_{[1]}\varepsilon_{[r]} + \ldots + T_{[15]}\varepsilon_{[r]} &= \\
= \varepsilon_{[0]} + \ldots + \varepsilon_{[15]} &= -1.
\end{aligned}$$

Мы воспользовались тем, что

$$T_{[m]}\varepsilon_{[k]} \cdot T_{[m]}\varepsilon_{[l]} = T_{[m]}(\varepsilon_{[k]}\varepsilon_{[l]})$$

и уже упоминавшимися свойствами $T_{[m]}$.

Значения $\sigma_{2,0}$, $\sigma_{2,1}$ найдены выше.

Переходим к следующему шагу. Мы хотим ввести в рассмотрение новые, меньшие группы корней, инвариантные относительно каких-нибудь $T_{[k]}$. По аналогии с задачей 3 можно показать, что при этом k обязательно должно делиться на 4. Поэтому имеются четыре группы корней, инвариантные относительно всех $T_{[4l]}$ и меньшие, чем уже рассмотренные; запишем суммы корней в каждой группе: $\sigma_{4,0}$, $\sigma_{4,1}$, $\sigma_{4,2}$, $\sigma_{4,3}$. Мы уже отмечали, что $\sigma_{4,0} + \sigma_{4,2} = \sigma_{2,0}$; $\sigma_{4,1} + \sigma_{4,3} = \sigma_{2,1}$.

Вычислим произведение $\sigma_{4,0} \cdot \sigma_{4,2}$; оно представляется в виде суммы 16 слагаемых вида $\varepsilon_{[4k]}\varepsilon_{[4l+2]}$. Каждое такое слагаемое однозначно записывается в виде $\varepsilon_{[2m]}\varepsilon_{[2m+2r]}$, $r = 1, 3$, $m = 0, 1, 2, 3, 4, 5, 6, 7$. Сгруппируем слагаемые с одним r и заметим, что $\varepsilon_{[0]}\varepsilon_{[2]} = \varepsilon_1\varepsilon_9 = \varepsilon_{10} = \varepsilon_{[3]}$, $\varepsilon_{[0]}\varepsilon_{[6]} = \varepsilon_{[1]}\varepsilon_{[15]} = \varepsilon_{[8]}$. При $r = 1$ получаем сумму

$$T_{[0]}\varepsilon_{[3]} + T_2\varepsilon_{[3]} + \ldots + T_{[14]}\varepsilon_{[3]} = \sigma_{2,1};$$

при $r = 3$ — сумму $\sum_k T_{[2k]}\varepsilon_{[8]} = \sigma_{2,0}$, т. е. $\sigma_{[4,0]} \cdot \sigma_{[4,2]} = \sigma_{2,0} + \sigma_{2,1} = -1$. Решая квадратные уравнения, мы нашли $\sigma_{[4,0]} \cdot \sigma_{[4,2]}$.

На последнем шаге мы рассмотрим группы корней, инвариантные относительно $T_{[8]}$; их восемь. В частности, $\sigma_{8,0} + \sigma_{8,4} = \sigma_{4,0}$. Вычислим $\sigma_{8,0} \cdot \sigma_{8,4}$. Учитывая, что $\varepsilon_{[0]} \cdot \varepsilon_{[4]} = \varepsilon_1\varepsilon_{13} = \varepsilon_{[14]} = \varepsilon_9$, получаем $\sigma_{8,0} \cdot \sigma_{8,4} = T_{[0]}\varepsilon_{[9]} + T_{[4]}\varepsilon_{[9]} + T_{[8]}\varepsilon_{[9]} + T_{[12]}\varepsilon_{[9]} = \sigma_{4,1}$. Это позволило найти $\sigma_{8,0} = 2\cos(2\pi/17)$ и тем самым закончить решение.

Мы видели, что рассуждение Гаусса целиком построено на использовании преобразований, переставляющих корни. Первым, кто обратил внимание на роль таких преобразований в вопросах разрешимости уравнений, был Лагранж (1736 — 1813). Вероятно, Гаусс в этот период еще не был знаком с работами Лагранжа. Позднее Галуа (1811 — 1832) положил изучение этих преобразований в основу замечательной теории, ныне носящей его имя. По существу для уравнения деления круга Гаусс построил теорию Галуа в полном объеме.

Возможные обобщения и простые числа Ферма. Если не стремиться получить явное выражение для корней, а доказывать лишь их квадратичную иррациональность, то выкладки можно почти полностью опустить, обыгрывая лишь соображения инвариантности. Именно, $\sigma_{2,0} \cdot \sigma_{2,1}$ — сумма каких-то корней $\varepsilon_{[l]}$, а поскольку эта сумма переходит в себя под действием всех преобразований $T_{[k]}$, все корни входят в нее одинаковое число раз, а значит $\sigma_{2,0} \cdot \sigma_{2,1}$ — целое число. Аналогично, $\sigma_{4,0} \cdot \sigma_{4,2}$ не меняется при всех преобразованиях вида $T_{[2k]}$, а потому является комбинацией $\sigma_{2,j}$; $\sigma_{8,0} \cdot \sigma_{8,4}$ сохраняется всеми $T_{[4k]}$, а значит, является комбинацией $\sigma_{4,j}$.

Это сокращенное рассуждение позволяет выявить, на какие простые p обобщается доказательство Гаусса квадратичной иррациональности корней p-й степени из 1. Анализ показывает, что мы пользовались лишь тем, что $p - 1 = 2^k$ (на каждом шаге группы делились пополам), и нумерацией корней, опирающейся на первообразность 3 для простого числа 17. Для нумерации можно было пользоваться любым первообразным корнем. Как мы уже отмечали, для любого простого p хотя бы один первообразный корень существует (кстати, можно показать (докажите!), что 3 является первообразным корнем для всех p вида $2^k + 1$). Заметим также, что если $p = 2^k + 1$ — простое число, то $k = 2^r$. Итак, *доказана возможность построения циркулем и линейкой правильного p-угольника для всех простых p вида* $2^{2^r} + 1$.

Простые числа вида $2^{2^r} + 1$ имеют свою историю. Эти простые числа принято называть *числами Ферма.* Ферма предполагал, что все числа такого рода являются простыми. Действительно, при $r = 0$ получаем 3, при $r = 1$ — 5, при $r = 2$ — 17. Далее при $r = 3$ получается 257, при $r = 4$ — 65 537. Оба эти числа простые. При $r = 5$ получается число 4 294 967 297. Ферма и у него не обнаружил простых делителей, но Эйлер выяснил, что Ферма «просмотрел» делитель 641. Сейчас известно, что числа Ферма являются составными при $r = 6, 7, 8, 9, 11, 12, 15, 18, 23, 36, 38, 73$ (например, при $r = 73$ имеется простой делитель $5 \cdot 2^{75} + 1$). Имеется гипотеза, что существует лишь конечное число простых чисел Ферма.

Что касается правильных n-угольников для составного n, то в силу обстоятельств, отмеченных выше (с. 315), мы сразу получаем возможность искомого построения для всех $n > 2$ вида $2^k p_1 p_2 \dots p_l$, где $p_1, p_2, \dots, p_l$ — различные простые числа Ферма. Замечательно, что других n, для которых возможно построение, вообще не существует. Доказательство этого утверждения Гаусс не опубликовал: «Хотя границы нашего сочинения не позволяют провести этого доказательства, мы думаем, что надо все же на это указать для того, чтобы кто-либо не пытался искать еще других случаев, кроме тех, которые указаны нашей теорией, например, не надеялся бы свести на геометрические построения (т. е. на построения циркулем и линейкой — С. Г.) деление окружности на $7, 11, 13, 19, \dots$ частей и не тратил бы зря своего времени». Из результата Гаусса следует принципиальная возможность построения правильного p-угольника при $p = 257$ и 65537, однако вычисление корней, не говоря уже о явном описании построения, требует колоссальной, но совершенно автоматической работы. Замечательно, что нашлись желающие ее провести не только при $p = 257$ (Ришело это сделал в сочинении из 80 страниц; есть сведения, что это построение проделал и сам Гаусс), но и при $p = 65537$ (решение, полученное Гермесом, содержится в чемодане солидных размеров в Геттингене). Вот какую шутку придумал по этому поводу английский математик Дж. Литтлвуд: «Один навязчивый аспирант довел своего руководителя до того, что тот сказал ему: «Идите и разработайте построение правильного многоугольника с 65537 сторонами». Аспирант удалился, чтобы вернуться через 20 лет с соответствующим построением».

Заключительные замечания. Мы уже отмечали, что день 30 марта 1796 г., когда было найдено построение правильного 17-угольника, определил судьбу Гаусса. Ф. Клейн пишет:

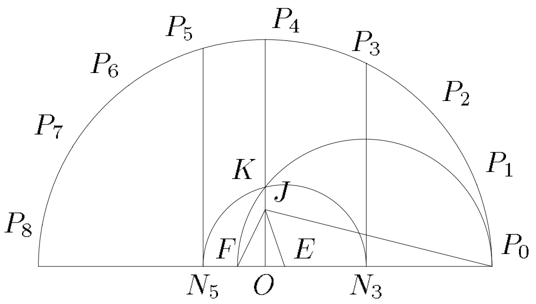
«С этой даты начинается дневник … Перед нашими глазами проходит гордый ряд великих открытий в арифметике, алгебре и анализе … И среди всех этих проявлений, мощных порывов гениального духа, можно сказать, трогательно находить до мелочей добросовестно выполненные ученические работы, от которых не освобождены и такие люди как Гаусс. Мы находим здесь записи добросовестных упражнений в дифференцировании, и непосредственно перед делением лемнискаты здесь встречаются совершенно банальные подстановки в интегралах, в которых должен упражняться любой студент».

Работа Гаусса надолго становится недосягаемым образцом математического открытия. Один из создателей неевклидовой геометрии Янош Бойяи (1802 — 1860) называл его «самым блестящим открытием нашего времени или даже всех времен». Только трудно было это открытие постигнуть! Благодаря письмам на родину великого норвежского математика Абеля (1802 — 1829), доказавшего неразрешимость в радикалах уравнения 5-й степени, мы знаем о трудном пути, который он прошел, изучая теорию Гаусса. В 1825 г. Абель пишет из Германии: «Если даже Гаусс — величайший гений, он, очевидно, не стремился, чтобы все это сразу поняли ...» Он решает не встречаться с Гауссом, но позднее пишет из Франции: «Мне в конце концов удалось приподнять завесу таинственности, окружавшую до сих пор теорию деления круга, созданную Гауссом. Теперь ход его рассуждений ясен мне, как божий день». Работа Гаусса вдохновляет Абеля на построение теории, в которой «столько замечательных теорем, что просто не верится». Он собирается в Германию, чтобы «взять Гаусса штурмом». Несомненно влияние Гаусса и на Галуа.

Сам Гаусс сохранил трогательную любовь к своему первому открытию на всю жизнь:

«Рассказывают, что Архимед завещал построить над своей могилой памятник в виде шара и цилиндра в память о том, что он нашел отношение объемов цилиндра и вписанного в него шара — 3 : 2. Подобно Архимеду Гаусс выразил желание, чтобы в памятнике на его могиле был увековечен семнадцатиугольник. Это показывает, какое значение сам Гаусс придавал своему открытию. На могильном камне Гаусса этого рисунка нет, но памятник, воздвигнутый Гауссу в Брауншвейге, стоит на семнадцатиугольном постаменте, правда, едва заметном зрителю» (Г. Вебер).

Приложение. Приведем выдержку из книги Г. Кокстера «Введение в геометрию» (М.: Наука, 1966, с. 49), содержащую рецепт Ричмонда для построения правильного 17-угольника: Соединим точку P_0 с точкой J, лежащей на радиусе OB на расстоянии $OB/4$ от центра. На диаметре, проходящем через точку P_0, выберем точки E и F так, чтобы $\angle OJE$ был равен четверти угла OJP_0, а $\angle FJE$ был равен 45°. Пусть окружность, построенная на FP_0 как на диаметре, пересекает OB в точке K и пусть окружность



с центром E и радиусом EK пересекает OP_0 в точках N_3 (между O и P_0) и N_5. Восставим перпендикуляры к OP_0 в этих двух точках до пересечения с первоначальной окружностью в точках P_3 и P_5. Тогда дуга P_3P_5 (и равная ей дуга P_1P_3) равна $\frac{2}{17}$ окружности. В доказательстве несколько раз используется тот факт, что корни уравнения $x^2 + 2x \cdot \operatorname{ctg} 2\alpha - 1 = 0$ равны $\operatorname{tg} \alpha$ и $-\operatorname{ctg} \alpha$.

2. Золотая теорема

> Я случайно натолкнулся на одну изумительную арифметическую истину, и, так как она не только показалась мне прекрасной сама по себе, но и навела на мысль, что она связана и с другими выдающимися фактами, я со всей энергией взялся за то, чтобы выяснить принципы, на которых она основывается, и получить строгое ее доказательство. После того как это желание, наконец, осуществилось, прелесть этих исследований настолько увлекла меня, что я уже не мог их оставить.
>
> *Гаусс*

30 марта 1796 г., в день когда был построен правильный 17-угольник, начинается дневник Гаусса — летопись его замечательных открытий. Следующая запись в дневнике появилась уже 8 апреля. В ней сообщалось о доказательстве теоремы, которую он назвал «золотой». Частные случаи этого утверждения доказали Ферма, Эйлер, Лагранж. Эйлер сформулировал общую гипотезу, неполное доказательство которой дал Лежандр. 8 апреля Гаусс нашел полное доказательство гипотезы Эйлера. Впрочем, Гаусс еще не знал о работах своих великих предшественников. Весь нелегкий путь к «золотой теореме» он прошел самостоятельно!

Все началось с детских наблюдений. Иногда, глядя на очень большое число, можно сразу сказать, что из него нельзя точно извлечь квадратный корень. Например, можно воспользоваться тем, что квадраты целых чисел не могут оканчиваться ни на 2, ни на 3, ни на 7, ни на 8. А иногда можно воспользоваться тем, что квадрат целого числа может либо делиться на 3, либо давать остаток 1 (но никогда 2). Оба эти свойства имеют одну природу, поскольку последняя цифра — это остаток от деления на 10. Гаусса интересует общая проблема: какими могут вообще быть остатки от деления квадратов на различные простые числа. Исследуем и мы этот вопрос.

Квадратичные вычеты. Всюду ниже мы будем предполагать, что p — простое число, причем $p \neq 2$. Делить целые числа можно «с недостатком» или «с избытком». Иными словами, остатки можно считать положительными или отрицательными. Условимся выбирать остаток наименьшим по абсолютной величине.

Нетрудно доказать, что если p нечетно, то всякое целое число a единственным образом представляется в виде

$$n = pq + r, \qquad |r| \leqslant \frac{p-1}{2}, \tag{23}$$

где q и r — целые.

Будем называть r остатком от деления n на p или вычетом числа n по модулю p. Это обозначается так:

$$n \equiv r \pmod{p}.$$

Выпишем в табл. 1 вычеты[1] для нескольких первых простых чисел $p > 2$. Нас интересует, какие вычеты (остатки) могут иметь квадраты целых чисел. Эти остатки мы будем называть квадратичными вычетами, а остальные — квадратичными невычетами.

Числа n^2 и r^2, где r — остаток числа n по модулю p, имеют один и тот же остаток при делении на p. Поэтому, если мы хотим найти квадратичные вычеты, то достаточно возводить в квадрат

[1]То, что мы называем вычетом (остатком), обычно называют абсолютно наименьшим вычетом (остатком). Мы сократили название, так как других вычетов нам не встретится. Обозначение $n \equiv r \pmod{p}$ также используется обычно в более общей ситуации: оно означает, что $n - r$ делится на p.

p	$k = \dfrac{p-1}{2}$	Вычеты (остатки) по модулю p
3	1	$-1\ 0\ 1$
5	2	$-2\ -1\ 0\ 1\ 2$
7	3	$-3\ -2\ -1\ 0\ 1\ 2\ 3$
11	5	$-5\ -4\ -3\ -2\ -1\ 0\ 1\ 2\ 3\ 4\ 5$
13	6	$-6\ -5\ -4\ -3\ -2\ -1\ 0\ 1\ 2\ 3\ 4\ 5\ 6$
17	8	$-8\ -7\ -6\ -5\ -4\ -3\ -2\ -1\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8$

Таблица 1.

p	$k = \dfrac{p-1}{2}$	Квадратичные вычеты и невычеты по модулю p
3	1	$-1\ \mathbf{0}\ \mathbf{1}$
5	2	$-2\ -\mathbf{1}\ \mathbf{0}\ \mathbf{1}\ 2$
7	3	$-\mathbf{3}\ -2\ -1\ \mathbf{0}\ \mathbf{1}\ 2\ 3$
11	5	$-5\ -4\ -3\ -\mathbf{2}\ -1\ \mathbf{0}\ \mathbf{1}\ 2\ \mathbf{3}\ \mathbf{4}\ 5$
13	6	$-6\ -5\ -\mathbf{4}\ -\mathbf{3}\ -2\ -\mathbf{1}\ \mathbf{0}\ \mathbf{1}\ 2\ \mathbf{3}\ \mathbf{4}\ 5\ 6$
17	8	$-\mathbf{8}\ -7\ -6\ -5\ -\mathbf{4}\ -3\ -\mathbf{2}\ -\mathbf{1}\ \mathbf{0}\ \mathbf{1}\ \mathbf{2}\ 3\ \mathbf{4}\ 5\ 6\ 7\ \mathbf{8}$

Таблица 2.

лишь вычеты, т. е. целые числа r, $|r| \leqslant k = (p-1)/2$. При этом, разумеется, достаточно рассматривать $r \geqslant 0$.

Проведем вычисления для простых чисел из предыдущей таблицы. Составим новую таблицу, в которой «жирные» числа отвечают квадратичным вычетам (табл. 2).

Попытаемся подметить некоторые закономерности и оценить степень их общности. Во-первых, *в каждой строке есть в точности* $k+1$ *жирное число.* Покажем, что так обстоит дело для всех простых $p > 2$. Из сказанного выше следует, что для каждого нечетного p (даже не простого) квадратичных вычетов не больше $k+1$. Мы покажем, что их точно $k+1$, если убедимся, что все числа r^2 $(0 \leqslant r \leqslant k)$ дают при делении на p различные остатки. Если $r_1 > r_2$ и при этом r_1^2 и r_2^2 дают одинаковые остатки, то $r_1^2-r_2^2$ делится на p. Поскольку p — простое число, то r_1+r_2 или r_1-r_2 должно делиться на p, чего не может быть, так как $0 < r_1+r_2 < 2k < p$. Здесь мы впервые воспользовались простотой p (покажите, что для составных чисел наше утверждение неверно).

Теорема Ферма и критерий Эйлера. Далее, очевидно, что 0 и 1 являются жирными во всех строчках. Что касается остальных столбцов, то сразу не видна закономерность, согласно которой в них появляются жирные числа. Начнем с $a=-1$. Оно является жирным при $p=5,13,17,\ldots$ и не является при $p=3,7,11\ldots$. Вы, может быть, заметили, что простые числа первой группы при делении на 4 дают остаток 1, а второй — остаток -1 (заметьте, что простые числа $p\neq 2$ других остатков вообще давать не могут) . Итак, можно предположить, что -1 является квадратичным вычетом для простых чисел вида $p=4l+1$ и квадратичным невычетом для $p=4l-1$. Эту закономерность первым заметил Ферма, однако оставил ее без доказательства. Попытайтесь найти доказательство самостоятельно! Вы убедитесь, что главная трудность в том, что не видно, как воспользоваться простотой p, а без этого предположения утверждение становится неверным.

Первое доказательство после нескольких неудачных попыток нашел в 1747 г. Эйлер. В 1755 г. Эйлер нашел другое, очень изящное доказательство, использующее «малую теорему Ферма»: *Если p — простое число, то для всякого целого a, $0<|a|<p$,*

$$a^{p-1}\equiv 1 \pmod{p}. \tag{24}$$

Доказательство. При $p=2$ утверждение очевидно, и можно считать p нечетным. Рассмотрим p чисел $0,\pm a,\pm 2a,\pm 3a,\ldots,\pm ka$; $k=(p-1)/2$. Все эти числа при делении на p дают разные остатки, так как в противном случае r_1a-r_2a, $r_1>r_2$, $|r_1|\leqslant k$, $|r_1|\leqslant k$, делится на p, но a не делится на p и r_1-r_2 не делится на p, так как $0<r_1-r_2<p$. Перемножим те из рассматриваемых чисел, которые отличны от нуля; получим $(-1)^k(k!)^2a^{p-1}$. Поскольку среди остатков сомножителей содержатся все ненулевые вычеты и учитывая правило вычисления остатка произведения, получаем, что произведение имеет тот же вычет, что и $(-1)^k(k!)^2$, т. е. $(k!)^2(a^{p-1}-1)$ делится на p. Так как $k!$ не делится на p $(0<k<p)$, то на p делится $a^{p-1}-1$, и доказательство окончено.

Следствие (критерий Эйлера квадратичности вычета). Вычет $b \neq$ $\neq 0$ является квадратичным тогда и только тогда, когда

$$b^k \equiv 1 \pmod p, \qquad k = \frac{p-1}{2}. \tag{25}$$

Доказательство. Необходимость условия (25) устанавливается легко. Если $a^2 \equiv b \pmod p$, $0 < a < p$, то $a^{2k} = a^{p-1}$ и b^k должны иметь одинаковые вычеты, равные, в силу (25), единице. Достаточность показывается сложнее. Мы выведем ее из следующей леммы.

Лемма 1. Если $P(x)$ — многочлен степени l, p — простое число и имеется более l различных вычетов r по модулю p, для которых

$$P(r) \equiv 0 \pmod p, \tag{26}$$

то (26) имеет место для всех вычетов.

Доказательство будем вести индукцией по l. При $l = 0$ утверждение очевидно. Пусть оно справедливо для многочленов степени не выше $l-1$. Пусть далее $r_0, r_1, \dots r_l$, $0 \leqslant r_j < p$, удовлетворяют сравнению $P(r) \equiv 0 \pmod p$. Представим $P(x)$ в виде $P(x) = (x - r_0)Q(x) + P(r_0)$, где $Q(x)$ — многочлен степени $l-1$, а $P(r_0)$ делится на p. Тогда, поскольку $P(r_0)$ делится на p, $(r_j - r_0)Q(r_j)$ делится на p при $1 \leqslant j \leqslant l$. Так как $r_j - r_0$ не может делиться на p, то $Q(r_j)$ делится на p, а тогда по предположению индукции $Q(r)$ будет делиться на p при всех r. Следовательно, $P(r)$ делится на p при всех r.

Применим лемму к многочлену $P(x) = x^k - 1$. Тогда соотношению (26) удовлетворяет k ненулевых квадратичных вычетов. Однако имеется вычет ($r = 0$), не удовлетворяющий (26); значит, по лемме, все квадратичные невычеты должны не удовлетворять (26) и, следовательно, условие (25) достаточно.

Замечание. Для квадратичного невычета b имеем: $b^{(p-1)/2} \equiv -1$ $\pmod p$.

Действительно, если $b^{(p-1)/2} \equiv r \pmod p$, то $r^2 \equiv 1 \pmod p$, откуда $r = -1$. (Сравнению $r^2 \equiv 1 \pmod p$ удовлетворяют только два вычета: $r \equiv 1 \pmod p$, $r \equiv -1 \pmod p$.)

Критерий Эйлера позволяет мгновенно решить вопрос о том, для каких p вычет -1 является квадратичным. Подставляя в (25)

$b=-1$, получаем, что при $p=4l+1$ соотношение (25) выполняется (k — четно), а при $p=4l-1$ — не выполняется (k — нечетно). Сформулированная выше гипотеза стала теоремой.

Задача 1. Доказать, что если $p \neq 2$ есть простой делитель числа n^2+1, то $p=4l+1$.

Итак, мы доказали, что -1 — квадратичный вычет для $p = 4l+1$ и квадратичный невычет для $p=4l-1$.

Обсудим некоторые особенности приведенного доказательства. Это утверждение состоит из двух частей: отрицательное утверждение для $p = 4l-1$ и положительное для $p = 4l+1$. В первом случае естественно пытаться найти некоторое свойство, которому квадратичные вычеты удовлетворяют, а -1 не удовлетворяет, что и сделал Эйлер. Найденное свойство оказалось характеристическим, т. е. одновременно удалось доказать и вторую часть гипотезы. Если вы пробовали доказать эту часть утверждения самостоятельно, то вы, вероятно, пытались явно построить по $p=4l+1$ число n^2, дающее при делении на p остаток -1. Доказательство Эйлера неэффективно в том смысле, что оно не дает явной конструкции для числа n по p, а лишь утверждает его существование. Иными словами, гарантируется, что если мы будем перебирать числа $1,2,\dots,2l$, возводить их в квадраты, брать остатки от деления квадратов на p, то рано или поздно мы получим -1. Остается открытым вопрос, нельзя ли указать более явную конструкцию n и p, не использующую процедуры перебора. Положительный ответ дал Лагранж (1736 — 1813) в 1773 г., используя следующую теорему.

Теорема Вильсона.[1] *Если $p=2k+1$ есть простое число, то*

$$(-1)^k(k!)^2 \equiv -1 \pmod p. \tag{27}$$

Для доказательства этой теоремы воспользуемся леммой 1. Положим $P(x) = (x^2-1)(x^2-4)\dots(x^2-k^2)$, $Q(x) = x^{2k}-1$. Тогда $R(x) = P(x) - Q(x)$ — многочлен степени не выше $2k-1$, который при $x = \pm 1, \pm 2, \dots, \pm k$ делится на p (этим свойством обладают P и Q). По лемме $R(x) \equiv 0 \pmod p$ для всех x. Собственно, новым фактом является лишь то, что $R(0) \equiv 0 \pmod p$. Поскольку $R(0) = (-1)^k(k!)^2+1$, получаем (27).

[1] Вильсон (1741 — 1793) — юрист, изучавший математику в Кембридже.

Следствие Лагранжа. *При $p = 4l + 1$ имеем:* $[(2l!)]^2 \equiv -1 \pmod{p}$.

Задача 2. Доказать, что если (27) верно, то p — простое число.

Эта задача дает повод отметить, что в конструкции Лагранжа простота p существенна.

Выяснив, когда $a = -1$ является квадратичным вычетом, Эйлер, используя огромный числовой материал, пытается найти аналогичные условия для других a. Он подмечает, что при $a = 2$ все зависит от остатка при делении p на 8; 2 оказывается квадратичным вычетом для простых $p = 8l \pm 1$ и невычетом при $p = 8l \pm 3$ (простое число $p > 2$ при делении на 8 может давать остатки $\pm 1, \pm 3$). Далее, 3 является квадратичным вычетом при $p = 12l \pm 1$ и квадратичным невычетом при $p = 12l \pm 5$. Эйлер высказывает гипотезу, что и в общем случае все определяется остатком от деления p на $4a$.

Гипотеза Эйлера.[1] *Число a одновременно является или квадратичным вычетом или квадратичным невычетом для всех простых чисел, входящих в арифметическую прогрессию $4aq + r$, $q = 0, 1, 2, \ldots$; $0 < r < 4a$.*

Ясно, что если $4a$ и r имеют общий делитель $s > 1$, то в арифметической прогрессии не будет ни одного простого числа. Если же первый член и разность прогрессии взаимно просты, то, как утверждает теорема Дирихле (1805 — 1859), в этой прогрессии имеется бесконечное число простых чисел (обобщение теоремы о бесконечности числа простых чисел в натуральном ряду).

Возвратимся к гипотезе Эйлера. Оказалось, что критерий Эйлера, который сослужил нам добрую службу при $a = -1$, отказывает уже при $a = 2$. Эйлеру не удалось разобраться в этом случае. Ему удалось доказать свою гипотезу, не считая $a = -1$, лишь при $a = 3$. Затем Лагранж, которого мы уже упоминали, доказал гипотезу при $a = 2, 5, 7$; Лежандр в 1785 г. предложил доказательство гипотезы для общего случая, которое, однако, содержало существенные пробелы.

Доказательство Гаусса. Вначале Гаусс, как и его предшественники, замечает утверждение для $a = -1$, затем, уже угадав результат для общего случая, последовательно разбирает случай

[1] Гаусс назвал ее «золотой теоремой».

за случаем, продвинувшись дальше других: им рассмотрены $a = \pm 2, \pm 3, \pm 5, \pm 7$. Общий случай (гипотеза Эйлера) не поддался первой атаке: «Эта теорема мучила меня целый год и не поддавалась напряженнейшим усилиям». Заметим, что это было то место, где Гаусс «догнал» современную математику: усилия крупнейших математиков, пытавшихся доказать гипотезу Эйлера, были безрезультатными.

Наконец, 8 апреля 1796 г. он находит общее доказательство, которое Кронекер (1823—1891) очень метко назвал «пробой сил гауссова гения». Доказательство проводится двойной индукцией по a и p; Гауссу приходится придумывать существенно различные соображения для рассмотрения восьми (!) различных случаев. Нужно было иметь не только поразительную изобретательность, но и удивительное мужество, чтобы не остановиться на этом пути. Позднее Гаусс нашел еще шесть доказательств «золотой» теоремы (ныне их известно около пятидесяти). Как это часто бывает, после того как теорема доказана, удается найти доказательства много более простые, чем первоначальное. Мы приведем здесь доказательство, мало отличающееся от третьего доказательства Гаусса. В его основе лежит ключевая лемма, доказанная Гауссом не ранее 1808 г.

Лемма 2. *Пусть $p = 2k + 1$ — простое число, a — целое число, $0 < |a| \leqslant 2k$; $r_1, r_2, \ldots, r_k$ — вычеты чисел $a, 2a, \ldots, ka$; ν — число отрицательных среди них. Тогда*

$$a^k \equiv (-1)^\nu \pmod{p}. \tag{28}$$

Применяя критерий Эйлера, получаем такое следствие:

Критерий Гаусса квадратичности вычета. *Вычет является квадратичным тогда и только тогда, когда фигурирующее в лемме 2 число ν четно.*

Доказательство леммы 2. Заметим, что все вычеты $r_1, \ldots, r_k$ различны по абсолютной величине. Это следует из того, что сумма и разность любых двух из них не делится на p: $r_i \pm r_j = (i \pm j)a$, $i \neq j$, $|i \pm j| < p$, $|a| < p$. Таким образом, набор модулей $|r_1|, \ldots, |r_k|$ — это числа $1, 2, \ldots, k$ в некотором порядке. В результате $a \cdot 2a \cdot \ldots \cdot ka = a^k k!$ при делении на p дает тот

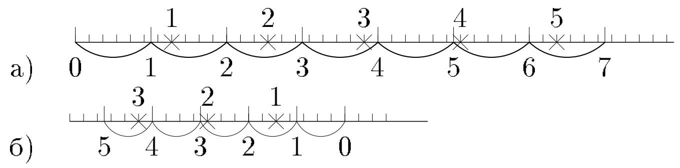


Рис. 33. а) $p = 11$ $(k = 5)$, $a = 7$, $\nu = 3$; б) $p = 7$ $(k = 3)$, $a = -5$, $\nu = 2$.

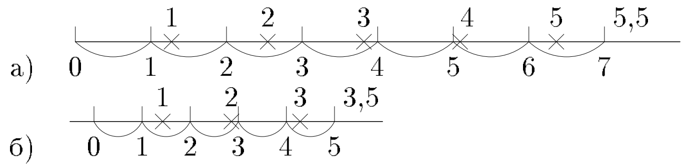


Рис. 34.

же остаток, что и $r_1 \dots r_k = (-1)^\nu k!$. Учитывая, что $k!$ не делится на простое число p, получаем (28).

Доказательство гипотезы Эйлера. Заметим, что в приводимом рассуждении уже не используется простота p — она в полной мере использована в лемме Гаусса. Отметим на числовой оси точки $mp/2$, если $a > 0$, и $-mp/2$, если $a < 0$ (рис. 33а, б). Занумеруем интервалы с концами в этих точках по номерам левых концов. Отметим теперь крестиками точки $a, 2a, \dots, ka$; так как a — целое, не делящееся на p, то крестики не могут совпасть с ранее отмеченными точками, причем все крестики попадут в какие-то из построенных интервалов ($|a|p/2 > |a|k$). Легко заметить, что фигурирующее в лемме *число ν — это число крестиков, попавших в интервалы с нечетными номерами* (докажите!).

Подвергнем теперь нашу картинку преобразованию подобия с коэффициентом $1/a$ (рис. 33 перейдет в рис. 34). При этом точки $mp/2$ перейдут в точки, делящие отрезок $[0, p/2]$ на $|a|$ равных частей, а крестики — в целочисленные точки $1, 2, \dots, k$.

Нумерация интервалов теперь будет зависеть от знака a: при $a > 0$ они нумеруются номерами левых концов, при $a < 0$ — номерами правых концов; ν — число целочисленных точек в интервалах с нечетными номерами. Если мы увеличим p на $4al$, то в каждый интервал добавится точно $2l$ целых точек. Это следует из того, что при сдвиге интервала на целое число количество

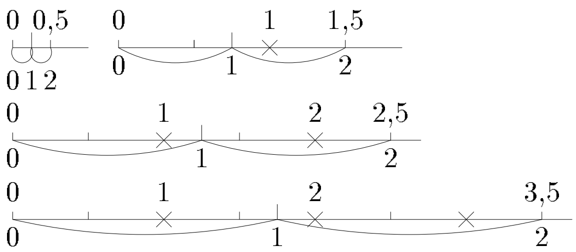


Рис. 35. $r = 1$, $a = 2$, $\nu = 0$; $r = 3$, $a = 3$, $\nu = 1$; $r = 5$, $a = 2$, $\nu = 1$; $r = 7$, $a = 2$, $\nu = 2$.

целых точек в нем не меняется, а на любом отрезке целочисленной длины n или интервале длины n с нецелочисленными концами имеется ровно n целых точек (докажите!). Итак, при замене p на $p+4al$ величина ν изменится на четное число, а $(-1)^\nu$ не изменится. Значит, для всех p в арифметической прогрессии $p = 4aq + r$ значение $(-1)^\nu$ одно и то же, и гипотеза Эйлера доказана.

Одновременно указан некоторый способ выяснить, является ли a квадратичным вычетом для p. Нужно взять остаток r от деления p на $4a$ (для удобства положительный); разделить $(0, r/2)$ на $|a|$ частей, занумеровав их номерами левых (правых) концов, если a положительно (отрицательно); сосчитать число ν целых точек, попавших в интервалы с нечетный номерами; a — квадратичный вычет в том и только в том случае, когда ν четно.

Проделаем эти вычисления для $a = 2$, чтобы подтвердить наблюдения Эйлера, о которых говорилось на с. 336. Пусть $a = 2$; тогда достаточно рассмотреть $r = 1, 3, 5, 7$, поскольку в остальных случаях арифметическая прогрессия не будет содержать простых чисел. Как видно из рис. 35, число 2 является квадратичным вычетом для $p = 8q + 1$, $p = 8q + 7$, т. е. $p = 8q \pm 1$.

Упражнение. Покажите, что -2 есть квадратичный вычет для $p = 8q + 1$, $p = 8q + 3$.

Аналогично рассматривается случай $a = \pm 3$. Приведем итоги вычислений (таблица для ν):

	$r = 1$	$r = 3$	$r = 5$	$r = 7$
$a = 3$	0	1	1	2
$a = -3$	0	1	2	3

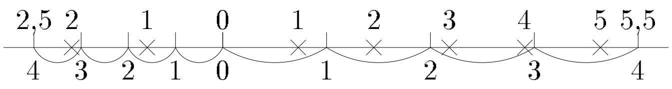


Рис. 36. $p = 11$, $q = 5$, $a = (p+q)/4$, $\nu(p) = 2$, $\nu(q) = 2$.

Таким образом, 3 — квадратичный вычет при $p = 12l \pm 1$ (невычет при $p = 12l \pm 5$), а (-3) — квадратичный вычет для $p = 12l + 1$, $p = 12l + 5$.

Для случая $a = 2, 3$ вы, конечно, заметили еще одну закономерность: простые числа, имеющие при делении на $4a$ остатки, равные по абсолютной величине, одновременно являются либо квадратичными вычетами, либо квадратичными невычетами. Это обстоятельство, разумеется, не осталось незамеченным для Эйлера, и он сформулировал гипотезу в более сильной форме, чем мы ее привели.

Сформулируем теперь

Дополнение к гипотезе Эйлера. Пусть p и q — простые числа и $p + q = 4a$. Тогда a или является квадратичным вычетом и по модулю p, и по модулю q, или квадратичным невычетом и по модулю p, и по модулю q.

Доказательство. Выполним построения, указанные при доказательстве гипотезы Эйлера, для интервалов $(0, p/2)$, $(0, q/2)$, $a = (p+q)/4$. Для удобства расположим интервалы так, чтобы они имели точку 0 общей, находясь по разные стороны от нее; при этом интервал $(0, q/2)$ мы перевернем (рис. 36). Пусть $\nu(p), \nu(q)$ — число целых точек в интервалах с нечетными номерами для p и q соответственно. Нам достаточно доказать, что $\nu(p) + \nu(q)$ четно. Пусть $\nu_j(p)$, $\nu_j(q)$ — число целых точек в соответствующих интервалах с номерами j. Легко видеть, что $\nu_j(p) + \nu_j(q) = 2$ при $j > 0$, откуда и будет следовать нужный результат.

Действительно, на интервале между j-ми левой и правой точками ($j > 0$) лежит $2j$ целых точек, поскольку, как мы уже отмечали, на интервале длины $2j$ с нецелочисленными концами лежит $2j$ целых точек.

Квадратичный закон взаимности. В 1798 г. Лежандр указал очень удобное утверждение, эквивалентное гипотезе, — квадратичный закон взаимности. Введем обозначение — так называемый символ Лежандра:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{если } a \text{ — квадратичный вычет по модулю } p, \\ -1, & \text{если } a \text{ — квадратичный невычет.} \end{cases}$$

В силу критерия Эйлера (и замечания к нему, с. 334)

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}. \tag{29}$$

Отсюда сразу следует мультипликативное свойство символа Лежандра:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \tag{30}$$

Отметим также, что символ Лежандра можно доопределить для всех a, не делящихся на p, с сохранением (29), (30), полагая

$$\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right). \tag{31}$$

Теперь мы можем сформулировать квадратичный закон взаимности:

Если p, q — нечетные простые числа, то

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \tag{32}$$

Другими словами, $\left(\frac{p}{q}\right)$ и $\left(\frac{q}{p}\right)$ имеют противоположные знаки, если $p = 4l + 3$, $q = 4m + 3$, и совпадают в остальных случаях.

Название закона связано с тем, что в нем устанавливается «взаимность» между вопросами о том, когда p — квадратичный вычет по модулю q и когда q — квадратичный вычет по модулю p.

Доказательство. Всегда или $p - q = 4a$, или $p + q = 4a$.

Случай 1. Пусть $p - q = 4a$, т. е. p и q имеют одинаковые остатки при делении на 4. Тогда $\left(\frac{p}{q}\right) = \left(\frac{q+4a}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right)$

(мы воспользовались (31), (30) и тем, что $\left(\dfrac{4}{q}\right) = 1$ при всех q). Далее, $\left(\dfrac{q}{p}\right) = \left(\dfrac{p-4a}{p}\right) = \left(\dfrac{-4a}{p}\right) = \left(\dfrac{-1}{p}\right)\left(\dfrac{a}{p}\right)$. В силу уже доказанной гипотезы Эйлера $\left(\dfrac{a}{p}\right) = \left(\dfrac{a}{q}\right)$, т. е. $\left(\dfrac{p}{q}\right) = \left(\dfrac{q}{p}\right)$ при $\left(\dfrac{-1}{p}\right) = 1$ и $\left(\dfrac{p}{q}\right) = -\left(\dfrac{q}{p}\right)$ при $\left(\dfrac{-1}{p}\right) = -1$. Остается вспомнить, что $\left(\dfrac{-1}{p}\right) = 1$ при $p = 4l+1$, $\left(\dfrac{-1}{p}\right) = -1$ при $p = 4l+3$.

Случай 2. Пусть $p + q = 4a$, т. е. p и q имеют разные остатки при делении на 4. Имеем $\left(\dfrac{p}{q}\right) = \left(\dfrac{4a-q}{q}\right) = \left(\dfrac{a}{q}\right)$. Аналогично, $\left(\dfrac{q}{p}\right) = \left(\dfrac{a}{p}\right)$. В силу дополнения к гипотезе Эйлера $\left(\dfrac{a}{p}\right) = \left(\dfrac{a}{q}\right)$, т. е. $\left(\dfrac{p}{q}\right) = \left(\dfrac{q}{p}\right)$. Доказательство окончено. Нетрудно заметить, что проведенные рассуждения можно обратить и вывести из квадратичного закона взаимности гипотезу Эйлера и дополнение к ней (проделайте это!). Отметим еще, что формулы (30) – (32) дают способ вычисления $\left(\dfrac{p}{q}\right)$ существенно более простой, чем описанный выше комбинаторный способ. Проиллюстрируем это на примере:

$$\left(\frac{59}{269}\right) = \left(\frac{269}{59}\right) = \left(\frac{59\cdot 4+33}{59}\right) = \left(\frac{3}{59}\right)\cdot\left(\frac{11}{59}\right) = -1,$$

так как $\left(\dfrac{3}{59}\right) = -\left(\dfrac{59}{3}\right) = -\left(\dfrac{2}{3}\right) = 1$; $\left(\dfrac{11}{59}\right) = -\left(\dfrac{59}{11}\right) = -\left(\dfrac{4}{11}\right) = -1$. Легко показать, что вычисление символа Лежандра всегда можно свести к случаю, когда p или q равно 2.

Упражнение. Сосчитайте $\left(\dfrac{37}{557}\right)$, $\left(\dfrac{43}{991}\right)$.

В заключение отметим, что задача о квадратичных вычетах послужила отправной точкой большой и плодотворной математической деятельности. Многочисленные попытки Гаусса получить новые доказательства квадратичного закона взаимности далеко не в первую очередь диктовались желанием упростить доказательства. Гаусса не оставляла мысль, что им по-настоящему не вскрыты глубокие закономерности, следствием которых является закон взаимности. В полной мере это удалось сделать лишь позднее, в рамках теории алгебраических чисел. Гаусс потратил много сил на обобщение квадратичного закона на кубический и биквадратный случаи, получив замечательные результаты. Эти исследования были продолжены, и изучение различных законов взаимности остается одним из центральных вопросов теории чисел по сей день.

3. Королевские будни

Мы подробно рассказали о двух первых великих открытиях Гаусса, сделанных им в Геттингене, на протяжении 10 дней, за месяц до того, как ему исполнилось 19 лет. Второе из этих открытий целиком относилось к арифметике (теории чисел), а первое в существенном опиралось на арифметические рассмотрения. Теория чисел — первая любовь Гаусса.

Любимейшая наука величайших математиков. Это один из многочисленных эпитетов, которыми Гаусс наделял арифметику (теорию чисел). К тому времени арифметика из набора изолированных наблюдений и утверждений уже превратилась в науку.

Позднее Гаусс напишет: «Главным образом, более поздним исследователям, правда немногочисленным, но завоевавшим непреходящую славу, — таким, как Ферма, Эйлер, Лагранж, Лежандр, мы обязаны тем, что они нашли доступ к сокровищнице этой божественной науки и показали, какими богатствами она наполнена».

Одна из самых удивительных сторон «феномена Гаусса» заключается в том, что он в своих первых работах практически не опирался на достижения предшественников, переоткрыв за короткий срок то, что было сделано в теории чисел за полтора века трудами крупнейших математиков.

Гаусс использует пребывание в Геттингене для изучения трудов классиков, он переосмысливает их достижения, сопоставляет с тем, что он открыл сам. По его замыслу результаты этой деятельности должны были быть подытожены во всеобъемлющем труде. К написанию этой книги Гаусс приступает после возвращения в Брауншвейг в 1798 г. после окончания университета. В книгу должны были войти собственные результаты, все еще остававшиеся неопубликованными, если не считать газетной заметки, в которой кстати обещалось: «Это открытие является собственно лишь следствием одной еще не совсем законченной большой теории. Как только она получит эту законченность, она будет предложена публике». На осуществление грандиозного замысла ушло четыре года напряженной работы.

В 1801 г. вышли знаменитые «Арифметические исследования» Гаусса. Эта огромная книга (более 500 страниц крупного формата) содержит основные результаты Гаусса: квадратичный закон взаимности, задачу деления круга, вопрос о представимости целых чисел в виде $am^2 + bmn + cn^2$ (в частности, в виде суммы квадратов). Книга была издана на средства герцога и ему посвящена. В изданном виде книга состояла из семи частей. На восьмую часть денег не хватило. В этой части речь должна была идти об обобщении закона взаимности на степени выше второй, в частности — о биквадратичном законе взаимности. Полное доказательство биквадратичного закона Гаусс нашел лишь 23 октября 1813 г., причем в дневниках он отметил, что это совпало с рождением сына.

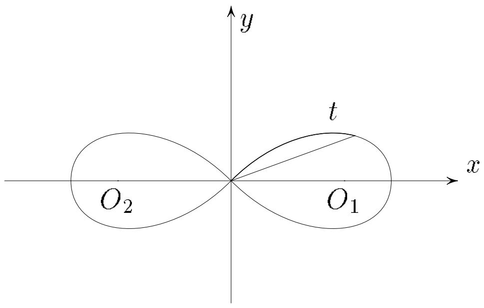
Клейн писал: «В своих „Арифметических исследованиях“ Гаусс в полном смысле этого слова создал современную теорию чисел и предопределил все ее дальнейшее развитие до нынешнего дня. Восхищение этим трудом возрастает еще больше, когда наблюдаешь, как Гаусс без всякого внешнего побуждения с самого начала черпает этот мир из самого себя».

За пределами «Арифметических исследований» Гаусс, по существу, теорией чисел больше не занимался. Он лишь продумывал и доделывал то, что было задумано в те годы. Например, он придумал еще шесть разных доказательств квадратичного закона взаимности. «Арифметические исследования» сильно опередили свое время. В процессе их создания Гаусс не имел серьезных математических контактов, а вышедшая книга долго не была доступна никому из немецких математиков. Во Франции, где можно было рассчитывать на интерес Лагранжа, Лежандра и др., книге не повезло: обанкротился книготорговец, который должен был распространять книгу, и большая часть тиража пропала. В результате ученикам Гаусса приходилось позднее переписывать отрывки из книги от руки. Положение в Германии стало меняться лишь в 40-х годах, когда Дирихле основательно изучил «Исследования» и читал по ним лекции. А в Казань — к Бартельсу и его ученикам — книга попала в 1807 г.

«Арифметические исследования» оказали огромное влияние на дальнейшее развитие теории чисел и алгебры. Отталкиваясь от работы Гаусса о делении круга, Галуа пришел к решению вопроса о разрешимости уравнений в радикалах. Законы взаимности до сих пор занимают одно из центральных мест в алгебраической теории чисел.

Гельмштадтская диссертация. В Брауншвейге Гаусс не имел литературы, необходимой для работы над «Арифметическими исследованиями». Поэтому он часто ездил в соседний Гельмштадт, где была хорошая библиотека. Здесь в 1798 г. Гаусс подготовил диссертацию, посвященную доказательству «основной теоремы алгебры» — утверждения о том, что всякий многочлен с комплексными (в частности, с действительными) коэффициентами имеет комплексный корень (если хотеть оставаться в области действительных чисел, то основную теорему алгебры можно сформулировать так: всякий многочлен с действительными коэффициентами раскладывается в произведение многочленов первой и второй степени). Гаусс критически разбирает все предшествующие попытки доказательства и с большой тщательностью проводит идею Даламбера. Безупречного доказательства все же не получилось, так как не хватало строгой теории непрерывности. В дальнейшем Гаусс придумал еще три доказательства основной теоремы (последний раз — в 1848 г.).

Лемниската и арифметико-геометрическое среднее. Расскажем еще об одной линии в работах Гаусса, начавшейся в детстве. В 1791 г., когда Гауссу было 14 лет, его занимала следующая игра. Он брал два числа a_0, b_0 и строил для них среднее арифметическое $a_1 = (a_0 + b_0)/2$ и среднее геометрическое $b_1 = \sqrt{a_0 b_0}$. Затем он вычислял средние от a_1, b_1: $a_2 = (a_1 + b_1)/2$, $b_2 = \sqrt{a_1 b_1}$, и т. д. Гаусс вычислял обе последовательности с большим числом знаков. Очень скоро он уже не мог различить a_n и b_n —



все вычисленные знаки совпадали. Другими словами, обе последовательности быстро стремились к общему пределу $M(a,b)$ (называемому *арифметико-геометрическим средним*).

В те же годы Гаусс много возился с кривой, называемой *лемнискатой* (или лемнискатой Бернулли), — множеством точек, произведение расстояний каждой из которых до двух фиксированных точек O_1, O_2 (фокусов) постоянно и равно $(O_1O_2/2)^2$. К систематическому изучению лемнискаты Гаусс перешел в 1797 г. Он долго пытается найти длину лемнискаты, пока не догадывается, что она равна $\frac{2\pi}{M(\sqrt{2},2)}O_1O_2$. Мы не знаем, как Гаусс сообразил это, но знаем, что было это 30 мая 1799 г. и что, не имея вначале доказательства, он сосчитал обе величины с одиннадцатью (!) десятичными знаками. Гаусс придумал для лемнискаты функции, аналогичные тригонометрическим функциям для окружности. Например, для лемнискаты, расстояние между фокусами которой равно $\sqrt{2}$, лемнискатный синус $\operatorname{sl} t$ — это просто длина хорды, соответствующей дуге длины t. Последние годы XVIII столетия у Гаусса уходят на построение теории лемнискатных функций. Для них были получены теоремы сложения и приведения, аналогичные теоремам для тригонометрических функций.

От лемнискатных функций Гаусс переходит к их обобщению — эллиптическим функциям. Он понимает, что речь идет «о совершенно новой области анализа». После 1800 г. Гаусс уже не смог уделять эллиптическим функциям столько времени, сколько было необходимо для доведения теории до состояния, удовлетворяющего его своей полнотой и строгостью. С самого начала он отказался от регулярных публикаций, надеясь опубликовать все разом, как это было с его арифметическими работами. Однако заботы так никогда и не доставили ему необходимого времени.

В 1808 г. он пишет своему другу и ученику Шумахеру: «С круговыми и логарифмическими функциями мы умеем теперь обходиться как единожды один, но великолепный золотой родник, хранящий сокровенное высших функций, остается пока почти terra incognita[1]. Я очень много работал над этим прежде и со временем дам собственный большой труд об этом, на что я намекал еще в моих „Арифметических исследованиях“. Приходишь в изумление от чрезвычайного богатства новых и в высшей степени интересных истин и соотношений, доставляемых этими функциями».

Гаусс считал, что может не торопиться с публикацией своих результатов. Тридцать лет так и было. Но в 1827 г. сразу два молодых математика — Абель и Якоби — опубликовали многое из того, что было им получено.

«Результаты Якоби представляют часть моей собственной большой работы, которую я собираюсь когда-нибудь издать. Она будет представлять исчерпывающий труд на эту тему, если только небесам будет угодно продлить мою жизнь и даровать мне силы и душевный покой» (письмо Шумахеру).

«Господин Абель предвосхитил многие мои мысли и примерно на треть облегчил мою задачу, изложив результаты с большой строгостью и изяществом. Абель шел тем же путем, что и я в 1798 г., поэтому нет ничего невероятного в том, что мы получили столь похожие результаты. К моему удивлению, это сходство распространяется даже на форму, а местами и на обозначения, поэтому многие его формулы кажутся списанными с моих. Но чтобы никто не понял меня неправильно, я должен добавить, что не помню ни одного случая, когда я говорил об этих исследованиях с кем-нибудь из посторонних» (письмо Бесселю).

Наконец, в письме Креллю: «Поскольку Абель продемонстрировал такую проницательность и такое изящество в вопросах изложения, я чувствую, что могу совершенно отказаться от опубликования полученных мной результатов» (май 1828 г.).

[1]Неизведанная область (лат.).

Следует отметить, что замечание Гаусса в «Арифметических исследованиях» о том, что теорию деления круга можно перенести на лемнискату, оказало большое влияние на Абеля.

С наступлением нового века научные интересы Гаусса решительно сместились в сторону от чистой математики. Он много раз эпизодически будет обращаться к ней и каждый раз получать результаты, достойные гения. В 1812 г. он опубликовал работу о гипергеометрической функции. (Эта функция зависит от трех параметров. Придавая им конкретные значения, можно получить большинство функций, встречающихся в математической физике.) Широко известна заслуга Гаусса в геометрической интерпретации комплексных чисел. О его геометрических работах мы расскажем ниже. Однако никогда математика уже не будет главным делом его жизни. Характерный внешний штрих: в 1801 г. Гаусс прекращает регулярно вести дневник (хотя отдельные записи появляются до 1814 г.). Мы редко отдаем себе отчет, как короток был «математический век» Гаусса — менее 10 лет. При этом бо́льшую часть времени заняли работы, оставшиеся неизвестными современникам (эллиптические функции).

Малые планеты. Расскажем теперь о новом увлечении Гаусса. Биографы много спорили о причинах, по которым Гаусс начал заниматься астрономией. Прежде всего надо иметь в виду, что, начиная с работ Кеплера, Галилея и Ньютона, астрономия была наиболее ярким местом приложения математики. Эта традиция была продолжена в трудах Эйлера, Даламбера, Клеро, Лагранжа, Лапласа. Предсказывая и объясняя небесные явления, математики чувствовали себя как бы допущенными к тайнам мироздания. Гаусс, с его ранним интересом к конкретным вычислениям, не мог, конечно, не попробовать своих сил на этом традиционном поприще.

Впрочем, были причины и прозаические. Гаусс занимал скромное положение приват-доцента в Брауншвейге, получая 6 талеров в месяц. Пенсия в 400 талеров от герцога-покровителя не настолько улучшила его положение, чтобы он мог содержать семью, а он подумывал о женитьбе. Получить где-нибудь кафедру по математике было непросто, да Гаусс и не очень стремился к активной преподавательской деятельности. Расширяющаяся сеть обсерваторий делала карьеру астронома более доступной.

Гаусс начал интересоваться астрономией еще в Геттингене. Кое-какие наблюдения он проводил в Брауншвейге, причем часть герцогской пенсии он израсходовал на покупку секстанта. Он ищет достойную вычислительную задачу, решая пока мелкие задачи. Так, он публикует простой способ вычисления времени пасхи и других циклических праздников вместо чрезвычайно путаных рецептов, которыми пользовались раньше. Мысль о настоящей задаче появилась в 1801 г. при следующих обстоятельствах.

1 января 1801 г. астроном Пиацци, составлявший звездный каталог, обнаружил неизвестную звезду 8-й звездной величины. Пронаблюдав за ней 40 дней, Пиацци обратился к крупнейшим астрономам с просьбой продолжить наблюдения. По разным причинам его просьба не была выполнена. В июне эти сведения дошли до Цаха, издававшего единственный в то время астрономический журнал. Цах высказал гипотезу, что речь идет «о давно подозреваемой между Марсом и Юпитером, а теперь, по-видимому, открытой, новой большой планете». Гипотеза Цаха показалась правдоподобной, и надо было срочно искать «потерянную» планету. А для этого надо было вычислить ее траекторию. Определить эллиптическую траекторию по дуге в 9°, которую знал Пиацци, было за пределами вычислительных возможностей астрономов. В сентябре 1801 г., оставив все свои дела, вычислением орбиты занялся Гаусс. В ноябре вычисления были закончены. В декабрьском номере журнала Цаха они были опубликованы, а в ночь с 31 декабря на 1 января — ровно через год после наблюдений Пиацци — известный немецкий астроном Ольберс, основываясь на траектории, вычисленной Гауссом, нашел планету (ее назвали Церерой). Это была подлинная сенсация!

25 марта 1802 г. Ольберс открывает еще одну планету — Палладу. Гаусс быстро вычисляет ее орбиту, показав, что и она располагается между Марсом и Юпитером. Действенность вычислительных методов Гаусса стала для астрономов несомненной.

К Гауссу приходит признание. Одним из признаков этого было избрание его членом-корреспондентом Петербургской академии наук. Вскоре его пригласили занять место директора Петербургской обсерватории. Гаусс пишет, что ему лестно получить приглашение в город, где работал Эйлер, и серьезно думает о переезде. В письмах Гаусс пишет, что в Петербурге часто плохая погода, а потому он не будет слишком занят наблюдениями, и будет оставаться время для занятий. Он пишет, что 1000 рублей, которые будет получать, больше 400 талеров, которые он имеет сейчас, но жизнь в Петербурге дороже.

В то же время Ольберс предпринимает усилия, чтобы сохранить Гаусса для Германии. Еще в 1802 г. он предлагает куратору Геттингенского университета пригласить Гаусса на пост директора вновь организованной обсерватории. Ольберс пишет при этом, что Гаусс «к кафедре математики имеет положительное отвращение». Согласие было дано, но переезд состоялся лишь в конце 1807 г. За это время Гаусс женился («жизнь представляется мне весной со всегда новыми яркими цветами»). В 1806 г. умирает от ран герцог, к которому Гаусс, по-видимому, был искренне привязан. Теперь ничто не удерживает его в Брауншвейге.

Жизнь Гаусса в Геттингене складывалась несладко. В 1809 г. после рождения сына умерла жена, а затем и сам ребенок. Вдобавок Наполеон обложил Геттинген тяжелой контрибуцией. Сам Гаусс должен был заплатить непосильный налог в 2000 франков. За него попытались внести деньги Ольберс и, прямо в Париже, Лаплас. Оба раза Гаусс гордо отказался. Однако нашелся еще один благодетель, на этот раз — аноним, и деньги возвращать было некому (много позднее узнали, что это был курфюрст Майнцский, друг Гете). «Смерть мне милее такой жизни», — пишет Гаусс между заметками по теории эллиптических функций. Окружающие не ценили его работ, считали его, по меньшей мере, чудаком. Ольберс успокаивает Гаусса, говоря, что не следует рассчитывать на понимание людей: «их нужно жалеть и им служить».

В 1809 г. выходит законченная в 1807 г. знаменитая «Теория движения небесных тел, обращающихся вокруг Солнца по коническим сечениям». Задержка произошла отчасти из-за опасений издателя, что книга на немецком языке не найдет спроса, а Гаусс из патриотических соображений отказался печатать книгу по-французски. Компромисс состоял в издании книги на латыни. Это единственная книга Гаусса по астрономии (сверх этого он напечатал несколько статей). Гаусс излагает свои методы вычисления орбит. Чтобы убедиться в силе своего метода, он повторяет вычисление орбиты кометы 1769 г., которую в свое время за три дня напряженного счета вычислил Эйлер (по некоторым сведениям, потерявший после этого зрение). Гауссу на это потребовался час. В книге был изложен метод наименьших квадратов, остающийся по сей день одним из самых распространенных методов обработки результатов наблюдений. Гаусс указывает, что он знает этот метод с 1794 г., а с 1802 г. систематически им пользуется. (За два года до выхода «Теории движения» Гаусса метод наименьших квадратов был опубликован Лежандром.)

На 1810 г. пришлось большое число почестей: Гаусс получил премию Парижской академии наук и Золотую медаль Лондонского королевского общества, был избран в несколько академий.

В 1804 г. Парижская академия выбрала в качестве темы для большой премии (золотая медаль весом 1 *кг*) теорию возмущений Паллады. Срок дважды переносился (до 1816 г.) в надежде, что Гаусс представит работу. Гауссу помогал в вычислениях его ученик Николаи («юноша, неутомимый в вычислениях»), и все же вычисления не были доведены до конца. Гаусс прервал их, находясь в тяжелой депрессии.

Регулярные занятия астрономией продолжались почти до самой смерти. Знаменитую комету 1812 г. (которая «предвещала» пожар Москвы!) всюду наблюдали, пользуясь вычислениями Гаусса. 28 августа 1851 г. Гаусс наблюдал солнечное затмение. У Гаусса было много учеников-астрономов (Шумахер, Герлинг, Николаи, Струве). Крупнейшие немецкие геометры Мёбиус и Штаудт учились у него не геометрии, а астрономии. Он состоял в активной переписке со многими астрономами, регулярно читал статьи и книги по астрономии, печатал рецензии. Из писем астрономам мы многое узнаем и о занятиях математикой. Как не похож облик Гаусса-астронома на представление о недоступном отшельнике, существовавшее у математиков!

Геодезия. К 1820 г. центр практических интересов Гаусса переместился в геодезию. Еще в начале века он пытался воспользоваться результатами измерений дуги меридиана, предпринятых французскими геодезистами для установления эталона длины (метра), чтобы найти истинное сжатие Земли. Но дуга оказалась слишком мала. Гаусс мечтал провести измерение достаточно большой дуги меридиана. К этой работе он смог приступить только в 1820 г. Хотя измерения растянулись на два десятилетия, Гаусс не смог осуществить свой замысел в полном объеме. Большое значение имели полученные в связи с геодезией исследования по обработке результатов измерений (к этому времени относятся основные публикации о методе наименьших квадратов) и различные геометрические результаты, связанные с необходимостью проводить измерения на поверхности эллипсоида.

В 20-е годы обсуждался вопрос о переезде Гаусса в Берлин, где он должен был стать во главе института. Сюда должны были быть приглашены наиболее перспективные молодые математики, прежде всего Якоби и Абель. Переговоры затянулись на четыре года; разногласия были по поводу того, должен ли Гаусс читать лекции, и сколько ему должны платить в год — 1200 или 2000 талеров. Переговоры окончились безрезультатно, Впрочем, не совсем: в Геттингене Гауссу стали платить то жалование, на которое он претендовал в Берлине.

Внутренняя геометрия поверхностей. Геодезии мы обязаны тем, что на сравнительно короткое время математика вновь стала одним из главных дел Гаусса. В 1816 г. он думает об обобщении основной задачи картографии — задачи об отображении одной поверхности на другую «так, чтобы отображение было подобно отображаемому в мельчайших деталях». Гаусс посоветовал Шумахеру выбрать этот вопрос при объявлении конкурса на премию Копенгагенского научного общества. Конкурс был объявлен в 1822 г. В том же году Гаусс представил свой мемуар, в котором вводятся характеристики, позволяющие полностью решить проблему, частные случаи которой изучались Эйлером и Лагранжем (отображение сферы или поверхности вращения на плоскость). Гаусс подробно описывает выводы из его теории для многочисленных конкретных случаев, часть из которых возникает из задач геодезии.

В 1828 г. вышел в свет основной геометрический мемуар Гаусса «Общие исследования о кривых поверхностях». Мемуар посвящен внутренней геометрии поверхности, т. е. тому, что связано со структурой самой этой поверхности, а не с ее положением в пространстве.

Образно говоря, внутренняя геометрия поверхности — это то, что можно узнать о геометрии поверхности, «не покидая ее». На поверхности можно измерять длины, натягивая нить так, чтобы она целиком лежала на поверхности. Возникающая кривая называется геодезической (аналог прямой на плоскости). Можно измерять углы между геодезическими, изучать геодезические треугольники и многоугольники. Если мы будем изгибать поверхность (считая ее нерастяжимой и неразрываемой пленкой), то расстояния между точками будут сохраняться, геодезические будут оставаться геодезическими и т. д.

Оказывается, «не покидая поверхности», можно узнать, кривая она или нет. «Настоящую» кривую поверхность ни при каком изгибании нельзя развернуть на плоскость; Гаусс предложил числовую характеристику меры искривления поверхности.

Рассмотрим около точки A на поверхности окрестность площади ε. В каждой точке этой окрестности проведем нормаль (перпендикуляр к поверхности) единичной длины. Для плоскости все нормали будут параллельны, а для кривой поверхности будут расходиться. Перенесем нормали так, чтобы их начала оказались в одной точке. Тогда концы нормалей заполнят некоторую фигуру на единичной сфере. Пусть $\varphi(\varepsilon)$ — площадь этой фигуры. Тогда $k(A) = \lim_{\varepsilon\to 0} \dfrac{\varphi(\varepsilon)}{\varepsilon}$ дает меру кривизны поверхности в точке A.

Оказывается, ни при каком изгибании $k(A)$ не меняется. Для того, чтобы кусок поверхности можно было развернуть на плоскость, необходимо, чтобы во всех точках A этого куска было $k(A) = 0$. Мера кривизны связана с суммой углов геодезического треугольника.

Гаусс интересуется поверхностями постоянной кривизны. Сфера является поверхностью постоянной положительной кривизны (во всех ее точках $k(A) = 1/R$, где R — радиус). В записях Гаусса упоминается поверхность вращения постоянной отрицательной кривизны. Потом ее назовут *псевдосферой,* и Бельтрами обнаружит, что ее внутренняя геометрия есть геометрия Лобачевского.

Неевклидова геометрия. По некоторым сведениям, Гаусс интересовался постулатом о параллельных еще в Брауншвейге в 1792 г. В Геттингене он много обсуждал проблему параллельных со студентом из Венгрии Фаркашем Бойяи. Из письма 1799 г., адресованного Ф. Бойяи, мы узнаем, насколько ясно понимал Гаусс, что имеются многочисленные утверждения, приняв которые, можно доказать пятый постулат: «Я достиг многого, что для большинства могло бы сойти за доказательство». И вместе с тем: «Однако дорога, которую я выбрал, ведет скорее не к желательной цели, а к тому, чтобы сделать сомнительной истинность геометрии». Отсюда до понимания возможности неевклидовой геометрии один шаг, но он все-таки еще не был сделан, хотя эта фраза часто ошибочно воспринимается как свидетельство того, что Гаусс пришел к неевклидовой геометрии уже в 1799 г.

Заслуживают внимания слова Гаусса, что он не имеет возможности уделить достаточно времени этим вопросам. Характерно, что о проблеме параллельных нет ничего в дневнике. По-видимому, она никогда не находилась в центре внимания Гаусса. В 1804 г. Гаусс опровергает попытки Ф. Бойяи доказать постулат о параллельных. Письмо заканчивается так: «Однако я еще надеюсь на то, что некогда, и еще до моего конца, эти подводные камни позволят перебраться через них». Похоже, что эти слова означают надежду, что доказательство будет найдено.

Вот еще несколько свидетельств: «В теории параллельных мы до сих пор не опередили Евклида. Это позорная часть математики, которая, рано или поздно, должна принять совершенно другой вид» (1813 г.). «Мы не продвинулись дальше того места, где был Евклид 2000 лет назад» (1816 г.). Однако в том же 1816 г. он говорит о «пробеле, который нельзя заполнить», а в 1817 г. в письме Ольберсу мы читаем: «Я все больше прихожу к убеждению, что необходимость нашей геометрии не может быть доказана, по крайней мере, человеческим умом и для человеческого ума. Может быть, в другой жизни мы придем к другим взглядам на природу пространства, которые нам теперь недоступны. До тех пор геометрию следует ставить в ряд не с арифметикой, существующей чисто априори, а скорее с механикой».

Примерно в то же время к мысли о невозможности доказать пятый постулат пришел юрист из Кенигсберга Швейкарт. Он предположил, что наряду с евклидовой геометрией существует «астральная геометрия», в которой постулат о параллельных не имеет места. Работавший в Кенигсберге ученик Гаусса Герлинг написал учителю о мыслях Швейкарта и приложил заметку последнего. В ответе Гаусс пишет: «Почти все списано с моей души». Деятельность Швейкарта продолжил его племянник Тауринус, с которым Гаусс обменялся несколькими письмами, начиная с 1824 г.

В письмах Гаусс подчеркивает, что его высказывания носят сугубо частный характер и их ни в коем случае не следует предавать гласности. Он не верит, что эти идеи могут быть восприняты, и боится заинтересованности толпы дилетантов. Гаусс пережил немало тяжелых лет и очень дорожит возможностью спокойно работать. Он предупреждает Герлинга, который собирался лишь упомянуть, что постулат о параллельных может оказаться неверен: «Но осы, гнездо которых Вы разрушаете, поднимутся над Вашей головой». Постепенно зреет решение записать результаты, но не публиковать их: «Вероятно, я еще не скоро смогу обработать свои пространные исследования по этому вопросу, чтобы их можно было опубликовать. Возможно даже, я не решусь на это во всю свою жизнь, потому что боюсь крика беотийцев[1], который поднимется, если я выскажу свои воззрения целиком» (письмо Бесселю 1829 г.). В мае 1831 г. Гаусс начинает систематические записи: «Вот уже несколько недель, как я начал излагать письменно некоторые результаты моих собственных размышлений об этом предмете, частично имеющих уже 40-летнюю давность, но никогда мною не записанных, вследствие чего я должен был 3 или 4 раза возобновлять весь труд в моей голове. Мне не хотелось бы, однако, чтобы это погибло вместе со мной» (письмо Шумахеру).

Однако в 1832 г. он получил от Фаркаша Бойяи небольшое сочинение его сына Яноша «Аппендикс» (название связано с тем, что оно было издано в виде приложения к большой книге отца). «Мой сын ставит на твое суждение больше, чем на суждение всей Европы». Содержание книги поразило Гаусса: в ней полно и систематически строилась неевклидова геометрия. Это были не отрывочные замечания и догадки Швейкарта-Тауринуса. Такое изложение собирался получить сам Гаусс в ближайшее время. Он пишет Герлингу: «...я нашел все мои собственные идеи и резуль-

[1]По преданию, жители Беотии славились в Древней Греции своей глупостью.

таты, развитые с большим изяществом, хотя, вследствие сжатости изложения, в форме, трудно доступной тому, кому чужда эта область ⟨...⟩; я считаю, что этот юный геометр Бойяи — гений первой величины». А вот что написано отцу: «...все содержание работы, путь, по которому твой сын пошел, и результаты, которые он получил, — почти сплошь совпадают с моими, которые я частично получил уже 30 – 35 лет тому назад. Я действительно этим крайне поражен. Я имел намерение о своей собственной работе, кое-что из которой я теперь нанес на бумагу, при жизни ничего не публиковать ⟨...⟩ я имел намерение ⟨...⟩, чтобы эти мысли, по, крайней мере, не погибли со мной. Я поэтому чрезвычайно поражен случившимся — оно освобождает меня от этой необходимости; и меня очень радует, что именно сын моего старого друга таким удивительным образом меня предвосхитил». Никакой публичной оценки или поддержки Янош Бойяи от Гаусса не получил. По-видимому, одновременно Гаусс прервал систематические записи по неевклидовой геометрии, хотя сохранились эпизодические заметки, относящиеся к 40-м годам.

В 1841 г. Гаусс познакомился с немецким изданием работы Лобачевского (первые публикации Лобачевского относятся к 1829 г.). Верный себе, Гаусс, интересуется другими публикациями автора, ограничиваясь высказываниями о нем в переписке с близкими корреспондентами. Впрочем, по предложению Гаусса, в 1842 г. Лобачевского «как одного из превосходнейших математиков русского государства» избрали членом-корреспондентом Геттингенского ученого королевского общества. Гаусс лично известил Лобачевского об избрании. Однако ни в представлении Гаусса, ни в дипломе, выданном Лобачевскому, неевклидова геометрия не упоминалась.

О работах Гаусса по неевклидовой геометрии узнали лишь при публикации посмертного архива. Так Гаусс обеспечил себе возможность спокойно работать отказом обнародовать свое великое открытие, вызвав не смолкающие по сей день споры о допустимости занятой им позиции,

Следует отметить, что Гаусса интересует не только чисто логический вопрос о доказуемости постулата о параллельных. Его интересует место геометрии в естественных науках, вопрос об истинной геометрии нашего физического мира (см. выше высказывание от 1817 г.). Он обсуждает возможность астрономической проверки, с интересом отзываясь о соображениях Лобачевского по этому поводу. При занятиях геодезией Гаусс не удержался от измерения суммы углов треугольника с вершинами Высокий Гаген, Брокен, Инсельберг. Отклонение от π не превысило $0{,}2^\circ$.

Электродинамика и земной магнетизм. К концу 20-х годов Гаусс, перешедший 50-летний рубеж, начинает поиски новых для себя областей научной деятельности. Об этом свидетельствуют две публикации 1829 и 1830 гг. Первая из них несет печать размышлений об общих принципах механики (здесь строится «принцип наименьшего принуждения» Гаусса); другая посвящена изучению капиллярных явлений. Гаусс решает заниматься физикой, но его узкие интересы еще не определились. В 1831 г. он пытается заниматься кристаллографией. Это очень трудный год в жизни Гаусса: умирает его вторая жена, у него начинается тяжелейшая бессонница. В этом же году в Геттинген приезжает приглашенный по инициативе Гаусса 27-летний физик Вильгельм Вебер. Гаусс познакомился с ним в 1828 г. в доме Гумбольдта. О замкнутости Гаусса ходили легенды, и все же в Вебере он нашел сотоварища по занятиям наукой, какого он никогда не имел прежде.

«Внутреннее различие этих людей достаточно выражалось также и в их внешнем облике. Гаусс — приземистый, крепкого телосложения, настоящий представитель Нижней Саксонии, малоразговорчивый и замкнутый в себе. Своеобразной противоположностью ему является небольшой, изящный, подвижный Вебер, чрезвычайная любезность и разговорчивость которого сразу же обнаруживали коренного саксонца; он был действительно родом из Виттенберга, этой страны „саксонцев в квадрате“. На геттингенском памятнике Гауссу и Веберу эта противоположность из художественных соображений смягчена, и даже по возрасту они кажутся более близкими, чем это было в действительности» (Ф. Клейн).

Интересы Гаусса и Вебера лежали в области электродинамики и земного магнетизма. Их деятельность имела не только теоретические, но и практические результаты. В 1833 г. они изобретают электромагнитный телеграф (это событие запечатлено в их общем памятнике). Первый телеграф связывал обсерваторию и

Карл Фридрих Гаусс

физический институт. По финансовым причинам внедрить телеграф в жизнь его создателям не удалось.

В процессе занятий магнетизмом Гаусс пришел к выводу, что системы физических единиц надо строить, вводя некоторое количество независимых величин и выражая остальные величины через них. Изучение земного магнетизма опиралось как на наблюдения в магнитной обсерватории, созданной в Геттингене, так и на материалы, которые собирались в разных странах «Союзом для наблюдения над земным магнетизмом», созданным Гумбольдтом после возвращения из Южной Америки. В это же время Гаусс создает одну из важнейших глав математической физики — теорию потенциала. Совместные занятия Гаусса и Вебера были прерваны в 1843 г., когда Вебера вместе с шестью другими профессорами изгнали из Геттингена за подписание письма королю, в котором указывались нарушения последним конституции (Гаусс не подписал письма). Возвратился в Геттинген Вебер лишь в 1849 г., когда Гауссу было уже 72 года. Мы закончим наш рассказ о Гауссе словами Клейна: «Гаусс напоминает мне образ высочайшей вершины баварского горного хребта, какой она предстает перед глазами наблюдателя, глядящего с севера. В этой горной цепи в направлении с востока на запад отдельные вершины подымаются все выше и выше, достигая предельной высоты в могучем, высящемся в центре великане; круто обрываясь, этот горный исполин сменяется низменностью новой формации, в которую на много десятков километров далеко проникают его отроги, и стекающие с него потоки несут влагу и жизнь».

Добавление. Задачи на построение, приводящие к кубическим уравнениям

В «Арифметических исследованиях» Гаусс сообщает без доказательства, что нельзя построить циркулем и линейкой правильные n-угольники для простых n, не являющихся простыми числами Ферма, в частности, правильный 7-угольник. Этот отрицательный результат должен был удивить современников не меньше, чем возможность построения правильного 17-угольника. Ведь $n = 7$ — первое значение n, для которого, несмотря на многочисленные попытки, построение правильного n-угольника не получалось. Несомненно, что греческие геометры подозревали, что с этой задачей дело обстоит неблагополучно, и неспроста, скажем, Архимед предложил способ построения правильного n-угольника, использующий конические сечения. Однако вопрос о доказательстве невозможности построения, по-видимому, даже не вставал.

Надо сказать, что доказательства отрицательных утверждений всегда играли в истории математики принципиальную роль. Доказательство невозможности требует так или иначе обозреть все мыслимые способы решения, построения или доказательства, в то время как для положительного решения достаточно указать один конкретный способ.

Доказательства невозможности в математике имели знаменательное начало, когда пифагорейцы (VI век до н. э.), стремившиеся всю математику свести к целым числам, собственными руками похоронили эту идею: оказалось, что не существует дроби, квадрат которой равен 2. Другая формулировка: диагональ и сторона квадрата несоизмеримы. Итак, целых чисел и их отношений недостаточно для описания очень простой ситуации. Это открытие удивило величайших мыслителей Древней Греции. Легенда утверждает, что боги покарали пифагорейца, сообщившего этот факт людям (он погиб при кораблекрушении). Платон (429 – 348 до н. э.) рассказывает о том, как поразило его существование иррациональных величин. Однажды Платон столкнулся с «практической» задачей, заставившей его переосмыслить возможности геометрии.

«Эратосфен рассказывает в своем сочинении „Платоник“, что когда бог возвестил через оракула делийцам, что, дабы избавиться от чумы, они должны построить жертвенник вдвое больше старого, строители стали в тупик перед задачей построить тело, в два раза большее данного. Они обратились за советом к Платону, и тот сказал им, что бог дал им это предсказание не потому, что ему нужен вдвое больший жертвенник, но что он возвестил это в укор грекам, которые не думают о математике и не дорожат геометрией» (Теон Смирнский). Платону не откажешь в умении использовать подходящий момент для пропаганды науки! По свидетельству Евтония, аналогичная задача (об удвоении надгробного камня Главку) фигурировала уже в одном варианте легенды о Миносе.

Итак, речь идет о нахождении стороны куба с удвоенным объемом, т. е. о построении корня уравнения $x^3 = 2$. Платон направил делийцев к Евдоксу и Геликону. Разные решения предложили Менехм, Архит и Евдокс, но никто из них не нашел построения при помощи циркуля и линейки. Позднее Эратосфен, построивший механический прибор для решения задачи об удвоении куба, в стихотворении, высеченном на мраморной доске в храме Птолемея в Александрии, квалифицирует решения своих предшественников как слишком сложные: «Нужды тебе уж не будет в премудром цилиндре Архита, в конусе не для тебя высек триаду Менехм, и с богоравным Евдоксом изогнутых линий не надо ...». Менехм заметил, что решаемая задача эквивалентна задаче о двух средних пропорциональных (для заданных a, b): $a : x = x : y = y : b$. Его решение использовало конические сечения. Об «изогнутых линиях» Евдокса мы ничего не знаем. Что касается механического решения, то Эратосфен не был первым. По свидетельству Плутарха, «сам Платон порицал друзей Евдокса, Архита и Менехма, которые хотели свести удвоение куба к механическим построениям; ибо они думали получить средние пропорциональные не из теоретических соображений, но ведь таким образом уничтожается и гибнет благо геометрии, и этим путем геометрия возвращается обратно к чувственному, вместо того чтобы подыматься выше этого и твердо держаться вечных, нематериальных образов, пребывающий в коих Бог есть вечный Бог». Впрочем, Евтоний приписывает самому Платону (по-видимому, ошибочно) некое механическое решение делийской задачи, использующее плотничьи угольники с пазами и подвижными рейками. Платону с его отвращением к «материальным вещам, которые требуют длительной обработки недостойным ремеслом» (Плутарх) нередко противопоставляют Архимеда (287 – 212 до н. э.), прославившегося многочисленными изобретениями, в частности, машинами, примененными при обороне Сиракуз. Впрочем, тот же Плутарх утверждает, что Архимед лишь поддался уговорам царя Гиерона «отвлечь свое искусство от абстракций $\langle\ldots\rangle$, и осязательным образом заняться тем, чего требует действительность», хотя и считал, что практика — «дело низкое и неблагородное; сам же он стремился лишь к тому, что по красоте своей и совершенству находится далеко от царства необходимости».

Наряду с делийской задачей греческая геометрия оставила еще несколько задач, в которых построение не удавалось осуществить циркулем и линейкой: трисекция угла (деление угла на три равные части), квадратура круга и задача о построении правильного n-угольника, в частности, 7-угольника и 9-угольника. Связь некоторых из этих задач с кубическими уравнениями сознавали греческие и еще в большей степени арабские математики.

Задача о правильном 7-угольнике сводится к уравнению $z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0$ (см. с. 316) или

$$\left(z^3 + \frac{1}{z^3}\right) + \left(z^2 + \frac{1}{z^2}\right) + \left(z + \frac{1}{z}\right) + 1 = 0.$$

Переходя к переменной $x = z + \dfrac{1}{z}$, получаем уравнение

$$x^3 + x^2 - 2x - 1 = 0.$$

Мы покажем, что корни уравнений удвоения куба и семиугольника не могут быть квадратичными иррациональностями, откуда и будет следовать невозможность построения циркулем и линейкой. Мы докажем результат, который обслуживает весьма общую ситуацию:

Теорема. *Если кубическое уравнение $a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ с целыми коэффициентами имеет корень, являющийся квадратичной иррациональностью, то оно имеет и рациональный корень.*

Доказательство. Пусть x_1 — такой корень. Он получается из целых чисел при помощи арифметических операций и извлечения квадратного корня. Проанализируем эту конструкцию. Вначале корень извлекается из некоторого количества рациональных чисел: $\sqrt{A_1}$, $\sqrt{A_2}, \ldots, \sqrt{A_a}$, затем из некоторых чисел, получающихся при помощи арифметических операций из рациональных чисел и $\sqrt{A_i}$ ($\sqrt{B_1}$, $\sqrt{B_2}, \ldots, \sqrt{B_b}$) и т. д.; на каждом шаге корень извлекается из каких-то чисел, арифметически выражающихся через полученные на всех предыдущих шагах. Возникают «этажи» квадратичных иррациональностей. Пусть $\sqrt{N}$ — одно из чисел, полученных на последнем шаге перед образованием x_1. Сконцентрируем внимание на том, как $\sqrt{N}$ входит в x_1. Оказывается, можно считать, что $x_1 = \alpha + \beta\sqrt{N}$, где $\sqrt{N}$ не входит в квадратичные иррациональности α и β. Достаточно заметить, что арифметические операции над выражениями вида $\alpha + \beta\sqrt{N}$ приводят к таким же выражениям: для сложения и вычитания это очевидно, для умножения проверяется непосредственно, для деления надо исключить $\sqrt{N}$ из знаменателя:

$$\frac{\alpha + \beta\sqrt{N}}{\gamma + \delta\sqrt{N}} = \frac{(\alpha + \beta\sqrt{N})(\gamma - \delta\sqrt{N})}{\gamma^2 - \delta^2 N}.$$

Если теперь подставить $x_1 = \alpha + \beta\sqrt{N}$ в уравнение и выполнить действия, то получится соотношение вида $P + Q\sqrt{N} = 0$, где P, Q — многочлены от α, β, a_i. Если $Q \neq 0$, то $\sqrt{N} = -P/Q$, и подставляя выражение для $\sqrt{N}$ в x_1, можно получить для x_1 представление, уже не содержащее $\sqrt{N}$. Если же $Q = 0$, то проверяется, что $x_2 = \alpha - \beta\sqrt{N}$ — также корень, а учитывая, что $-a_2/a_3 = x_1 + x_2 + x_3$ — сумма корней (теорема Виета), получаем: $x_3 = -a_2/a_3 - 2\alpha$, т. е. опять-таки имеется корень, являющийся квадратичной иррациональностью, выражающейся через $\sqrt{A_i}$, $\sqrt{B_i}, \ldots$, как и x_1, но без $\sqrt{N}$. Продолжая этот процесс дальше, мы избавимся в выражении для корня уравнения ото всех радикалов поэтажно, начиная с последнего этажа. После этого получится рациональный корень, и доказательство окончено.

Теперь остается проверить, что у интересующих нас уравнений нет рациональных корней. Предположим, что у уравнения старший коэффициент $a_3 = 1$. Тогда всякий рациональный корень является целым. Достаточно подставить $x = p/q$ (p и q взаимно просты) в уравнение, умножить обе части на q^3 и убедиться, что p^3, а значит и p, делится на q, т. е. $q = 1$. Далее, если α — корень, то $x^3 + a_2x^2 + a_1x + a_0 = (x - \alpha)(x^2 + mx + n)$, где $a_2 = \alpha + m$, $a_1 = -\alpha m + n$, $a_0 = -\alpha n$, т. е. $m = a_2 + \alpha$, $n = a_1 + a_2\alpha + \alpha^2$. Значит, если a_i и α — целые, то m и n — целые, и α должен быть делителем a_0. В результате для уравнений с $a_3 = 1$ поиски рациональных корней сводятся к перебору конечного числа возможностей — делителей свободного члена. Для интересующих нас уравнений легко проверяется отсутствие целочисленных корней, а значит, отсутствие корней, являющихся квадратичными иррациональностями.