НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ МИРЗА УЛУГБЕКА

Механико-математический факульет

РЕФЕРАТ

на тему:

«Гаусс всегда живет в сердцах математиков»

Выполнил: Эргашев О.

Проверил: Нормуродов Н.

Ташкент 2013

Содержание

О жизни

Иоганн Карл Фри́дрих Га́усс (нем. *Johann Carl Friedrich Gauß*; 30 апреля 1777, Брауншвейг — 23 февраля 1855, Гёттинген) — немецкийматематик, астроном и физик, считается одним из величайших математиков всех времён, «королём математиков». Лауреат медали Копли (1838), иностранный член шведской (1821) и российской (1824) Академий наук, английского Королевского общества.

Биография

1777—1798 годы

Дом, где родился Гаусс (не сохранился)

Дед Гаусса был бедным крестьянином, отец — садовником, каменщиком, смотрителем каналов в герцогстве Брауншвейг. Уже в двухлетнем возрасте мальчик показал себя вундеркиндом. В три года он умел читать и писать, даже исправлял счётные ошибки отца. Согласно легенде, школьный учитель математики, чтобы занять детей на долгое время,

предложил им сосчитатьсумму чисел от 1 до 100. Юный Гаусс заметил, что попарные суммы с противоположных концов одинаковы: 1+100=101, 2+99=101 и т. д., и мгновенно получил результат: $50 \times 101 = 5050$.

До самой старости он привык большую часть вычислений производить в уме.

С учителем ему повезло: М. Бартельс (впоследствии учитель Лобачевского) оценил исключительный талант юного Гаусса и сумел выхлопотать ему стипендию от герцога Брауншвейгского. Это помогло Гауссу закончить колледж Collegium Carolinum в Брауншвейге (1792—1795).

Свободно владея множеством языков, Гаусс некоторое время колебался в выборе между филологией и математикой, но предпочёл последнюю. Он очень любил латинский язык и значительную часть своих трудов написал на латыни; любил английскую, французскую и русскую литературу. В возрасте 62 лет Гаусс начал изучать русский язык, чтобы ознакомиться с трудамиЛобачевского, и вполне преуспел в этом деле.

В колледже Гаусс изучил труды Ньютона, Эйлера, Лагранжа. Уже там он сделал несколько открытий в теории чисел, в том числе доказал закон взаимности квадратичных вычетов. Лежандр, правда, открыл этот важнейший закон раньше, но строго доказать не сумел; Эйлеру это также не удалось. Кроме этого, Гаусс создал «метод наименьших квадратов» (тоже независимо открытый Лежандром) и начал исследования в области «нормального распределения ошибок».

С 1795 по 1798 год Гаусс учился в Гёттингенском университете. Это наиболее плодотворный период в жизни Гаусса.

1796 год: Гаусс доказал возможность построения с помощью циркуля и линейки правильного семнадцатиугольника. Более того, он разрешил проблему построения правильных многоугольников до конца и нашёл критерий возможности построения правильного *n*-угольника с помощью циркуля и линейки: если *n* — простое число, то оно должно быть

вида $n = 2^{2^k} + 1$ (числом Ферма). Этим открытием Гаусс очень дорожил и завещал изобразить на его могиле правильный 17-угольник, вписанный в круг.

С 1796 года Гаусс ведёт краткий дневник своих открытий. Многое он, подобно Ньютону, не публиковал, хотя это были результаты исключительной важности (эллиптические функции,неевклидова геометрия и др.). Своим друзьям он пояснял, что публикует только те результаты, которыми доволен и считает завершёнными. Многие отложенные или заброшенные им идеи позже воскресли в трудах Абеля, Якоби, Коши, Лобачевского и др. Кватернионы он тоже открыл за 30 лет до Гамильтона (назвав их «мутациями»).

Все многочисленные опубликованные труды Гаусса содержат значительные результаты, сырых и проходных работ не было ни одной.

1798 год: закончен шедевр «Арифметические исследования» (лат. *Disquisitiones Arithmeticae*), напечатан только в 1801 году.

В этом труде подробно излагается теория сравнений в современных (введенных им) обозначениях, решаются сравнения произвольного порядка, глубоко исследуются квадратичные формы, комплексные корни из единицы используются для построения правильных n-угольников, изложены свойства квадратичных вычетов, приведено доказательство квадратичного закона взаимности и т. д. Гаусс любил говорить, что математика — царица наук, а теория чисел — царица математики.

1798—1816 годы

Памятник Гауссу в Брауншвейге с изображенной на нём 17-лучевой звездой

В 1798 году Гаусс вернулся в Брауншвейг и жил там до 1807 года.

Герцог продолжал опекать молодого гения. Он оплатил печать его докторской диссертации (1799) и пожаловал неплохую стипендию. В своей докторской Гаусс впервые доказал основную теорему алгебры. До Гаусса было много попыток это сделать, наиболее близко к цели подошёлД'Аламбер. Гаусс неоднократно возвращался к этой теореме и дал 4 различных её доказательства.

С 1799 года Гаусс — приват-доцент Брауншвейгского университета.

1801 год: избирается членом-корреспондентом Петербургской Академии наук.

После 1801 года Гаусс, не порывая с теорией чисел, расширил круг своих интересов, включив в него и естественные науки. Катализатором послужило открытие малой планеты Церера (1801), вскоре после наблюдений потерянной. 24-летний Гаусс проделал (за несколько часов) сложнейшие вычисления по новому, открытому им же методу, и указал

место, где искать беглянку; там она, к общему восторгу, и была вскоре обнаружена.

Слава Гаусса становится общеевропейской. Многие научные общества Европы избирают Гаусса своим членом, герцог увеличивает пособие, а интерес Гаусса к астрономии ещё более возрастает.

1805 год: Гаусс женился на Иоганне Остгоф. У них было трое детей.

1806 год: от раны, полученной на войне с Наполеоном, умирает его великодушный покровитель-герцог. Несколько стран наперебой приглашают Гаусса на службу (в том числе в Петербург). По рекомендации Александра фон Гумбольдта Гаусса назначают профессором вГёттингене и директором Гёттингенской обсерватории. Эту должность он занимал до самой смерти.

1807 год: наполеоновские войска занимают Гёттинген. Все граждане облагаются контрибуцией, в том числе огромную сумму — 2000 франков— требуется заплатить Гауссу. Ольберс и Лаплас тут же приходят ему на помощь, но Гаусс отклоняет их деньги; тогда неизвестный из Франкфурта присылает ему 1000 гульденов, и этот дар приходится принять. Только много позднее узнали, что неизвестным был курфюрст Майнцский, друг Гёте.

1809 год: новый шедевр, «Теория движения небесных тел». Изложена каноническая теория учёта возмущений орбит.

Как раз в четвёртую годовщину свадьбы умирает Иоганна, вскоре после рождения третьего ребёнка. В Германии разруха и анархия. Это самые тяжёлые годы для Гаусса.

1810 год: новая женитьба, на Минне Вальдек, подруге Иоганны. Число детей Гаусса вскоре увеличивается до шести.

1810 год: новые почести. Гаусс получает премию Парижской академии наук и золотую медаль Лондонского королевского общества.

1811 год: появляется новая комета. Гаусс быстро и очень точно рассчитывает её орбиту. Начинает работу над комплексным анализом,

открывает (но не публикует) теорему, позже переоткрытую Коши и Вейерштрассом: интеграл от аналитической функции по замкнутому контуру равен нулю.

1812 год: исследование гипергеометрического ряда, обобщающего разложение практически всех известных тогда функций.

Знаменитую комету «пожара Москвы» (1812) всюду наблюдают, пользуясь вычислениями Гаусса.

1815 год: публикует первое строгое доказательство основной теоремы алгебры.

1816—1855 годы

1821 год: в связи с работами по геодезии Гаусс начинает исторический цикл работ по теории поверхностей. В науку входит «гауссова кривизна». Положено начало дифференциальной геометрии. Именно результаты Гаусса вдохновили Римана на написание его классической диссертации о «римановой геометрии».

Итогом изысканий Гаусса была работа «Исследования относительно кривых поверхностей» (1822). В ней свободно использовались общие криволинейные координаты на поверхности. Гаусс далеко развил метод конформного отображения, которое в картографии сохраняет углы (но искажает расстояния); оно применяется также в аэро/гидродинамике и электростатике.

1824 год: избирается иностранным почётным членом Петербургской Академии наук.

Гаусс в 1828 г.

1825 год: открывает гауссовы комплексные целые числа, строит для них теорию делимости и сравнений. Успешно применяет их для решения сравнений высоких степеней.

Гаусс и Вебер. Скульптура в Гёттингене.

1831 год: умирает вторая жена, у Гаусса начинается тяжелейшая бессонница. В Гёттинген приезжает приглашённый по инициативе Гаусса 27-летний талантливый физик Вильгельм Вебер, с которым Гаусс познакомился в 1828 году, в гостях у Гумбольдта. Оба энтузиаста науки сдружились, несмотря на разницу в возрасте, и начинают цикл исследований электромагнетизма.

1832 год: «Теория биквадратичных вычетов». С помощью тех же целых комплексных гауссовых чисел доказываются важные арифметические теоремы не только для комплексных, но и для вещественных чисел. Здесь же Гаусс приводит геометрическую интерпретацию комплексных чисел, которая с этого момента становится общепринятой.

1833 год: Гаусс изобретает электрический телеграф и (вместе с Вебером) строит его действующую модель.

1837 год: Вебера увольняют за отказ принести присягу новому королю Ганновера. Гаусс вновь остаётся в одиночестве.

1839 год: 62-летний Гаусс овладевает русским языком и в письмах в Петербургскую Академию просил прислать ему русские журналы и книги, в частности «Капитанскую дочку» Пушкина. Предполагают, что это связано с работами Лобачевского. В 1842 году по рекомендации Гаусса Лобачевский избирается иностранным членом-корреспондентом Гёттингенского королевского общества.

Умер Гаусс 23 февраля 1855 года в Гёттингене.

Современники вспоминают Гаусса как жизнерадостного, дружелюбного человека, с отличным чувством юмора.

Математические работы

Дебют Гаусса

Карл Фридрих родился 30 апреля 1777 г. в доме №1550, что стоял на канале Венденгребне 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, Гаусс успел переоткрыть формулу для суммы арифметической прогрессии! Слава о чуде-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 путь 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 нескольких 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 первые попавшуюся в его руки литературу: Эйлера и Лагранжа».

1 июня 1796 года в газете «Jenenser Intelligenzbllatt» 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, стоит вспомнить то, что «известно каждому начинающему геометру».

О построениях циркулем и линейкой. Предполагается заданным отрезок единичной длины. Тогда при помощи циркуля и линейки можно стоить новые отрезки, длины которых получаются из длин имеющихся отрезков при помощи следующих 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 иррациональностями. Можно доказать, что никакие другие отрезки построить при помощи циркуля и линейки нельзя.

Задача о построении правильного n-угольника, как легко понять, эквивалента 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 $\sin(\pi/n)$ – 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

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

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^kp 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 и 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.

Несколько слов о комплексных числах. Комплексному числу z=a+ib ставится в соответствие точка с координатами (a, b) и вектор с концом в этой точке и началом в (0,0). Длина вектора $r = \sqrt{a^2 + b^2}$ называется модулем данного числа IzI. Комплексоне число z можно записать в тригонометрической форме: z=a+ib= r(cosφ+sinφ); угол φ называется аргументом числа z.

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

$$\varepsilon_k = cos\frac{2\pi k}{n} + i\,sin\frac{2\pi k}{n},\ k = 0,1,\ldots, n-1. \quad (1)$$

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

Уравнение (2) имеет своими корнями ε_k при $1 \leq k \leq n - 1$. В дальнейшем будем иметь дело с уравнением (2).

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

$$z^4+z^3+z^2+z+1=0, \qquad (3)$$

имеющее четыре корня $\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4$. Хотя и существует формула Феррари для решения общего уравнения 4-й степени, пользоваться ею практически невозможно. В нашем случае помогает специальный вид уравнения (3). Чтобы решить его, разделим сначала уравнение (3) на z^2. Получим

$$z^2 + 1/z^2 + z + 1/z + 1 = 0 \text{ или } (z + 1/z)^2 + (z + 1/z) - 1 = 0.$$

Сделаем подстановку $\omega = z + \frac{1}{z}$

$$\omega^2 + \omega - 1 = 0 \quad (4)$$

Отсюда

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

Далее можно найти ε_k из уравнений

$z + \frac{1}{z} = \omega_1$, $z + \frac{1}{z} = \omega_2$, (5)

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

$2\cos(2\pi/5) = \varepsilon_1 + \varepsilon_4 = \varepsilon_1 + = \omega_1 = \frac{1 \pm \sqrt{5}}{2}$

Из того, что ω_1 – квадратичная иррациональность, следует, что ε_1 и ε_4 представляют собой квадратичные иррациональности. Для ε_2 и ε_3 рассуждаем в точности также.

Итак, для n=5 решение нашей задачи удалось свести к последовательному решению двух квадратичных уравнений: сначала решается уравнение (2), корнями которого являются суммы $\varepsilon_1 + \varepsilon_4$ и $\varepsilon_1 + \varepsilon_4$ симметричных корней уравнения (3), а затем из уравнений (5) находятся и сами уравнения (3).

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 $p<1000$.

Известно, что Гаусс не сразу попытался доказать периодичность получающейся дробив 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. 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 $10^{k1,}$ 10^{k2} при делении на p дадут одинаковые остатки. Но тогда $10^{k1-k2} - 1$ делится на p.

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, носящей название малой теоремы Ферма. Когда Ферма (1601–1655) открыл ее, он писал, что его «озарило ярким светом». Теперь ее переоткрыл Гаусс. ОН всегда будет ценить это утверждение: «Эта теорема… 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). До сих пор неизвестно, конечно или бесконечно число таких p.

Гаусс заменяет 10 на любое число a и интересуется, когда $a^k - 1$ не делится на p при $k<p-1$ (предполагается, что a не делится на p). Такие p принято называть первообразными корнями для a. Условие того, что p – первообразный корень, равносильно тому, что среди остатков от деления 1, a, a^2, …, a^{p-2} на p встречаются все ненулевые остатки 1, 2, …, p – 1.

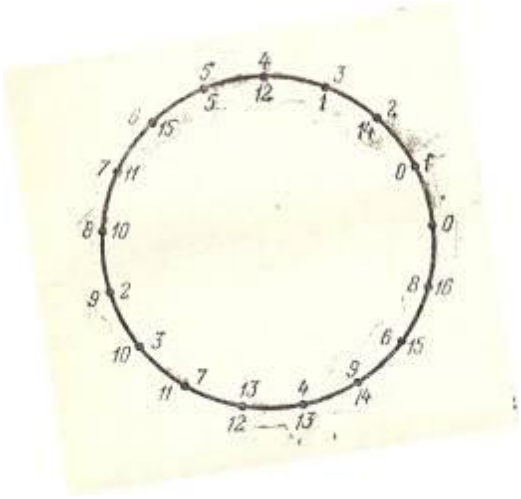
Гаусс не знал тогда, что первообразными корнями интересовался уже Эйлер (1707–1783), который предполагал (но не смог доказать), что для каждого простого числа существует хотя бы один первообразный корень. Первое доказательство гипотезы Эйлера дал Лагранж (1752–1833); очень изящное доказательство дал Гаусс. Но это было позднее, а пока Гаусс манипулировал с конкретными примерами. Он знал, например, что для a = 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. Стоит обратить внимание на то, что во 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

$$Z^{16} + z^{15} + z^{14} + \ldots + z + 1 = 0 \quad (6)$$

(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 (6) на группы, свести решение (6) к цепочке квадратных уравнений.



Именно, на первом шагу берутся $\sigma_{2,0}$, $\sigma_{2,1}$ – соответственно сумы 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 $\sigma_{s,I}$ 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: $\sigma_{s,0} = 2\cos(2\pi/17)$ и из квадратичной иррациональности $\sigma_{s,0}$ следует возможность построения правильного семнадцатиугольника циркулем и линейкой. Поучительно записать разбиение корней на группы в старой нумерации. Но в таком виде угадать разбиение не возможно. Теперь реализуем только что описанный путь.

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

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

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

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

Чтобы различить корни, опять воспользуемся рисунком. 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:

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

Имеем: $\sigma_{4,0} + \sigma_{4,2} = \sigma_{2,0}$; $\sigma_{4,1} + \sigma_{4,3} = \sigma_{2,1}$. Можно показать далее, что $\sigma_{4,0} \times \sigma_{4,2} = \sigma_{2,0} \times \sigma_{2,1} = -1$, а значит, $\sigma_{4,0}$, $\sigma_{4,2}$ – корни уравнения $x^2 - \sigma_{2,0} x - 1 = 0$. Решая это уравнение и учитывая, что $\sigma_{4,0} > \sigma_{4,2}$, получаем после несложных преобразований

$$\sigma_{4,0} = {}^1/_4 (\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}}),$$
$$\sigma_{4,2} = {}^1/_4 (\sqrt{17} - 1 - \sqrt{34 - 2\sqrt{17}}).$$

Аналогично показывается, что

$$\sigma_{4,1} = {}^1/_4(-\sqrt{17} - 1 + \sqrt{34 + 2\sqrt{17}}),$$
$$\sigma_{4,3} = {}^1/_4(-\sqrt{17} - 1 - \sqrt{34 + 2\sqrt{17}}).$$

Переходим к заключительному этапу. Положим

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

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

$$\sigma_{s,0} = 2\cos\frac{2\pi}{17} = {}^1/_2(\sigma_{4,0} + \sqrt{(\sigma_{4,0})^2 - 4\sigma_{4,1}}) =$$
$$= {}^1/_8(\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}}) +$$
$$+ {}^1/_4\sqrt{17 + 3\sqrt{17} - \sqrt{170 + 38\sqrt{17}}}.$$

Мы несколько преобразовали непосредственно получаемое выражение для $\sqrt{\sigma_{4,0} - 4\sigma_{4,1}}$;

Пользуясь полученной формулой для $\cos(2\pi/17)$, построение правильного 17-угольниука можно выполнить при помощи элементарных правил построения выражений, являющихся квадратичными иррациональностями. Разумеется, получится весьма громоздкая процедура. В настоящее время известны довольно компактные способы построения. 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 построение 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 (6) остался совершенно невыясненным вопрос о том, почему оказалось удачным разбиение корней, использующее нумерацию $\varepsilon_{[l]}$, как можно 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 (6). 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 до деления k на n. Положим $\varepsilon = \varepsilon_1$; тогда ε_k есть просто ε в степени k, поэтому $\varepsilon_k \times \varepsilon_l = \varepsilon_{k+l}$, где сумма берется по модулю n (остаток от деления на n); в частности $\varepsilon_k \times \varepsilon_{n-k} = \varepsilon_0 = 1$.

Задача 1. Если p – просто число и δ – любой комплексный корень p-й степени из единицы, то множество δ^k, k = 0, 1, …, 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, …, p – 1, на p содержатся все числа 0, 1, …, p – 1.

Обозначим через T_k следующее преобразование (возведение в степень k): $T_k\varepsilon_l = (\varepsilon_1)^h = \varepsilon_{lk}$.

Задача 2. Доказать, что если n = p – просто число, то каждое из преобразований T_k (k = 1, 2, …, 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 $1 \le l \le p-1$ множество $\{T_0\varepsilon_l, T_1\varepsilon_l, \ldots, T_{p-1}\varepsilon_l\}$ 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 $T_k\varepsilon_1$, $1 \le k, l \le p-1$; тогда в каждой строке и каждом столбце стоят все корни $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{p-1}$ в некотором порядке без повторений. Отметим, что $T_{p-1}\varepsilon_l = \varepsilon_{-l} = (\varepsilon_l)^{-1}$.

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

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).

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 четным k: корни $\varepsilon_{[l]}$ с четными l и корни с нечетными l. Их суммы обозначим через $\sigma_{2,0}$, $\sigma_{2,1}$.

Ясно, что $\sigma_{2,0} + \sigma_{2,1} = -1$. Исследуем $\sigma_{2,0} \times \sigma_{2,1}$. Это произведение является суммой попарных произведений $\varepsilon_{[k]} \times \varepsilon_{[l]}$, 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 $\sigma_{2,0} \times \sigma_{2,1} = -4$. Воспользуемся тем, что преобразования $T_{[k]}$ сохраняют группы корней при k четном и переводят их одна в другую при k нечетном. Каждое слагаемое в $\sigma_{2,0} \times \sigma_{2,1}$ однозначно представимо в виде $\varepsilon_{[m]} \varepsilon_{[m+r]}$, где $0 \leq m \leq 15$, r = 1, 3, 5, 7. Сгруппируем слагаемые с одинаковыми r. Полученные суммы будут иметь вид

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

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 имеется четыре группы корней, инвариантные 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 $\sigma_{4,0} \times \sigma_{4,2}$; оно представляется в виде суммы слагаемых вида $\varepsilon_{[4l]} \varepsilon_{[4l+2]}$. 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 $\varepsilon_{[0]}\,\varepsilon_{[2]} = \varepsilon_1\,\varepsilon_9 = \varepsilon_{10} = \varepsilon_{[3]}$, $\varepsilon_{[0]}\,\varepsilon_{[6]} = \varepsilon_1\,\varepsilon_{15} = \varepsilon_{16} = \varepsilon_{[16]}$. При r = 1 получаем сумму

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

при r = 3 – сумму = $\sigma_{2,0}$, т.е. $\sigma_{4,0} \times \sigma_{4,2} = \sigma_{2,0} + \sigma_{2,1} = -1$. Решая квадратные уравнения, мы нашли $\sigma_{4,0}$, $\sigma_{4,2}$.

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

Мы видела, 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, $\sigma_{2,0}$, $\sigma_{2,1}$ – 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 $\sigma_{2,0} \times \sigma_{2,1}$ – целое число. Аналогично, $\sigma_{4,0} \times \sigma_{4,2}$ не меняется при всех преобразованиях вида $T_{[2k]}$, а потому является комбинацией $\sigma_{2,j}$; $\sigma_{8,0} \times \sigma_{8,4}$ 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 корней. Как мы уже отмечали, для любого простого p хотя бы один первообразный корень существует (кстати, можно показать, 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 n-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 – 65537. Оба эти числа простые. При r = 5 получается число 4294967297. 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 $5\times2^{75} + 1$). Имеется гипотеза, что существует лишь конечное число простых чисел Ферма.

Что касается правильных n-угольников для составного n, то в силу обстоятельств, отмеченных выше, мы сразу получаем возможность искомого построения для всех n>2 вида $2^k p_1 p_2 \ldots p_l$, где $p_1 p_2 \ldots p_l$, – 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 других случаев, кроме тех, которые указаны нашей теорией, например, не надеялся бы свести на геометрические

построения деление окружностей на 7, 11, 13, 19, … 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 солидным размеров в Геттингене). Вот какую шутку придумал по этому поводу английский математик Дж. Литлвуд: «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 года, когда было найдено построение правильного 17-угольника, решил 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 неевклидовской 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 уравнений 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).

Золотая теорема

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 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 извлечь 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 = просто число, причем p≠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 n единственным образом представляется в виде

$$n = pq + r, \quad |r| \leqslant \frac{p-1}{2} \qquad (1)$$

где q и r – целые.

Таблица 1

p	$k = \frac{p-1}{2}$	Вычеты (остатки) по модулю
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

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 таблицу 1 вычеты 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, имеютодин и тот же остаток при делении на p. Поэтому, если мы хотим найти квадратичные вычеты, то достаточно возводить в квадрат лишь вычеты, т.е. целые числа r, $|r| \le k = (p-1)/2$. При этом, разумеется, достаточно рассматривать $r \ge 0$.

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

Таблица 2

p	k	Квадратичные вычеты и невычеты по модулю
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**

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 простоого) квадратичных вычетов не больше k + 1. Мы покажем, что их точно k + 1, если убедимся, что все числа $r^2 (0 \le r \le k)$ дают при делении на p различные остатки. Если $r_1 > r_2$ и $r_1^2 - r_2^2$ дают одинаковые остатки, то $r_1^2 - r_2^2$ делится на p. Поскольку p – просто число, то $r_1 + r_2$ или $r_1 - r_2$ должно делиться на p, чего не может быть, так как $0 < r_1 \pm r_2 < 2k < p$. Здесь мы впервые воспользовались простотой p.

Теорема Ферма и критерий Эйлера. Далее, очевидно, что 0 и 1 являются жирными во всех строчках. Что касается остальных столбуов, то сразу не видна закономерность, согласно которой в них появляются жирные числа. Начнем с a = – 1. Оно является жирным при p = 5, 13, 17, … и не является при p = 3, 7, 11… Простые числа первой группы при делении на 4 дают остататок 1, а второй – остаток -1 (простые числа p≠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.

Первое доказательство после нескольких неудачных попыток нашел в 1747 году Эйлер. В 1755 году Эйлер нашел другое, очень изящное доказательство, использующее малую теорему Ферма: Если p – просто число, то для всякого целого a, 0<IaI<p,

$$a^{p-1} \equiv 1 \pmod{p}. \quad (2)$$

Доказательство. При p = 2 утверждение очевидно, и можно считать p нечетным. Рассмотрим p чисел 0, ±a, ±2a, ±3a, …, ±ka; k = (p – 1)/2. Все эти числа при делении на p дают разные остатки, так как в противном случае $r_1a – r_2a$, $r_1 > r_2$, $Ir_1I \le k$, $Ir_2I \le k$, 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≠0 является квадратичным тогда и только тогда, когда

$b^k \equiv 1 \pmod{p}$, $k = \frac{p-1}{2}$ (3)

Доказательство. Необходимость условия (3) 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 (2), единице. Достаточность показывается сложнее. 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

$P(r) \equiv 0 \pmod{p}$, (4)

то (4) 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 $r_0, r_1, \ldots, r_l$, $0 \le r_j < p$, 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 $1 \le j \le l$. 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 делится 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 (4) удовлетворяет k ненулевых квадратичных вычетов. Однако имеется вычет (r = 0), не удовлетворяющий (4); значит, по лемме, все квадратичные невычеты должны не удовлетворять (4) и, следовательно, условие (3) достаточно.

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

Критерий Эйлера позволяет мгновенно решить вопрос о том, для каких p вычет –1 является квадратичным. Подставляя в (3) b = – 1, получаем, что при p = 4l + 1 (3) выполняется (k – четно), а при p = 4l – 1 (3) не выполняется (k – нечетно). Сформулированная выше гипотеза стала теоремой.

Задача 1. Доказать, что если p≠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.

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. Доказательство Эйлера не эффективно в том смысле, что оно не дает явной конструкции для числа n по p, а лишь утверждает его существование. Иными словами, гарантируется, что если перебирать числа 1, 2, …, 2l, возводить их в квадраты, брать остатки от деления квадратов на p, то рано или поздно получится -1. Остается открытым вопрос, нельзя ли указать более явную конструкцию N и p, не использующую процедуры перебора. Положительный ответ дал Лагранж в 1774 году, используя следующую теорему.

Теорема Вильсона. Если p = 2k+1 есть простое число, то

$$(-1)^k(k!)^2 \equiv -1 \pmod{p}. \quad (5)$$

Для доказательства этой теоремы воспользуемся леммой 1. Положим $P(x) = (x^2 - 1)(x^2 - 4)\ldots(x^2 - k^2)$, $Q(x) = x^{2k-1} - 1$. Тогда R(x) = P(x) – Q(x) – многочлен степени не выше 2k – 1, который при x = ±1, ±2, …, ±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 (5).

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

Задача 2. Доказать, что если (5) 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 на p на 8; 2 оказывается квадратичным вычетом для простых $p=8l\pm1$ и невычетом при $p=8l\pm3$ (простое число при делении на 8 может давать остатки ±1, ±3). Далее, 3 является квадратичным вычетом при $p = 12l\pm1$ и квадратичным невычетом при $p = 12l\pm5$. Эйлер высказывает гипотезу, что и в общем случае все определяется остатком от деления p на 4a.

Гипотеза Эйлера. 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 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 выполнялся при a = -1, не действует 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 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 за случаем, продвинувшись дальше других: им рассмотрены a = ±2,±3,±5,±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 остановится 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. Приведем доказательство, мало отличающееся от третьего доказательства Гаусса. В его основе лежит ключевая лемма, доказанная Гауссом не ранее 1808 года.

Лемма2. Пусть p = 2k+1 – простое число, a – целое число, $0<|a|\le 2k$; r_1, r_2, …, r_k – вычеты чисел a, 2a, …, ka; v – число отрицательных среди них. Тогда

$$a^k \equiv (-1)^v \pmod p \quad (6)$$

Применяя критерий Эйлера, получаем такое следствие:

Критерий Гаусса квадратичности вычета. Вычет является квадратичным тогда и только тогда, когда фигурирующее в лемме 2 число v 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: $r_i \pm r_j = (i+j)\,a$, $i \neq j$; $I\,i+j\,I<p$, $IaI<p$. Таким образом, набор модулей $Ir_1I, \ldots, Ir_kI$ – это числа 1,2,…, k в некотором порядке. В результате $a \times 2a \ldots ka = a^k k!$ при делении на p дает тот же остаток, что и $r_1, \ldots, r_k = (-1)^v k!$. Учитывая, что k! не делится на простое число p, получаем (6).

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 (рис. 1, а, б) mp/2, если a>0, и – mp/2, если a<0; m=0,1,2,…, IaI. Занумеруем интервалы с концами в этих точках по номерам левых концов. Отметим теперь крестиками точки a, 2a, …, ka; так как a – целое число, неделящееся на p, то крестики не могут совпасть с ранее отмеченными точками, причем все крестики попадут в какие-то из построенных интервалов (IaIp/2>IaIk). Легко заметить, что фигурирующее в лемме число v – это число крестиков, попавших в интервалы с нечетными номерами.

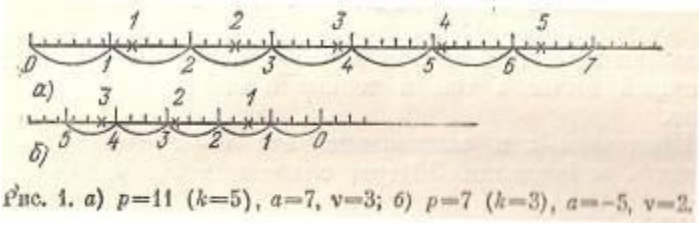


Рис. 1. *а)* $p=11$ $(k=5)$, $a=7$, $v=3$; *б)* $p=7$ $(k=3)$, $a=-5$, $v=2$.

Подвергнем теперь нашу картинку преобразованию подобия с коэффициентом 1/a (рис. 1 перейдет в рис. 2).

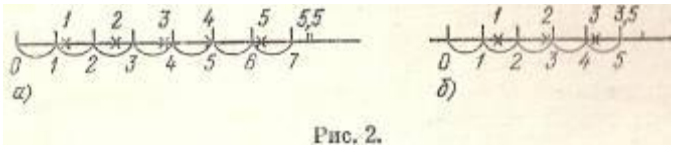


Рис. 2.

При этом точки mp/2 перейдут в точки, делящие отрезок [0, p/2] на IaI равных частей, а крестики – в целочисленные точки 1, 2, …, k.

Нумерация интервалов теперь будет зависеть от знака a: при a>0 они нумеруются номерами левых концов, при a<0 – номерами правых концов; v – 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 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. Итак, при изменении p на p+4al величина v изменится на четное число, а $(-1)^v$ не изменится. Значит, для всех p в арифметической прогрессии p=4aq+r значение $(-1)^v$ – 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 IaI частей, занумеровав их номерами левых (правых концов), если a – положительное (отрицательное); сосчитать число v целых точек, попавших в интервалы с нечетными номерами; a–квадратичный вычет в том и только в том случае, когда v четно.

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

Доказательство. Выполним построения, указанные при доказательстве гипотезы Эйлера для интервалов (0, p/2), (0, q/2), a = (p+q)/4.

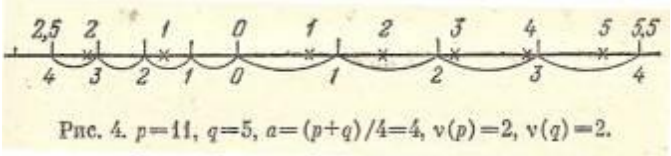


Рис. 4. $p=11$, $q=5$, $a=(p+q)/4=4$, $v(p)=2$, $v(q)=2$.

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. 4). Пусть v(p), v(q) – число целых точек в интервалах с нечетными номерами для p и q соответственно. Нам достаточно доказать, что

v(p)+v(q) – четно. Пусть $v_j(p)$, $v_j(q)$ – число целых точек в соответствующих интервалах с номерами j. Легко видеть, что $v_j(p)+ v_j(q) =2$ 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:

$$\left(\frac{a}{p}\right)=\begin{cases}+1, \text{ если } a\not\equiv 0 \text{ квадратичный} \\ \qquad\qquad \text{вычет по модулю } p, \\ -1, \text{ если } a \text{ — квадратичный невычет.}\end{cases}$$

В силу критерия Эйлера

$$\left(\frac{a}{p}\right)-a^{\frac{p-1}{2}}\equiv 0 \pmod p. \quad (7)$$

Отсюда сразу следует мультипликативное свойство символа Лежандра:

$$\frac{ab}{p}=\frac{a}{p}\frac{b}{p}$$

Отметим также, что символ Лежандра можно доопределить для всех a, не делящихся на p, с сохранением (7), (8), полагая

$$\frac{a+p}{p}=\frac{a}{p}$$

Квадратичный закон взаимности. Если p, q – нечетные простые числа, то

$$\frac{p}{q}\frac{q}{p} = (-1)^{\frac{p-1}{2}\times\frac{q-1}{2}}$$

Другими словами, (p/q) и (q/p) 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.

I случай. Пусть p – q = 4a, т.е. p и q имеют одинаковые остатки при делении на 4. Тогда $\frac{p}{q} = \frac{q+4a}{q} = \frac{4a}{q} = \frac{a}{q}$ (мы воспользовались (9), (8) и тем, что при всех q). Далее, $\frac{q}{p} = \frac{p-4a}{p} = \frac{-4a}{p} = \frac{-1}{p}\frac{a}{p}$. В силу уже доказанной гипотезы Эйлера $\frac{a}{p} = \frac{a}{q}$, т.е. $\frac{p}{q} = \frac{q}{p}$ при $\frac{-1}{p} = 1$ и $\frac{p}{q} = -\frac{q}{p}$ при $\frac{-1}{p} = -1$. Остается вспомнить, что $\frac{-1}{p} = 1$ при p = 4l+1, $\frac{-1}{p} = -1$ при p = 4l+3.

II случай. Пусть p + q = 4a, т.е. p и q имеют разные остатки при делении на 4. Имеем $\frac{p}{a} = \frac{4a-q}{q} = \frac{a}{q}$. Аналогично, $\frac{q}{p} = \frac{a}{p}$. В силу дополнения к гипотезе Эйлера $\frac{a}{q} = \frac{a}{p}$, т.е. $\frac{p}{q} = \frac{q}{p}$. Доказательство окончено.

Нетрудно заметить, что проведенные рассуждения можно обратить и вывести из квадратичного закона взаимности гипотезу Эйлера и дополнение к ней. Отметим еще, что формулы (8) – (10) дают способ вычисления $\frac{p}{q}$ существенно более простой, чем описанный выше комбинаторный способ. Проиллюстрируем это на примере:, т.к. $\frac{3}{59} = -\frac{59}{3} = -\frac{2}{3} = 1$; $\frac{11}{59} = -\frac{59}{11} = -\frac{4}{11} = -1$. Легко показать, что вычисление символа Лежандра всегда можно свести к случаю, когда p или q равно 2.

Место ученого в истории

Гаусс – человек с универсальными математическими способностями; им затрагивались почти все главные отрасли чистой и прикладной математики, причем всюду девизом автора было: panca sed matura (немного, но зрело); он оставил неопубликованными много работ, считая их не достаточно обработанными. Гаусс всегда стремился к оригинальности; затрагивая уже ранее разрабатывавшийся вопрос, казалось, что Гаусс не знаком с предшествовавшими работами, так оригинальны приемы и формы, которые Гаусс придавал изложению. К сожалению, эта оригинальность методы при излишней лаконичности изложения делает многие места сочинений Гаусса весьма трудными для читателя. Замечательная способность Гаусса к числовым выкладкам обнаружилась во многих его работах, о чем свидетельствуют посмертные рукописи.

Многие исследования Гаусс не публиковал при жизни. Они сохранились в виде очерков, набросков, переписки с друзьями. Изучением этих трудов до Второй мировой войны занималось Геттингенское научное общество, которому удалось издать 12 томов сочинений Гаусса. Наиболее интересную часть наследия составляет уже упоминавшийся дневник.

Научное творчество Гаусса наглядно показывает неосновательность деления наук на «чистые» и «прикладные»: «принц математиков» находил практические применения результатам своих фундаментальных исследований и из конкретных задач прикладных областей умел извлекать проблемы, представляющие интерес для фундаментальной науки.

Закончим 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».

Список используемой литературы

1. Башмакова И.Г. Карл Фридрих Гаусс
2. Бюлер В.К. Гаусс. М., 2003
3. Энциклопедия, 2001

Литература

- *Белл Э. Т.* Творцы математики. — М.: Просвещение, 1979. — 256 с.
- *Бюлер В.* Гаусс. Биографическое исследование. М.: Наука, 1989.
- Гаусс К. Ф.: сборник статей под ред. Виноградова (к 100-летию со дня смерти). М.: АН СССР, 1956.
- *Гиндикин С. Г.* Рассказы о физиках и математиках. — издание третье, расширенное. — М.: МЦНМО, 2001. — ISBN 5-900916-83-9
- *Колмогоров А. Н., Юшкевич А. П. (ред.)* Математика XIX века. М.: Наука.
- Башмакова И.Г. Карл Фридрих Гаусс
- Бюлер В.К. Гаусс. М., 2003