Компьютерные инструменты в образовании, 2023
№ -: 2–55
УДК: 621.320
http://ipo.spb.ru/journal
doi:10.1000/182

КОМПЬЮТЕР КАК НОВАЯ РЕАЛЬНОСТЬ МАТЕМАТИКИ: VI. ЧИСЛА ФЕРМА И ИХ РОДСТВЕННИКИ

Н. А. Вавилов
СПбГУ

Аннотация

В этой части, составляющей пандан к части, посвященной числам Мерсенна, я продолжаю обсуждать фантастический прогресс в решении классических задач теории чисел, достигнутый в последние десятилетия с использованием компьютеров. Здесь будет рассказано о проверке простоты, факторизациях и поиске простых делителей чисел специального вида, в первую очередь чисел Ферма, их друзей и родственников, таких как обобщенные числа Ферма, простые Прота и т.д. Кроме того, мы детально обсудим роль чисел Ферма и чисел Пирпойнта в циклотомии.

Ключевые слова: *числа Ферма, обобщенные числа Ферма, числа Прота, числа Пирпойнта, циклотомия*

Цитирование: Н. А. Вавилов Компьютер как новая реальность математики // Компьютерные инструменты в образовании, 2023. № -. С. 2–55 .

Благодарности: *Настоящая статья возникла в процессе работы над грантом РФФИ 19-29-14141.*

Памяти великого мастера компьютерной математики Володи Гердта

1. ВВЕДЕНИЕ

Настоящая статья является непосредственным продолжением [3–7]. В этой части, составляющей пандан к [5], посвященной **числам Мерсенна** $M_p = 2^p - 1$, я продолжу обсуждать роль компьютеров в исследованиях по теории чисел, в первую очередь в факторизация больших чисел *специального вида*, на примере еще одной классической задачи.

• **Гипотеза Ферма.** Доказать, что все **числа Ферма** $F_n = 2^{2^n} + 1$, где $n \in \mathbb{N}$, простые.

Позволю себе повториться: то, что гипотеза Ферма оказалась безнадежно неверна, не делает ее менее великой. Ее роль в развитии теории чисел и алгебры в целом огромна.

Опровержение этой гипотезы, а именно доказательство непростоты числа F_5, составило содержание *первой* работы Леонарда Эйлера по теории чисел — а всего теории чисел Эйлер посвятил после этого около *сотни* статей! Построение правильного

17-угольника, также теснейшим образом связанное с числами Ферма, составило содержание *первой* математической работы Карла Фридриха Гаусса, после которой он окончательно решил посвятить себя математике.

В настоящее время известно 360 простых делителей [составных] чисел Ферма. Из них 16 были открыты в докомпьютерную эпоху за > 300 лет, в среднем примерно один делитель раз в 19 лет. В то же время, за < 70 лет компьютерной эпохи было открыто 344 новых простых делителя, *в среднем* примерно 5 делителей каждый год — хотя, как мы увидим, в действительности этот процесс шел крайне неравномерно. В частности с 1976 года новые простые делители открывали каждый год, кроме ровно одного, 1989. Я предоставляю читателю самому судить, отвечает ли подобный рост наших вычислительных возможностей нашим ожиданиям.

Леонид Шебаршин как-то заметил — вероятно, по другому поводу, но полностью применимо к истории чисел Ферма и их факторизаций — Мы всегда готовы говорить правду. Но как мы ее узнаем? Если говорить о ранней истории, то, кроме нашего обычного источника, “Истории” Диксона [146], совершенно уникальным источником знаний являются Труды Ферма [161–165]. В томе IV содержится история чисел Ферма, доведенная до начала XX века. Подлинной находкой для меня оказалась статья Яна ван Маанена [281], где содержатся точные постраничные ссылки на письма Ферма, на переписку Гольдбаха и Эйлера и на реконструкции вычислений Эйлера.

Огромное количество собранного в одном месте материала представлено в книге Кжижека, Луки и Сомера [260], которую я не знал во время работы над [8] и открыл для себя только в процессе работы над настоящей статьей[1]. Эта книга является неисчерпаемым источником знаний по всем аспектам, связанным с числами Ферма и я советую обращаться непосредственно к ней по поводу дальнейших исторических ссылок. Кроме того, я совершенно не обсуждаю различные приложения чисел Ферма, в частности основанные на них варианты дискретного преобразования Фурье и другие их приложения в теории кодирования и передачи информации.

В рамках одной журнальной статьи невозможно, разумеется, отразить все аспекты связанные с факторизацией обобщенных чисел Ферма $F_n(a,b) = a^{2^n} + b^{2^n}$, проектом Каннингема[2], теоремой Банга—Жигмонди, и всеми остальными аспектами факторизаций сумм и разностей степеней. Поэтому я сосредоточусь в первую очередь собственно на факторизациях числах Ферма и фантастических продвижениях в поиске их простых делителей, полученных в эпоху распределенных вычислений.

Кроме того, я упомяну еще несколько связанных с этим тем, в частности, следующие.

• **Обобщенные числа Ферма** $F_n(a) = a^{2^n} + 1$, среди которых *много* простых и которые, судя по динамике последних лет, имеют все шансы заменить числа Мерсенна в качестве рекордных простых.

• **Числа Прота** $k \cdot 2^m + 1$, $k < 2^m$, которые возникают как делители чисел Ферма и также играют центральную роль в построении рекордных простых и цепочек простых с контролируемыми разностями. Вокруг чисел Прота естественно возникает масса задач рекреативного и учебного характера.

• Роль простых Ферма и **простых Пирпойнта** $2^r \cdot 3^s + 1$ в циклотомии, т. е. вычислении и фактическом геометрическом построении корней соответствующих степеней из 1.

[1] “The book had 3 authors, took 5 years to prepare, consisted of 17 lectures, had 257 pages, and hopefully will make USD 65 537 in royalties”

[2] `https://homes.cerias.purdue.edu/~ssw/cun/index.html`

Как и в предыдущих статьях этой серии, фокус здесь троякий.

• Во-первых, **общекультурный и исторический**, это классические темы, исторически сыгравшие огромную роль в развитии математики, которые могут быть интересны многим математикам, независимо от специальности, и просто образованным любителям. Как и в других случаях, я был *шокирован* состоянием литературы и тем, что большинство текстов общего характера совершенно некритически воспроизводят мифы и измышления 100 или 150-летней давности.

В частности, чисто пропагандистские лекции Клейна школьным учителям [238], посвященные возвеличиванию роли Гаусса лично и математики в Геттингене в целом, при полном игнорировании работ французских, русских и даже прусских математиков, были восприняты последующими поколениями популяризаторов как окончательная истина в вопросе истории циклотомии.

Трудно не согласиться с тем, что говорит по этому поводу ван дер Варден в предисловии к своей книге: “Сколько утверждений в книгах по истории математики списывалось из других подобных же книг без всякой критики и без изучения источников! Сколько находится в обращении побасенок, которые считаются “общепризнанными истинами”! . . . Для того, чтобы избежать подобных ошибок, я неуклонно проверял все утверждения, которые я встречал у современных авторов. Это не так трудно, как кажется, даже если человек (как я) не знает египетского языка, не может читать клинописных текстов и не является филологом-классиком.” [10]

Поэтому я привожу ссылки на источники и воспроизвожу некоторые их фрагменты, достаточные, чтобы квалифицированный читатель мог убедиться в том, что со стандартными версиями далеко не все в порядке. И, кроме того, затрагиваю несколько близких тем, которые, как мне кажется, недостаточно известны, но представляют большой интерес с точки зрения истории и социологии математики.

• Во-вторых, собственно **вычислительный**: я хочу рассказать о том СОВЕРШЕННО НЕВЕРОЯТНОМ ПРОГРЕССЕ, который был достигнут в этой области в последние несколько десятилетий, и, в особенности в последние примерно 20 лет, связан не просто с ролью компьютера, но с растущей популярностью ПРОЕКТОВ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛЕНИЙ таких, как `PrimeGrid`.

• В-третьих, **педагогический**: это, разумеется, та роль, которую эти темы могут играть в преподавании математики. Я здесь привожу несколько задач такого типа как мы фактически использовали в классе, см. [8] и описание всего проекта в [9]. Ясно, что простор для творчества здесь огромный. Эти задачи легко формулируются, исторически мотивированы, вызывают естественное любопытство, непосредственно связаны со школьным курсом математики, легко программируются, и в то же время открыты в сторону серьезной профессиональной математики.

Здесь, как и в работах [4–6] и, в особенности, в [7], я не делаю *никакой* попытки дать *систематический* обзор литературы — более того, в том, что касается обобщенных чисел Ферма и дальнейших вариаций на эту тему, это было бы невозможно в рамках журнальной статьи. Столь же нереально было бы и полностью задокументировать историю поиска сотен известных простых делителей самих чисел Ферма, это также предполагало бы совершенно другой формат (и другую вовлеченность!).

Поэтому, как и в предыдущих статьях серии, я ограничиваюсь ссылками на 1) классические результаты, 2) несколько фундаментальных монографий и обзоров, 3) статьи, в которых представлены результаты компьютерных вычислений, 4) некоторые

статьи элементарного и *алгебраического* характера, которые мы использовали при составления задач для студентов.

2. ГИПОТЕЗА ФЕРМА О ЧИСЛАХ ФЕРМА

Совершенно ясно, что теория чисел, как мы ее знаем, основана одним человеком, Пьером де Ферма. Вот что пишет по этому поводу Андре Вейль [395]: “Fermat is one of the most fascinating mathematical personalities of all times, the creator (with Descartes) of analytic geometry, one of the founders of the calculus, the undisputed founder of modern number theory. The aura of mystery that still surrounds some of his best work provides an added attraction.“

2.1. Исходная формулировка гипотезы о числах Ферма

Начнем со следующего незамысловатого наблюдения, которое Ферма сделал в переписке с Бернаром Френиклем.

Задача. Проверьте (или докажите!), что если $2^m + 1$, где $m \in \mathbb{N}$, простое, то $m = 2^n$, $n \in \mathbb{N}_0$.

Число вида $F_n = 2^{2^n} + 1$, где $n \in \mathbb{N}_0$, называется **числом Ферма**. Числа Ферма возникают в самых различных вопросах теории чисел, комбинаторики, алгебры и геометрии.

В письме Френиклю Ферма *высказал предположение*, что **все** числа Ферма F_n простые, но смог проверить лишь, что

$$F_0 = 3, \qquad F_1 = 5, \qquad F_2 = 17, \qquad F_3 = 257, \qquad F_4 = 65537$$

просты. Фрагменты всех писем Ферма на эту тему, которые я смог найти, воспроизведены ниже. Все письма цитируются по Œuvres de Fermat, том 2, [162][3].

• Вот исторически первая формулировка гипотезы Ферма в письме XLIII Френиклю, предположительно август 1640 года, [162], p. 206:

“Mais voici ce que j’admire le plus: c’est que je suis quasi persuadé que tous les nombres progressifs augmentés de l’unité, desquels les exposants sont des nombres de la progression double, sont nombres premiers, comme

$$3, \quad 5, \quad 17, \quad 257, \quad 65537, \quad 4\,294\,967\,297$$

et le suivant de 20 lettres

$$18\,446\,744\,073\,709\,551\,617; \qquad \text{etc.}$$

Je n’en ai pas la démonstration exacte, mais j’ai exclu si grande quantité de diviseurs par démonstrations infaillibles, et j’ai de si grandes lumières, qui établissent ma pensée, que j’aurois peine à me dédire.”

Многие заявляют, что Ферма, якобы, утверждал простоту чисел Ферма как факт. В действительности, он прямо говорит, что он **почти** убежден (= “quasi persuadé”) в этом,

[3] Вот, что пишет по поводу этого издания Андре Вейль: “Fermat’s complete writings and correspondence have been excellently published by Ch. Henry and P. Tannery in four splendid volumes (Gauthier Villars, Paris, 1891–1912, with a supplementary volume, ibid., 1922); this includes authoritative French translations of all Latin texts, valuable commentaries, and virtually all relevant passages from the writings and correspondence of Fermat ’s contemporaries”, [395]. I cannot agree more!

хотя у него нет никакого точного доказательства (= “je n’en ai pas la démonstration exacte”)[4].

И в дальнейших его письмах я вижу только, что ему *очень хотелось бы*, чтобы это было правдой, ему *очень важно*, чтобы это было правдой, потому что из этого ВЫТЕКАЛИ БЫ ОЧЕНЬ ВАЖНЫЕ СЛЕДСТВИЯ, и что эта мысль его настолько *воодушевляет*, что ему было бы трудно от нее отказаться.

Почему Ферма так хотелось, чтобы это было правдой, тоже совершенно понятно.

• Во-первых, он хотел иметь *формулу*, которая позволяет строить простые числа, большие любого наперед заданного числа. Конечно, мы все *верим*, что такие числа существуют, но видеть мы их никогда не видели. Идея *предъявить* такие числа казалась Ферма очень привлекательной.

• Во-вторых, он, очевидно интересовался *обращением* **малой теоремы Ферма**. Ему хотелось получить удобный **тест простоты**. Но, к сожалению, он, скорее всего, не знал еще теорему Корсельта[5] об **абсолютно псевдопростых** числах [в смысле Ферма] — то, что теперь принято называть **числами Кармайкла** — т. е. *составных* числах n таких, что

$$a^n \equiv a \pmod{n}, \qquad \text{для всех } a.$$

Как хорошо известно, первые два числа Кармайкла, это $561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$. Кстати, весьма символично[6] что 1729 — номер года, когда Гольдбах привлек внимание Эйлера к задаче Ферма, — тоже число Кармайкла[7], $1729 = 7 \cdot 13 \cdot 19$.

• В третьих, он рассчитывал на дальнейшие обобщения, связанные с явными критериями простоты для **обобщенных чисел Ферма** — и явно упоминал это в своих письмах!

Задача. Подтвердите или опровергните утверждение Ферма.

Ответ. Приведенные выше пять чисел являются *единственными* известными сегодня простыми числами Ферма! В действительности, как установил Эйлер, F_5 делится на 641.

[4] Вот Мерсенн на странице 181 “Novarum observationum” похоже действительно формулирует простоту чисел Ферма как факт, or so it seems: “Deinde, quilibet numerus analogiæ binariæ, plus 1, exponentem eiusdem analogiæ habens, primus est; ita siquidem 256, cuius exponens 8, plus 1, dat 257 primum.”

[5] Опубликованный в 1899 году **критерий Корсельта** состоит в следующем: составное натуральное число n в том и только том случае удовлетворяет сравнению $a^{n-1} \equiv 1 \pmod{n}$ для всех a взаимно простых с n, когда n бесквадратное и $p-1$ делит $n-1$, для всех его простых делителей p. Сам Арвин Рейнгольт Корсельт, 1864–1947, был школьным учителем вначале в Дрездене и других городах восточной Германии, потом большую часть жизни в Плауэне. Притом даже не в гимназии, а в Realschule! Что я могу сказать, *безмерно* крутые школьные учителя математики были в XIX веке не только в Германии, но и по всей Европе. И кому все это мешало?

[6] Такого рода совпадения безумно любил Освальд Шпенглер. Он построил целую теорию на основе того, что три величайших европейских — “фаустовских” — композитора, Иоганн Себастьян Бах, Георг Фридрих Гендель и Доменико Скарлатти, родились в один год, 1685. Не помню, кстати, упоминает ли он в этой связи Лодовико Джустини? Для полной симметрии следовало. Жан-Филипп Рамо со своим 1683 годом, конечно, чуть промахнулся, но на это у Шпенглера тоже есть объяснение.

[7] Кроме того, это, конечно, **число Рамануджана** — хотя в данном случае правильнее говорить **число Френикля де Бесси**, который в 1657 году заметил, что 1729 — наименьшее число, представимое как сумма двух кубов натуральных чисел двумя существенно различными способами, $1729 = 1^3 + 12^3 = 9^3 + 10^3$, near miss для теоремы Ферма. Уму непостижимо, как Харди мог этого не помнить: “I remember once going to see him when he was ill at Putney. I had ridden in taxi cab number 1729 and remarked that the number seemed to me rather a dull one”, [32].

2.2. Числа Ферма в переписке Ферма

В своих письмах Ферма несколько раз на протяжении двух десятилетий реитерировал эту гипотезу именно как ГИПОТЕЗУ, в справедливость которой он *очень* хотел бы верить, но КОТОРУЮ ОН НЕ МОЖЕТ ДОКАЗАТЬ.

• Письмо XLIV Френикю от четверга 18 ноября 1640 года, ibid., p.207–208:

“Mais je vous avoue tout net (car par avance je vous averti que, comme je ne suis pas capable de m’attrbuer plus que je ne sais, je dis avec même franchise ce que je ne sais pas) que je n’ai pu encore démontrer l’exclusion de tous diviseurs en cette belle proposition que je vous envoyée et que vous m’aves confirmée, touchant les nombres 3, 5, 17, 257, 65537, etc. Car, bien que je réduise l’exclusion à la plupart des nombres et que j’aie même des raisons probables pour le reste, je n’ai pu encore démontrer nécessairment la verité de cette proposition, de laquelle pourtant je ne doute non plus à cette heure que je faisois auparavant. Si vous en avez la preuve assurée, vous m’obligerez de la communiquer; car, aprés cela, rien ne m’arrètera en ces matières.”

• Письмо XLV Марену Мерсенну от вторника 25 декабря 1640 года, ibid., c.212–213:

“. . . voici trois questions que je lui propose, pource que les spéculations que j’y ai faites ne me satisfont pas pleinement: 1^0 La raison essentielle pourquoi 3, 5, 17, 257, etc. à l’infini, sont toujours nombres premiers.”

Он тут же поясняет, почему это ему так важно! В этом случае для любого четного q все числа вида $q^{2^n}+1$, кроме тех, которые делятся на 3, 5, 17, 257, etc., будут простыми — “laquelle proposition, *si elle est vraie*, est de très grand usage.” Он продолжает:

“Si je puis une fois tenir la raison fondamentale que 3, 5, 17, etc. sont nombres premiers, il me semble que je trouverai de très belles choses en cette matière, car déjà j’ai trouvé des choses merveilleuses dont je vous ferai part,. . . ”

• Письмо LXXIII Блезу Паскалю от субботы 29 августа 1654 года, ibid. c.309–310:

“Songez cependant, si vous le trouvez à propos, à cette proposition: Les puissances quarrées de 2, augmentées de l’unité, sont toujours des nombres premiers.. . . Et ainsi à l’infini. C’est une propriété de la vérité de laquelle je vous réponds. La démonstration en est très malaisée et je vous avoue que je n’ai pu encore la trouver pleinement; je ne vous la proposerois pas pour la chercher, se j’en étois venu à bout.”

• В письме Кенельму Дигби, письмо XCVI, ibid. p.402–403 (само письмо не датировано, но Дигби переслал его Джону Валлису 16 июня 1658 года) Ферма реитерирует вопрос как вызов английским математикам:

“1^0 Potestates omnes numeri 2, quarum exponentes sunt termini progressionis geometricæ ejusdem numeri 2, unitate auctae, sunt numeri primi.”

Он комментирует: “Sed ingenuitatem gallicam sapient magis propositiones aliquot quarum demonstrationem a nobis ignorari non diffitemur, licet de earum veritate nobis constet. . . . Quaeritur demonstratio illius propositionis, . . . ” = “. . . мы не будем отрицать, что нам [здесь он говорит от имени французских математиков] неизвестно доказательство . . . предлагается найти доказательство этих утверждений . . . ”

• В письме Пьеру Каркави, письмо CI, август 1659 года, ibid. 433–434. Ферма мельком высказывает надежду, что теперь *наконец-то* сможет решить эту задачу методом бесконечного спуска.

Чрезвычайно интересно, что хотя Ферма высказывал эту гипотезу в письмах всем своим основным корреспондентам, он нигде не упоминает ее в своих примечаниях к Диофанту!

2.3. Числа Ферма в переписке Гольдбаха и Эйлера

Эйлер в своих первых работах по теории чисел шел буквально по следам Ферма, давая полные доказательства теорем, сформулированных Ферма. Вот что пишет по этому поводу Андре Вейль: “while Fermat was far ahead of the few who were also interested in number theory during his lifetime, and owed nothing to them, most of the work of Euler in that field may be regarded as an inspired commentary on the work of Fermat”, [395].

Вот более развернутый комментарий Франца Леммермайера на ту же тему, в котором особо подчеркивается именно проблема Ферма о простоте чисел Ферма и роль Гольдбаха: “Even more important for defining Euler’s mathematical interests was Goldbach’s fascination with number-theoretic problems. Goldbach’s innocent question whether Euler knew of Fermat’s claim that all numbers of the form $2^{2^n}+1$ are prime eventually made Euler study everything by Fermat he could lay his hands on. Euler’s contemporaries, first of all the Bernoullis, remained indifferent to this aspect of Euler’s research, leaving Goldbach as virtually the only person with whom Euler could discuss such topics until, towards the end of Euler’s life and after Goldbach’s death, Lagrange entered the stage”, [156], c.27.

Как отмечается в литературе, в переписке Эйлера и Гольдбаха проблема простоты чисел Ферма непосредственно *обсуждается* в шести[8] письмах (и *упоминается* еще в нескольких). Вот соответствующие фрагменты этих писем[9].

• Вот судьбоносный постскриптум *первого* письма Гольдбаха Эйлеру (Письмо I, Москва, 1 декабря 1729 года, с.10):

“Notane Tibi est Fermatii observatio omnes numeros huius formulae $2^{2^{x-1}}+1$, nempe 3,5,17, &c. esse primos, quam tamen ipse fatebatur se demonstrare non posse et post eum nemo, quod sciam, demonstravit.” = “Знаешь ли Ты наблюдение Ферма, что все числа вида $2^{2^{x-1}}+1$, а именно 3, 5, 17 и так далее, простые? Он сам признавался, что не мог этого доказать и, насколько мне известно, и потом никто не доказал.”

Считается, что сам Гольдбах узнал об этой гипотезе из переписки Валлиса *Commercium Epistolicum* (1658), где на странице 186 воспроизведено письмо Ферма Кенельму Дигби от июня 1658 года. Или, возможно, из трудов Валлиса, *Opera*, vol. III, 1699.

• Эйлер отвечает (Письмо III, Петрополь, 8 января 1730 года, с.18):

“Nihil prorsus invenire potui, quod ad Fermatianam observationem spectaret. Sed nondum prorsus persuasus sum, quomodo sola inductione id inferre legitime potuerit, cum certus sim

[8] https://edoc.unibas.ch/58842/2/IVA4_PDFA.pdf

[9] При подготовке предыдущих статей серии в качестве источника я пользовался главным образом изданием Фукса, как наиболее ранним. Однако в настоящее время по *практическим* соображением перешел на базельское издание [156, 157] под редакцией Франца Лемермайера и Мартина Маттмюллера — HABENT SUA FATA EDITIONES. Оно полнее, лучше аннотировано и содержит много дополнительных материалов. Наличие английского перевода может быть полезным тем, кто не знает немецкого и латыни, “Since the languages used (18th-century German and Latin) are no longer universally familiar to scholars and students of either mathematics or history, it seemed advisable to complement the source text by an English translation”. Не скрою, однако, что мысль о возможности заниматься историей математики без знания этих языков оказалась для меня совершенно новой. Я, скорее согласен с мнением самих редакторов, что написанный на пиджине — “peculiar mixture of 18th century German and Latin” — текст Эйлера и Гольдбаха ПОНЯТЕН ДО СЛОВА as is: “Actually Euler and Goldbach express themselves clearly and most of the time simply, so there has only rarely been any doubt in the editors’ minds what the original text intends to say.”

ipsum numeris in formula 2^{2^x} loco x substituendis nec ad senarium quidem pervenisse." = "В отношении наблюдения Ферма я не смог вообще ничего придумать. Я однако полностью убежден, что придти к этому одной лишь индукцией невозможно, так как подставляя значения x в 2^{2^x} он, несомненно, не дошел даже до шестого из них."

• Ответ Гольдбаха содержит обширный фрагмент на эту тему, в котором, в частности, упоминается малая теорема Ферма (Письмо IV, Москва, 11 мая 1930 года):

"Quod ad Fermatii observationem attinet, tecum sentio, non credibile videri, eum ad sex terminos illius suae seriei exprimendos progressum fuisse, neque tanto labore opus est ad verisimilitudinem illius observationis, facile enim experimur divisore quocunque accepto residua ex terminis ordine quo sequuntur divisis in circulum redire."

• Эйлер отвечает (Письмо V, Петрополь, 4 июня 1730 года):

"Postquam ultimas ad Te misissem literas, de Theoremate Fermatiano diligentius cogitare coepi, idque non tam levi nixum fundamento, quam primum putaveram, perspexi."

Там же Эйлер начинает рассматривать более общий вопрос о делителях чисел вида $a^n + b^n$, потом эту тему продолжает Гольдбах в своем ответе (Письмо VI, Москва, 15 июня 1730 года).

• Следующее письмо Эйлера снова начинается с обширного фрагмента о числах Ферма (Письмо VII, Петрополь, 25 июня 1930 года):

"Theorematis Fermatiani veritas quotidie mihi magis elucere videtur; sed tamen demonstrationem ejus nondum sum nactus. Sunt mihi autem nonnullae ejus inventae proprietates, quae fortasse ad demonstrationem conficiendam utiles esse possent. Fiat series, cujus terminus generalis est $2^{2^{x-1}} + 1$, sequens 3, 5, 17, 257, etc., cujus singuli termini secundum Fermatium sunt numeri primi. Demonstrare autem possum, nullum terminum per quemquam praecedentium dividi posse, et praeterea si quis terminus haberet divisorem, sequentium nullum per eundem dividi posse, sed semper residuum fore 2. Certum igitur ex hoc est, omnes ejus progressionis terminos inter se esse primos, vel duos reperiri non posse, qui communem habeant divisorem."

• А вот пример из позднейшей переписки. В части, посвященной проблеме Варинга [4], мы уже цитировали письмо LI от 27 мая 1742 года: "Des Fermatii Einfall daß jeder numerus $2^{2^{n-1}} + 1$ eine seriem numerorum primorum gebe, kan zwar, wie Ew. H. bereits gezeiget haben, nicht bestehen. . . "

3. ПРОСТОТА ЧИСЕЛ ФЕРМА

В действительности в 1732 году Эйлер нашел разложение на множители следующего числа Ферма:

$$F_5 = 4294967297 = 641 \cdot 6700417 = (5 \cdot 2^7 + 1) \cdot (52347 \cdot 2^7 + 1),$$

и сейчас мы реконструируем, как именно он это сделал.

3.1. Критерий Пепана и критерий Люка—Эйлера

Оказывается, узнать, является ли число Ферма F_n простым, совсем просто и не предъявляя никаких его собственных делителей. Например, сегодня мы не знаем

никаких простых делителей чисел Ферма F_{20}, F_{24} и многих других[10]. В то же время известно, что эти числа не являются простыми.

Это устанавливается при помощи следующего легко проверяемого теста, который в 1878 году доказал, развивая идею Люка, Теофиль Пепан[11,12], [304].

Критерий Пепана. Для того, чтобы число Ферма F_n, $n \geq 2$, было простым, необходимо и достаточно, чтобы

$$5^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

Однако, как было тогда же замечено, 5 здесь можно заменить на любой квадратичный невычет по модулю F_n, см. [146], так что сегодня в большинстве учебников критерий Пепана формулируется следующим образом.

Критерий Пепана. Для того, чтобы число Ферма F_n, $n \geq 1$, было простым, необходимо и достаточно, чтобы

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

В статье Олега Василенко [11] приведено совсем простое доказательство критерия Пепана с заменой 5 на 7, использующее квадратичный закон взаимности, а также обсуждаются аналогичные критерии, в которых в качестве оснований берутся другие числа Ферма, числа Мерсенна и т.д.

В действительности первый критерий такого типа был предложен Эдуаром Люка[13], как обращение малой теоремы Ферма. Пусть $n \geq 3$ нечетно и существует a, $1 < a < n$, такое, что $a^{n-1} \equiv 1 \mod n$. Если для любого простого q, делящего n, выполняется сравнение

$$a^{\frac{n-1}{q}} \not\equiv 1 \pmod{n},$$

то n простое.

Задача. Проверьте, что числа F_n, $n = 10, \ldots, 15$, не являются простыми.

Указание. Непосредственно возвести 3, 5 или 7 в степень такого порядка нет шансов, поэтому используйте функцию `PowerMod`. Посмотрите, какой остаток она возвращает и аккуратно сформулируйте условие!

Как мы уже упоминали, опровержение гипотезы Ферма — это вообще *первая* арифметическая работа Эйлера [154], которая, вероятно, и стимулировала его интерес к теории чисел. Не следует думать, что Эйлер настолько любил считать, чтобы делить вручную 10-значное число на все простые подряд, пока *случайно* не наткнулся на делитель 641. В действительности, ему пришлось для этого выполнить всего три–четыре деления, а, скорее всего, ни одного.

[10] В тот момент, когда мы писали [8], не было известно также ни одного простого делителя чисел F_{14} и F_{22}, они были найдены только в 2010 году!

[11] Жан Франсуа Теофиль Пепан, 1826–1904, вступил в орден иезуитов в возрасте 20 лет, некоторое время преподавал математику в иезуитских колледжах, после чего стал профессором канонического права в Лионе, а потом Риме. Кроме теста Пепана известно еще несколько его результатов, в частности, новое доказательство теоремы Ламе об отсутствии нетривиальных решений у уравнения Ферма $x^7 + y^7 = z^7$. Его официальный некролог в “Atti della Pontificia Accademia Romana dei Nuovi Lincei”, **58** (1905), 210–216, упоминает 52 его публикации, большей частью относящиеся к теории чисел.

[12] Обычно по-русски пишут “Пепин”, но это представляется мне совсем абсурдным. Если в этой фамилии по-французски где и звучит “и”, то скорее в первом слоге, “Пипан”.

[13] Эдуар Люка, 1842–1891, несомненно один из самых интересных теоретико-числовиков XIX века. При этом он не был университетским профессором. Вынужденный уйти из обсерватории в результате конфликта с Ле Веррье, он поработал в школах в Туре и Мулене, после чего, все-таки, вернулся в Париж, где преподавал в Lycée Charlemagne и Lycée Saint-Louis. Да, безмерно крутые школьные учителя были в XIX веке.

Реконструируем рассуждения Эйлера, чтобы читатель мог на этом *игрушечном* примере представить, при помощи каких примерно соображений ищутся простые делители у чисел, содержащих многие сотни или тысячи десятичных знаков, ЕСЛИ ИЗВЕСТНА ИХ СТРУКТУРА.

В [154] Эйлер не говорит, как он это сделал, но [155] дает возможность восстановить детали. Дело в том, что для того, чтобы разложить число Ферма F_n на множители, достаточно проверять не все простые $p \le \sqrt{F_n}$, а лишь простые вида $p = k \cdot 2^{n+2} + 1$, где $m \in \mathbb{N}$. Это вытекает из следующего легко проверяемого соображения,

Критерий Эйлера—Люка. Любой простой делитель числа F_n, $n \ge 3$, имеет вид $k \cdot 2^{n+2} + 1$, для некоторого $k \in \mathbb{N}$.

Этот критерий доказан Люка, сам Эйлер утверждал лишь, что делители имеют вид $k \cdot 2^{n+1} + 1$, в такой форме это очевидно.

Задача. Докажите критерий Эйлера.

Решение. Пусть p — простой делитель числа $F_n = 2^{2^n} + 1$, он нечетен. Тогда по малой теореме Ферма p делит $2^p - 1$. С другой стороны, по предположению p делит

$$2^{2^{n+1}} - 1 = \left(2^{2^n} - 1\right) \cdot \left(2^{2^n} + 1\right).$$

Так как $2^{2^n} - 1$ не может делиться на p, то $d = 2^{n+1}$ является наименьшим показателем степени таким, что $2^d - 1$ делится на p и, значит, $p - 1 = kd$ для некоторого k.

В действительности Эйлер утверждает даже, что сумма двух степеней $a^{2^n} + b^{2^n}$, в которой показатели степени являются степенями двойки, не имеет никаких делителей, кроме делителей вида $k \cdot 2^{n+1} + 1$.

В силу этого критерия делителями числа Ферма F_5 могут быть только простые числа вида $p = k \cdot 2^7 + 1$. Первые два таких числа, это $p = 257$ и $p = 641$, которые получаются при $k = 2$ и $k = 5$, соответственно. Очевидно, что 257 взаимно просто с F_5, поэтому нужно проверять лишь 641. Если Эйлер пользовался более слабым критерием из [155], согласно которому простые делители имеют вид $p = k \cdot 2^6 + 1$, ему нужно было бы еще проверить 193, 449 и 577, но даже и в этом случае он нашел бы 641 в результате четвертого деления (раньше, если смотреть на наибольшие общие делители!).

Однако вероятно, ему не пришлось делать даже этого. В самом деле, очевидно, что $641 = 2^4 + 5^4$ делит $a = 2^{32} + 2^{28}5^4$. С другой стороны, применяя формулу для разности квадратов, мы видим, что $641 = 5 \cdot 2^7 + 1$ делит $b = 2^{28}5^4 - 1$. Таким образом, 641 делит и разность этих чисел $F_5 = a - b$.

Для того, чтобы проверить, будет ли 6700417 простым, достаточно, *в худшем случае*, произвести еще не более 4 делений, а именно, проверить, что оно не делится на простые числа вида $p = k \cdot 2^7 + 1$, $5 \le k \le 20$, каковых, очевидно (см. таблицу простых) ровно 4, а именно, 641, 769, 1153, 1409.

Однако, зная Эйлера, можно предположить, что он, скорее всего, и здесь обошелся вообще без явных вычислений, а придумал что-то в таком же духе. Экстраполируя этот пример, мы видим, что ОДИН ИЗОБРЕТАТЕЛЬНЫЙ МАТЕМАТИК МОЖЕТ С УСПЕХОМ ЗАМЕНИТЬ *сотни* ВЫЧИСЛИТЕЛЕЙ — *два* изобретательных математика заменяют небольшой компьютер.

На самом деле, далеко не все простые числа $k \cdot 2^n + 1$ могут быть делителями чисел Ферма. Например, Морхед [292] заметил, что из кубического закона взаимности вытекает, что ни одно простое вида $3 \cdot 2^n + 1$ не может быть делителем чисел Ферма.

В статье [152] Фриман Дайсон показывает, как факторизовать шестое число Ферма в таком же элементарном духе, ВООБЩЕ БЕЗ ВЫЧИСЛЕНИЙ. А именно, он объясняет, почему F_6 делится на 274177.

Делькур [139] упоминает еще одно забавное приложение того, что числа Ферма F_5, F_6, F_7 не являются простыми, а именно, доказывает, что уравнение $\phi(x) = 2^n$ имеет $n+2$ решения при $n \le 31$ и всего 32 решения — а не 33, как утверждал Кармайкл — при $32 \le n \le 255$.

3.2. Классические ослабления гипотезы Ферма.

В 1844 году Эйзенштейн высказал следующее предположение, которое, в отличие от исходной гипотезы Ферма, до сих пор не доказано и не опровергнуто.

• **Гипотеза Эйзенштейна.** Существует бесконечно много простых чисел Ферма.

Харди и Райт [208], с. 14, приводят правдоподобные соображения в пользу того, что ответ на гипотезу Эйзенштейна тоже отрицательный, иными словами, количество простых чисел Ферма конечно. Недавно Боклан и Конвей [83] предложили совершенно подавляющие свидетельства в пользу того, что никаких простых чисел Ферма, кроме пяти известных самому Ферма, не существует.

В 1963 Анджей Шинцель высказал следующее более слабое предположение, которое имеет все шансы быть верным.

• **Гипотеза Шинцеля.** Существует бесконечно много бесквадратных чисел Ферма (т.е. таких, которые являются произведениями различных простых).

Заметим, что числа Ферма дают еще один подход к доказательству теоремы Эвклида бесконечности числа простых. В самом деле, из следующей задачи — взятой непосредственно из переписки Гольдбаха и Эйлера[14] — вытекает, что числа Ферма попарно взаимно просты. Вот, что пишет Гольдбах (письмо VIII, Москва 20 июня 1730):

“Jam diu animadverti numerum $2^{2^{x+p}}+1$, ubi x et p sint numeri integri, divisum per $2^{2^x}+1$, relinquere 2, propterea quod $\left(2^{2^x}+1\right)\left(2^{2^x}+1\right)$ est $= 2^{2^{x+1}}-1$, rursus $\left(2^{2^{x+1}}+1\right)\left(2^{2^{x+1}}+1\right)$ est $= 2^{2^{x+2}}-1$, et sic porro, donec perveniatur ad $\left(2^{2^{x+p}}-1\right)$, qui numerus binario minor est quam $2^{2^{x+p}}+1$; ex eo quidem certe sequitur omnes numeros seriei Fermatianae esse inter se primos, ut dicis; at quantulum hoc est ad demonstrandum omnes illos numeros esse absolute primos?” = “Я уже довольно давно заметил, что при делении на $2^{2^x}+1$ числа $2^{2^{x+p}}+1$, где x и p целые, дают остаток 2, потому что . . . ; отсюда, разумеется, сразу следует, что числа Ферма взаимно просты, как Ты и говоришь; но что это нам дает для доказательства того, что все эти числа сами простые?”

Задача. Проверьте (или докажите!), что

$$F_0 F_1 F_2 \dots F_n = F_{n+1} - 2.$$

Таким образом, если F_m делит F_n, при некотором $n > m$, то F_m делит 2, что невозможно.

[14] Доказательство, основанное на той же идее, но при этом содержащее несколько ЧРЕЗВЫЧАЙНО УДАЧНЫХ УХУДШЕНИЙ, воспроизводится в книге “Задачи и теоремы из анализа”, поэтому некоторые авторы *ошибочно* приписывают его Пойа и Сеге.

4. ФАКТОРИЗАЦИИ ЧИСЕЛ ФЕРМА

Несмотря на столь простой критерий для формы простых делителей, *единственными* числами Ферма, которые сегодня полностью разложены на простые множители, являются F_5, F_6, которые были факторизованы в XVIII–XIX веках, и $F_7, F_8, F_9, F_{10}, F_{11}$, которые были полностью факторизованы лишь в компьютерную эпоху.

• Число F_6 тоже довольно легко раскладывается на множители от руки:

$$F_6 = 18446744073709551617 = 274177 \cdot 67280421310721 = (1071 \cdot 2^8 + 1) \cdot (262814145745 \cdot 2^8 + 1).$$

В это большинстве классических книг по теории чисел утверждается, что это разложение было найдено в 1880 году Ландри [267] и Ле Лассером. Однако в 1964 году Курт-Р. Бирманн[15] обнаружил, что что Томас Клаузен[16] привел эту факторизацию в письме к Гауссу, датированном 1 января 1855 года, и что он знал, что оба множителя простые, [76]. Более того, второй из них был самым большим известным на тот момент простым числом! Вот это место из письма Клаузена: “Auch habe ich gefunden, daß die Zahl $2^{64} + 1$ in die beiden Primfactoren 274177 und 67280421310721 zerlegt werden kann; die letztere ist, so viel ich weiß, die großte bis jetzt bekannte Primzahl.”

А вот полностью разложить на множители дальнейшие числа Ферма в докомпьютерную эпоху не было *никакой* возможности. Как мы сейчас увидим, на полную факторизацию одного числа Ферма у человечества уходило примерно 10 лет, начиная с 1970 года, причем после 2000 года прогресс *замедлился*.

Еще в начале XX века Морхед и Вестерн показали, что числа F_7 и F_8 составные, в 1954 году это еще раз проверил на компьютере Робинсон [328]. Тем не менее, предъявить ни одного их простого делителя довольно долго не удавалось.

• В действительности, разложение F_7 было найдено лишь в 1970 году(!!) Моррисоном и Бриллхартом [295]:

$$F_7 = 59649589127497217 \cdot 5704689200685129054721 = \\ (116503103764643 \cdot 2^9 + 1) \cdot (11141971095088142685 \cdot 2^9 + 1).$$

Таким образом, между полной факторизацией F_6 и полной факторизацией F_7 прошло 115 лет!

[15] Курт-Райнхарт Бирманн, 1919—2002, “der Nestor der deutschen Mathematikhistoriographie”, тот самый Бирман, которого все мы знаем по новой публикации дневников Гаусса [182]. Он обнаружил и вовлек в оборот многие десятки неизвестных до этого документов по истории математики XIX века. До 1949 года он был в советском плену, впоследствии работал в Академии Наук ГДР и публиковал довольно много статей на русском.

[16] Томас Клаузен, 1801–1885, был сыном крестьянина из Шлезвига [ныне Дания] и в 1813 году еще не умел читать и писать. Не имея формального университетского диплома, основное образование получил в Германии, между Гамбургом и Мюнхеном, ключевую роль в этом сыграл Шумахер. Начиная с 1842 года Клаузен работал в России, в обсерватории Дерпта [ныне Эстония], в 1856 году был избран членом-корреспондентом Петербургской Академии Наук, в 1865 году стал профессором, а потом директором обсерватории. Удивительный XIX век, одна из абсолютных вершин развития человечества. Как хорошо известно, классик синтетической геометрии Якоб Штейнер, 1796–1863, тоже был сыном крестьянина и научился читать в 14 лет. А в 1832 году заботами Якоби получил степень университета Кенигсберга [ныне Россия] и вскоре после этого стал профессором геометрии в Берлине.

• Следующее число F_8, было факторизовано еще на 10 лет позже, в 1980 году Брентом и Поллардом [95], *ровно* через 100 лет после *второй* факторизации F_6:

$$F_8 = 1238926361552897\cdot$$
$$93461639715357977769163558199606896584051237541638188580280321 =$$
$$(604944512477\cdot 2^{11}+1)\cdot$$
$$(45635566267264637582599393652151804972681268330878021767715\cdot 2^{11}+1).$$

Приятно, что *сегодня* это разложение за секунды ищется на бытовом компьютере при помощи функции `FactorIntegerECM`, использующей эллиптические кривые.

Задача. А теперь напишите *от руки* программу, раскладывающую числа F_6, F_7 и F_8 на множители быстрее, чем это делает внутренняя команда `FactorInteger`.

Однако в этот момент шутки кончились. Дальше начинается серьезная профессиональная математика серьезных профессиональных математиков.

• Что касается F_9, то еще в 1903 году Вестерн обнаружил, что оно делится на $37\cdot 2^{16}+1 = 2424833$. Несмотря на это, полная факторизация F_9 на множители была получена лишь в 1990 году Ленстрой, Ленстрой, Манассе и Поллардом [276]. При этом оказалось, что два других делителя числа F_9 содержат 49 и 99 цифр, соответственно:

$$F_9 = 2424833\cdot 7455602825647884208337395736200454918783366342657\cdot P99 =$$
$$(37\cdot 2^{16}+1)\cdot([46\text{ цифр}]\cdot 2^{11}+1)\cdot([96\text{ цифр}]\cdot 2^{11}+1).$$

Единственными другими числами Ферма, которые сегодня *полностью* разложены на простые множители, являются F_{10} и F_{11}.

• Факторизация F_{10} была завершена в 1999 году в работе Брента [93]:

$$F_{10} = 45592577\cdot 6487031809\cdot 4659775785220018543264560743076778192897\cdot P252 =$$
$$(11131\cdot 2^{12}+1)\cdot(395937\cdot 2^{14}+1)\cdot([37\text{ цифр}]\cdot 2^{12}+1)\cdot([248\text{ цифр}]\cdot 2^{13}+1).$$

• Интересно, что хотя само число F_{11} значительно больше, чем F_{10}, его факторизация оказалась заметно проще, она была завершена уже в 1988 году Брентом и Морэном, [90], т.е. еще до факторизации не только F_{10}, но и F_9! Это связано с тем, что у F_{11} оказалось четыре относительно небольших простых фактора и один огромный, с 564 цифрами:

$$F_{11} = 319489\cdot 974849\cdot 167988556341760475137\cdot 3560841906445833920513\cdot P564 =$$
$$(39\cdot 2^{13}+1)\cdot(119\cdot 2^{13}+1)\cdot(10253207784531279\cdot 2^{14}+1)\cdot$$
$$(434673084282938711\cdot 2^{13}+1)\cdot([560\text{ цифр}]\cdot 2^{13}+1)$$

Хорошо известно, что сложность факторизации числа методом ECM определяется, главным образом, размером *второго* по величине простого множителя.

5. ПРОСТЫЕ ДЕЛИТЕЛИ ЧИСЕЛ ФЕРМА

В предыдущем параграфе воспроизведены все *полные* факторизации чисел Ферма, известные на сегодня (осень 2022 года). Для всех остальных чисел Ферма в лучшем случае имеются лишь доказательства непростоты или *частичные* факторизации — т.е. найдены лишь *какие-то* простые делители, иногда даже *несколько* таких простых делителей, но не полная факторизация.

5.1. Рукотворные простые делители чисел Ферма

Вот, насколько мне известно, *все* делители чисел Ферма F_n, $n \ge 7$, найденные в докомпьютерную эпоху[17]. Первые такие делители, после работы Клаузена 1855 года, были открыты Пермским священником Иваном Первушиным, работы которого, относящиеся к числам Мерсенна, мы уже обсуждали в [5].

• В 1877 году Иван Михеевич Первушин доказал, что $114689 = 7\cdot 2^{14}+1$ делит F_{12}. Через два месяца тот же результат объявил Эдуар Люка.

• В 1878 году Первушин доказал, что $167772161 = 5\cdot 2^{25}+1$ делит F_{23}. См. по этому поводу сообщения Буняковского [1, 87, 88].

• В 1880 году Фортюнэ Ландри[18] [267], [которому было на тот момент 82 года — впрочем, он прожил после этого еще 15 лет!] снова нашел факторизацию Клаузена $F_6 = 274177\cdot 67280421310721$, однако не был уверен, что второй множитель прост. Это было проверено в том же 1880 году ЛеЛассёром и Жерарданом. Очень интересная реконструкция того, как именно это было сделано, с постраничными ссылками на оригинальные работы и письма, приведена в работе Хью Уилльямса [405].

• В 1886 Пауль Зеельхоф[19] [347] доказал, что $2748779069441 = 5\cdot 2^{39}+1$ делит F_{36}.

• В 1899 году Аллан Каннингем нашел два простых делителя F_{11}, а именно

$$319489 = 39\cdot 2^{13}+1 \quad \text{и} \quad 974849 = 119\cdot 2^{13}+1.$$

• В 1903 году Альфред Вестерн нашел *четыре* новых простых делителя

$$2424833 = 37\cdot 2^{16}+1 | F_9, \qquad 13631489 = 13\cdot 2^{20}+1 | F_{18}, \qquad 26017793 = 397\cdot 2^{16}+1 | F_{12},$$
$$63766529 = 973\cdot 2^{16}+1 | F_{12}.$$

• В 1903 Джеймс Каллен и Каннингем убедились, что $6597069766657 = 3\cdot 2^{41}+1$ делит F_{38}, а Вестерн доказал, что это число простое.

• В 1903 году Вестерн и Каннингем [136] доказали, что ни одно другое число Ферма F_n не имеет простых множителей, меньших 10^6.

• В 1905 году Морхед [292] доказал, что

$$188894659314785808547841 = 5\cdot 2^{75}+1 | F_{73}.$$

• В 1925 году Морис Борисович Крайчик [248] доказал, что $1214251009 = 579\cdot 2^{21}+1$ делит F_{15}.

[17] Я исхожу из того предположения, что доведенный до 1918 года список работ по числам Ферма, содержащийся в главе XV книги Диксона [146], полон. Работа Крайчика про F_{15} упомянута на странице 220 его книги [250].

[18] Fortuné Landry, 1798–1895. В 1867–1869 годах он опубликовал две книги [265, 266], в которых описал факторизации всех чисел вида $2^n \pm 1$, $1 \le n \le 64$, кроме четырех, а именно, $2^{59}-1$, $2^{61}-1$, $(2^{61}+1)/3$ и $2^{64}+1$. В [265] он делает совершенно поразительное для того времени замечание, что, без знания использованного метода проверки простоты и без повторения всех проведенных вычислений, утверждение о простоте данного числа является просто “актом веры” = “un acte de foi”.

[19] Paul Peter Heinrich Seelhoff, 1829–1896, преподавал математику в гимназиях Саарбрюкена и Мюльхайма ан дер Рур, а потом в навигационной школе Бремена. В 1886 году он опубликовал еще несколько работ, в частности, список 28 простых чисел Прота [346]. В том же томе я с удивлением заметил работу [348], в которой он независимо переоткрыл число Первушина $M(9) = M_{61} = 2^{61}-1$, о чем я не знал в момент написания [5].

5.2. Частичные факторизации чисел Ферма

Дело в том, что вычислительная сложность задачи факторизации F_n растет *невероятно* быстро с ростом n. Числа Ферма F_{12}, F_{13}, F_{14} и F_{15} имеют 1234, 2467, 4933, 9865 разрядов, соответственно.

Даже установление простоты чисел такого порядка на бытовых компьютерах может оказаться проблематичным, а искать разложение таких чисел на множители сегодня мы просто не умеем даже в тех случаях, когда нам известно уже несколько их простых делителей.

Вот, например, *начало* факторизации чисел Ферма F_{12}, F_{13}, F_{14} и F_{15}. Отметим, что эти факторизации F_{12} и F_{13} рекордные — для F_{12} известно *шесть* простых делителей, а для F_{13} — *четыре*. Еще для четырех чисел Ферма, а именно F_{15}, F_{19}, F_{25}, F_{52} известны *три* простых делителя, для всех остальных — не более двух.

$$F_{12} = 114689 \cdot 26017793 \cdot 63766529 \cdot 190274191361 \cdot 1256132134125569 \cdot$$
$$5686306475353569551690334109408678048393607420608184 33 \cdot C1133 =$$
$$(7 \cdot 2^{14} + 1) \cdot (397 \cdot 2^{16} + 1) \cdot (973 \cdot 2^{16} + 1) \cdot (11613415 \cdot 2^{14} + 1) \cdot$$
$$(76668221077 \cdot 2^{14} + 1) \cdot ([50 \text{ цифр}] \cdot 2^{15} + 1) \cdot C1133,$$

$$F_{13} = 2710954639361 \cdot 2663848877152141313 \cdot 3603109844542291969 \cdot$$
$$319546020820551643220672513 \cdot C2391 =$$
$$(41365885 \cdot 2^{16} + 1) \cdot (20323554055421 \cdot 2^{17} + 1) \cdot (6872386635861 \cdot 2^{19} + 1) \cdot$$
$$(609485665932753836099 \cdot 2^{19} + 1) \cdot C2391,$$

$$F_{14} = 1169280858730743698290359938345963713403867034233733 13 \cdot C4880 =$$
$$([49 \text{ цифр}] \cdot 2^{16} + 1) \cdot C4480$$

$$F_{15} = 1214251009 \cdot 2327042503868417 \cdot 1687688170295169723830241270169 61 \cdot C9808 =$$
$$(579 \cdot 2^{21} + 1) \cdot (17753925353 \cdot 2^{27} + 1) \cdot (12876038896905286589281015 55 \cdot 2^{27} + 1) \cdot C9808,$$

но это мало приближает нас к тому, чтобы разложить на множители остающийся делитель, имеющий для F_{12} больше тысячи — а для остальных *несколько* тысяч! — цифр.

Приведем список известных простых делителей нескольких следующих чисел Ферма:

F_{16}	$1575 \cdot 2^{19} + 1, \quad 180227048850079840107 \cdot 2^{20} + 1$
F_{17}	$59251857 \cdot 2^{19} + 1, \quad [44 \text{ цифры}] \cdot 2^{19} + 1$
F_{18}	$13 \cdot 2^{20} + 1, \quad 9688698137266697 \cdot 2^{23}$
F_{19}	$33629 \cdot 2^{21} + 1, \quad 308385 \cdot 2^{21} + 1, \quad 89621676240286241260825267 03 \cdot 2^{22}$

А вот про число Ферма F_{20} в 1987 году было доказано, что оно составное, но ни одного его простого делителя до сих пор не известно. Вот еще несколько следующих чисел:

$$\begin{array}{ll} F_{21} & 534689\cdot 2^{23}+1 \\ F_{22} & 38539592024440676575336322 11\cdot 2^{24}+1 \\ F_{23} & 5\cdot 2^{25}+1 \end{array}$$

Ситуация с F_{24} ровно такая же как с F_{20}. В 1999 году было установлено, что оно составное, но ни одного их простого делителя до сих пор не найдено. Более того, в момент работы над [8] был неизвестен и статус F_{22}, только в 2010 году было доказано, что это число составное и найден его простой множитель, указанный выше.

Для остальных чисел F_n с $n \le 30$ известен хотя бы один простой делитель:

$$\begin{array}{ll} F_{25} & 48413\cdot 2^{29}+1, \quad 1522849979\cdot 2^{27}+1, \quad 16168301139\cdot 2^{27}+1 \\ F_{26} & 143165\cdot 2^{29}+1 \\ F_{27} & 141015\cdot 2^{30}+1, \quad 430816215\cdot 2^{29}+1 \\ F_{28} & 25709319373\cdot 2^{36}+1 \\ F_{29} & 1120049\cdot 2^{31}+1 \\ F_{30} & 149041\cdot 2^{32}+1, \quad 127589\cdot 2^{33}+1 \end{array}$$

5.3. Нерукотворные простые делители чисел Ферма

При этом все остальные простые множители чисел Ферма, кроме перечисленных выше в 5.1, были найдены уже с использованием компьютеров. Обратите внимание на такого же типа, как и для чисел Мерсенна, исторический зазор, 1925–1953, между последним простым множителем, найденным вручную, и первым, найденным с помощью компьютеров.

• В 1953 году Джон Селфридж [350] объявил первые простые делители чисел F_{10} и F_{16}, а именно

$$11131\cdot 2^{12}+1 | F_{10}, \qquad 1575\cdot 2^{19}+1 | F_{16}.$$

• В 1957 году Робинсон [330], экспериментируя с делителями вида $k\cdot 2^n+1$, $k<100$, нашел два новых простых делителя

$$95\cdot 2^{61}+1 | F_{58}, \qquad 5\cdot 2^{1947}+1 | F_{1945}.$$

• В том же 1957 году Селфридж [350] слегка оптимизировал программу Робинсона и продолжил эти эксперименты для некоторых значений $k>100$. Ему удалось найти еще четыре новых простых делителя, а именно,

$$425\cdot 2^{79}+1 | F_{77}, \qquad 271\cdot 2^{84}+1 | F_{81}, \qquad 403\cdot 2^{252}+1 | F_{250}, \qquad 177\cdot 2^{271}+1 | F_{267}.$$

Таким образом, к 1958 году было известно 38 простых множителей чисел Ферма, их полный список приведен в [332].

• В 1961 году Паксон [303] установил, что число F_{13} составное.

• В 1963 году Клод Рэтхолл [414] обнаружил 11 новых простых делителей чисел Ферма:

$$2^{21}308385+1|F_{19},\quad 2^{23}534689+1|F_{21},\quad 2^{29}48413+1|F_{25},\quad 2^{29}143165+1|F_{26},$$
$$2^{30}141015+1|F_{27},\quad 2^{32}149041+1|F_{30},\quad 2^{33}127589+1|F_{30},\quad 2^{34}1479+1|F_{32},$$
$$2^{40}2653+1|F_{38},\quad 2^{45}43485+1|F_{42},\quad 2^{54}4119+1|F_{52},$$

Фактически вычисления производились на IBM 709 в университете Вашингтона и на IBM 7090 в Университете Калифорнии в Лос Анжелесе = UCLA. Потом все они были проверены Робинсоном на компьютере SWAC, также в UCLA.

• В 1975 году Джон Халлибертон и Джон Бриллхарт [222] открыли приведенные выше простые делители F_{12} и F_{13}.

• В 1978 году Шиппи [354] нашел четыре новых простых делителя чисел Ферма, а именно

$$297\cdot 2^{64}+1|F_{62},\quad 7551\cdot 2^{69}+1|F_{66},\quad 683\cdot 2^{73}+1|F_{71},\quad 1421\cdot 2^{93}+1|F_{91}.$$

• В 1978 году Гостин [190] нашел делитель $59251857\cdot 2^{19}+1$ числа F_{17}.

• В 1979 году Роберт Бэйли [51] нашел еще три новых простых делителя чисел Ферма, а именно

$$629\cdot 2^{257}+1|F_{255},\quad 247\cdot 2^{302}+1|F_{298},\quad 225\cdot 2^{547}+1|F_{544}$$

Даже проверка того, что достаточно большое индивидуальное число Ферма составное, часто требовала отдельной статьи. Вот уже упоминавшиеся выше два относительно небольших составных числа Ферма без известных простых множителей.

• В 1987 году Джеффри Янг и Данкан Бюэль [421] доказали, что число $F_{20}=C315653$ составное.

• В 1999 году Ричард Крэндалл, Эрнст Майер и Джейсон Пападопулос [132] доказали, что число $F_{24}=C5050446$ составное.

Очень интересно отслеживать историю по статьям в Math. Comput., в которых воспроизводились таблицы всех известных на тот момент простых делителей и/или соответствующие ссылки. Вот как, примерно, выглядел прогресс по десятилетиям в XX веке:

• 1958 год — 38 простых множителей, [330];

• 1964 год — 51 простых множителей, [414];

• 1975 год — 55 простых множителей, [222];

• 1983 год — 90 простых множителей, [236];

• 1995 год — 161 простых множителей, из них 46 новых, [191]!

В XXI веке, который начался с 1999 года, внезапное ускорение всей этой деятельности придали распределенные вычисления.

5.4. Сверхестественные простые делители чисел Ферма

Нет, разумеется, никакой возможности описать здесь с такой же степенью подробности историю открытия остальных простых делителей чисел Ферма. Упомянем, поэтому, лишь наиболее спектакулярное событие, которое запустило последующее развитие.

В январе 1999 года Джон Косгрейв и Ив Галло, проверили, что простое $3 \cdot 2^{382449} + 1$ делит число Ферма $F_{382447} = 2^{2^{382447}} + 1$. До этого самым большим числом Ферма, про которое было известно, что оно составное, было $F_{303088} = 2^{2^{303088}} + 1$ с простым множителем $3 \cdot 2^{303093} + 1$, Джеффри Янг [420].

Вот что сам Джон Косгрейв писал в газете “The Irish Time“ в понедельник 16 августа 1999 года:

“... F_5 to F_{23} are composite, but F_{24} (5,050,446 decimal digits), requiring a 47 by 47 feet surface to write it, allowing four digits per inch, is unresolved. A team led by Dr Richard Crandall has been attempting to establish its status as prime or composite for some time.

While F_{24} is large, it is insignificant compared to F_{382447} found by me on July 24th in St Patrick’s College, Drumcondra, Dublin, to be evenly divisible by 3 × 2 to-the-power-of 382449 + 1 (115130 digits). This almost unimaginably large number — F_{382447} (over 10 to-the-power-of 115136 digits) - would require a board measuring more than 10 to-the-power-of 57550 by 10 to-the-power-of 57550 light years to write out at four digits per inch.”

Просто вдумайтесь в приведенный здесь образ — квадратная доска со стороной 10^{57550} **световых лет** для записи десятичных цифр числа F_{382447}, по 6мм на цифру!

Совершенно поразительно, что этот множитель был найден на *бытовом* компьютере с процессором `350 MHz Pentium II` — разумеется, это был один из *многих* компьютеров использованных для поиска, в том числе собственно в St. Patrick’s College of Dublin City University. Кроме того, конечно, требовалась установка написанной Ивом Галло программы `proth.exe` под `Windows 9x/NT/2000`, именно с тем, чтобы ее можно было использовать на большинстве бытовых компьютеров. Как мы увидим, сам по себе тест чрезвычайно простой, подлинная сложность состояла в реализации быстрого умножения *больших* чисел. Это сделано при помощи эффективизации сверток в духе [131] и быстрого преобразования Фурье, оптимизированного под размер кэша бытовых процессоров.

К тому моменту с использованием программы `proth.exe` уже было найдено четыре больших простых делителя чисел Ферма:

- $165 \cdot 2^{49095} + 1$ делит F_{49093}, Ив Галло;
- $169 \cdot 2^{63686} + 1$ делит F_{63679}, Харви Дубнер;
- $99 \cdot 2^{83863} + 1$ делит F_{83861}, Геннадий Гусев;
- $39 \cdot 2^{113549} + 1$ делит F_{113547}, Джон Рензи.

Как показывает само название программы, она связана с числами Прота и сейчас мы совсем коротко напомним, что это такое.

6. ЧИСЛА ПРОТА

В связи с критерием Люка—Эйлера представляется естественным взглянуть чуть подробнее на следующий класс чисел, которые уже возникали у нас в связи построением лестницы простых при экспериментальной проверке нечетной гипотезы Гольдбаха.

Натуральное число n называется **числом Прота**[20] если n имеет вид $n = k \cdot 2^m + 1$, для некоторых натуральных чисел k, m, причем k нечетное и $2^m > k$. Простые числа такого вида называются **простыми Прота**.

[20] Числа Прота названы так в честь Франсуа Прота, 1852–1879, французского фермера-самоучки, который обнаружил в 1878 году критерий их простоты.

Числа Ферма — частный случай чисел Прота при $k = 1$, другой частный случай, к которому мы вернемся в § 8, это **числа Каллена** $n = m \cdot 2^m + 1$, возникающие при $k = m$. Подобно числам Ферма числа Прота допускают простые бинарные представления.

Напомним, что **критерий Прота** состоит в следующем. Рассмотрим число Прота $n = k \cdot 2^m + 1$, где $k < 2^m$ нечетно. Если найдется a, для которого

$$a^{\frac{(n-1)}{2}} \equiv -1 \pmod{n},$$

то n просто. Отметим, что это *детерминистический* алгоритм, всегда возвращающий правильный ответ. Любое a работает здесь с вероятностью $1/2$, поэтому этот тест достаточно эффективен для практической проверки простоты.

С учетом совершенно исключительной важности простых Прота в вычислительной теории чисел, количество относящихся к ним *содержательных* текстов удивительно невелико. Вот несколько первых простых Прота

$$3, 5, 13, 17, 41, 97, 113, 193, 241, 257, 353, 449, 577, 641, 673, 769, 929, 1153, 1217, 1409, 1601,$$
$$2113, 2689, 2753, 3137, 3329, 3457, 4481, 4993, 6529, 7297, 7681, 7937, 9473, 9601, 9857,$$
$$10369, 10753, 11393, 11777, 12161, 12289, 13313,$$

Это последовательность A080076 в Энциклопедии Целочисленных Последовательностей.

Всего имеется ровно 4304683178 простых Прота, не превосходящих $2^{72} \approx 4.7 \cdot 10^{21}$, что [без сжатия] требует для своего хранения примерно 95.8Gb.

• Самым большим известным на осень 2022 года простым Прота продолжает оставаться $10223 \cdot 2^{31172165} + 1$, которое имеет 9,383,761 цифр. Это число было найдено 6 ноября 2016 года Питером Шаболчем в рамках проекта распределенных вычислений `PrimeGrid`. Кроме того, это САМОЕ БОЛЬШОЕ ИЗВЕСТНОЕ НА СЕГОДНЯ ПРОСТОЕ ЧИСЛО, НЕ ЯВЛЯЮЩЕЕСЯ ЧИСЛОМ МЕРСЕННА. Все 8 больших известных сегодня простых чисел, как и следующие за ним 3, являются **числами Мерсенна**.

• Предыдущим рекордом было $19249 \cdot 2^{13018586} + 1$, которое имеет 3,918,990 цифр. Это число было открыто 26 марта 2007 года Константином Агафоновым в рамках проекта `Seventeen of Bust`[21].

• С тех пор было обнаружено еще *десять* больших простых Прота с 4–6.5 миллионами цифр — в том числе два летом 2022 года — однако все они меньше, чем $10223 \cdot 2^{31172165} + 1$. Во втором из них по величине $202705 \cdot 2^{21320516} + 1$, открытом 1 декабря 2021 года Павлом Атнашевым, 6418121 цифр. Это 15-е по величине простое число, известное сегодня. Перед ним на позициях 13 и 14 два **обобщенных числа Ферма**, см. следующий параграф.

• Третье по величине простое Прота $7 \cdot 2^{20267500} + 1$, в котором 6101127 цифр, нашел 21 июля 2022 Райан Проппер, как делитель обобщенного числа Ферма

$$F_{20267499}(12) = 12^{2^{20267499}} + 1.$$

[21] Начатый в 2002 году проект распределенных вычислений, целью которого было решение 17 остающихся случаев в проблеме Серпиньского. До апреля 2016 года было решено 11 случаев. В этот момент он был прекращен по техническим причинам, а соответствующая деятельность пересена в `Prime Grid`, который продолжает с тех пор оставаться главным проектом по поиску новых простых Прота.

Ранее Проппер обнаружил многие другие простые Прота именно как делители обобщенных чисел Ферма[22].

В 1914 году Поклингтон обобщил критерий Прота на случай чисел вида $n = kp^m + 1$, где $k < p^m$. **Критерий Поклингтона** утверждает, что если для какого-то $a \in \mathbb{Z}$ выполняются условия

i) $a^{n-1} \equiv 1 \pmod{n}$,

ii) $\gcd(a^{(n-1)/p} - 1, n) = 1$,

то n простое.

7. ОБОБЩЕННЫЕ ЧИСЛА ФЕРМА

Со времени Эйлера рассматриваются различные вариации на тему чисел Ферма. Наиболее известная из них, это числа вида $F_n(a,b) = a^{2^n} + b^{2^n}$, **обобщенные числа Ферма**. Первоначально я хотел включить сюда обсуждение их факторизации — и вообще факторизаций чисел вида $a^n + b^n$ и $a^n - b^n$, в связи с теоремой Банга—Жигмонди и т.д. Несколько забавных задач в таком духе приведено в нашем задачнике с Володей Халиным [8]. Но это оказалось огромной самостоятельной темой, которой также посвящены сотни работ. Ограничусь поэтому совсем беглым обсуждением обобщенных чисел Ферма по одному основанию $F_n(a) = F_n(a,1)$.

7.1. Обобщенные числа Ферма

Особенно интенсивно изучались числа вида

$$F_n(a) = a^{2^n} + 1,$$

известные как **обобщенные числа Ферма** = **GFN** по основанию a. Обычные числа Ферма $F_n = F_n(2)$ получаются здесь при $a = 2$.

Ясно, что обобщенное число Ферма может быть простым только при *четном* основании a. При *нечетном* a оно заведомо делится на 2, поэтому некоторые авторы называют при нечетном основании a обобщенными числами Ферма числа вида $(a^{2^n}+1)/2$. Нам кажется более правильным сохранить и в этом случае обозначение $F_n(a)$ за теми числами, которые были определены выше, а эти новые числа называть, как это обычно принято, **half-Fermat integers**.

Факторизации обобщенных чисел Ферма посвящена огромная литература и мы не будем даже пытаться здесь ее как-то систематизировать. Дело в том, что обобщенных чисел Ферма *больше*, чем чисел Мерсенна того же порядка и многие большие — субрекордные! — простые возникают как их простые множители, см., например, [72, 73, 79, 108, 149, 151, 153, 209, 210]. Ограничимся поэтому иллюстрацией того, как мы использовали GFN в классе.

Задача. Найдите первые несколько простых полу-Ферма по основанию 3 и профакторизуйте остальные. До какого индекса Вам удалось дойти на бытовом компьютере?

[22] См. по этому поводу страницу проекта Рэя Баллинджера и Вильфрида Келлера, Proth Search Page, `http://www.prothsearch.net/`. Меня там поразило идеальное соответствие, даже для совсем маленьких значений, экспериментальных данных результатам Анатолия Моисеевича Вершика [12] об асимптотическом распределении простых делителей и то, как это отражается в фактической цене поиска.

Ответ. Вот все известные сегодня простые такого вида:

$$2,\ 5,\ 41,\ 21523361,\ 926510094425921,\ 1716841910146256242328924544641,$$

отвечающие индексам 0, 1, 2, 4, 5, 6. Эти числа образуют начало последовательности A093625 в Энциклопедии Целочисленных Последовательностей[23]. Там отмечается, что следующий член этой последовательности, если он существует, имеет индекс $n \geq 21$ и, таким образом, содержит больше миллиона десятичных цифр. Раскладывать числа такого порядка на множители, при наличии по крайней мере двух больших простых делителей, нам пока без шансов.

Число $F_3(3) = 6562$ моментально факторизуется в уме, если помнить из начальной школы признак делимости на 17: $6562 \to 646 \to 34$. Таким образом $F_3(3) = 2 \cdot 17 \cdot 193$. Но следующие, конечно, только на компьютере. Ну,

$$F_7(3) = 2 \cdot 257 \cdot 275201 \cdot 138424618868737 \cdot 3913786281514524929 \cdot 153849834853910661121$$

все еще очень маленькое. А вот дальше не сразу и только потому, что крупно повезло

$$F_8(3) = 2 \cdot 12289 \cdot 8972801 \cdot 8912061245203736028 17 \cdot P90,$$

где, как обычно, $P90 = 70727\ldots00097$ обозначает простое число с 90 цифрами, см. [411]. Числа, у которых один из простых множителей настолько больше остальных, легко факторизуются, *например*, при помощи квадратичного решета. Но на этом везение более-менее заканчивается, у $F_9(3)$ — 244 цифры, а у $F_{10}(3)$ — 489. Факторизация этих и дальнейших чисел $F_n(3)$ любыми *обычными* алгоритмами на бытовом компьютере займет дни, недели, месяцы или годы, если вообще возможна. В любом случае, гипотеза состоит в том, что все они составные.

Задача. Продолжите этот эксперимент для других небольших оснований и индексов, скажем до $a = 30$ или $a = 50$.

Ответ. *Интересных* обобщенных простых Ферма, возникающих в *этом* интервале оснований, чрезвычайно мало. Вот следующее простое полу-Ферма:

$$F_5(21)/2 = 10232633887503346841646713190513110823395 21$$

А вот первое настоящее обобщенное простое Ферма индекса ≥ 5, которое сразу резко больше, чем все предыдущие, но все еще много меньше, чем все полноразмерные примеры и легко ищется на бытовом компьютере:

$$F_5(30) = 185302018885184100000000000000000000000000000001$$

Впрочем, последний блок цифр — 1, потом 31 нуль, потом снова 1 — легко вычисляется в уме, в самом деле, 2^5 делится на $\varphi(10) = 4$, а $2^5 - 1 = 31$. Я обычно использую такого рода ментальную арифметику просто чтобы контролировать, что правильно набрал вопрос в `Mathematica`.

Следующие два интересных обобщенных простых полу-Ферма и Ферма, где-то между которыми проходит граница возможностей бытового компьютера, это

$$F_5(35)/2 = (35^{32} + 1)/2 = 330616742651\ldots115356445313 \quad (99 \text{ цифр}),$$
$$F_9(46) = 46^{512} + 1 = 214787904487\ldots289480994817 \quad (852 \text{ цифр}).$$

[23] `https://oeis.org/A093625`

Многие дальнейшие интересные обобщенные простые Ферма, было бы трудно обнаружить на бытовом компьютере, но их простоту все еще легко проверить, зная их существование. Так, например, в числе $F_{11}(150) = 150^{2048} + 1$ уже 4457 цифр — больше двух страниц текста, — причем снова не включая компьтер ясно, что последние из них таковы: 5, потом 2047 нулей и последняя цифра 1.

7.2. Рекорды простых чисел.

Как мы уже обсуждали в [5], большинство известных сегодня самых больших простых чисел, в частности, все 7 известных чисел с более чем 10^7 цифр, это числа Мерсенна вида $M_p = 2^p - 1$, где p простое. Единственное число среди 12 самых больших простых, не являющееся числом Мерсенна, это обсуждавшееся в предыдущем параграфе число Прота.

Наибольший индекс, для которого в настоящее время известны простые обобщенные числа Ферма, это 20. Их основания образуют последовательность OEIS A321323:

$$1,\ 919444,\ 1059094,\ 1951734,\ 1963736$$

Все нетривиальные такие числа были открыты за последние 5 лет, в каждом из них больше 6 миллионов цифр и все они попадают в top 20 самых больших известных сегодня простых. Вот они, в порядке убывания[24].

• Простое $F_{20}(1963736) = 1963736^{1048576} + 1$ было открыто 24 сентября 2022 года. В нем 6598776 цифр:

$$F_{20}(1963736) = 80651637087363405\ldots\text{еще 6598741 цифр}\ldots080313425433460737$$

• Простое $F_{20}(1951734) = 1951734^{1048576} + 1$ было открыто 09 августа 2022 года. В нем 6,595,985 цифр

• Простое $F_{20}(1059094) = 1059094^{1048576} + 1$ было открыто 31 октября 2018 года. В нем 6,317,602 цифр.

• Простое $F_{20}(919444) = 919444^{1048576} + 1$ было открыто 29 августа 2017 года. В нем 6,253,210 цифр.

Номинально у каждого из этих чисел есть, конечно, свой индивидуальный первооткрыватель. Однако в действительности все эти числа являются продуктом огромного распределенного проекта `PrimeGrid`, в рамках которого тысячи волонтеров предоставляют свои компьютеры для установки специализированных программ.

Этот проект администрируется десятком энтузиастов и, в свою очередь использует систему распределенных вычислений `BOINC`, специализированный пакет `PRPNet`, где довольно много еще чего спрятано внутри (в частности, программы быстрого умножения больших чисел, и т.д.), и, кроме того, специализированные теоретико-числовые программы. Например, программы Дэвида Андербакке `AthGFNSieve` и Ананда Наира `GFNSvCUDA` реализующие решето.

Важным аспектом поиска является то, что первооткрыватель заявляет число как **probable prime**, для этого используется программа Ива Галло `GeneferOCL5`. Обычно соответствующее вычисление для индивидуального числа занимает на бытовом компьютере несколько часов. Уже после этого команда тестировщиков убеждается в

[24] `https://www.primegrid.com/download/`

том, что это **provable prime** при помощи созданных Жаном Пенне и Павлом Атнашевым программ `LLR` и `LLR2`, это вычисление занимает уже несколько суток на рабочих станциях.

Обобщенных простых Ферма с меньшими индексами известно уже довольно много.

• Например, сегодня известно 14 оснований простых $F_{19}(a)$ индекса 19, это последовательность OEIS A243959:

1, 75898, 341112, 356926, 475856, 1880370, 2061748, 2312092, 2733014,
2788032, 2877652, 2985036, 3214654, 3638450,

в то время как всего 10 лет назад было известно лишь 5 членов этой последовательности. Замечу, что в старшем члене этой последовательности $F_{19}(3638450)$ уже 3439810 цифр, так что всего каких-нибудь 20 с небольшим лет назад оно было бы рекордным.

• А вот 30 оснований простых $F_{18}(a)$ индекса 18, это последовательность OEIS A244150:

1, 24518, 40734, 145310, 361658, 525094, 676754, 773620, 1415198, 1488256, 1615588,
1828858, 2042774, 2514168, 2611294, 2676404, 3060772, 3547726, 3596074, 3673932, 3853792,
3933508, 4246258, 4489246, 5152128, 5205422, 5828034, 6287774, 6291332, 8521794,

но это все относительно маленькие простые, в каждом из которых меньше миллиона цифр.

• Кроме того, сегодня известно по 31 основанию простых $F_n(a)$ индексов $n = 17$ и $n = 16$, это последовательности OEIS A253854 и A251597; 36 таких оснований индекса $n = 15$, это последовательность OEIS A226530 и 46 таких оснований индекса $n = 14$, это последовательность OEIS A226529.

В нстоящее время продолжается интенсивный поиск обощенных простых Ферма с этими индексами и начат активный поиск простых $F_n(a)$ с индексами $n = 21$ и $n = 22$.

Как мы уже упоминали, сегодня 12 среди top 20 рекордных простых это числа Мерсенна, 4 числа Прота и 4 — обобщенные простые Ферма индекса 20. Однако среди top 100 картина меняется — там всего 13 чисел Мерсенна — и еще одно простое, являющееся нормой числа Мерсенна в кольце $\mathbb{Z}[i]$ целых гауссовых чисел. В то же время, там уже 19 обобщенных простых Ферма и 6 старших простых делителей обобщенных чисел Ферма.

Обобщенных чисел Ферма гораздо больше, чем чисел Мерсенна того же порядка, а *систематический* распределенный поиск обобщенных простых Ферма начался относительно недавно. Судя по динамике последних 5 лет, я не удивлюсь, если вскоре мы увидим обобщенные простые Ферма в первой десятке самых больших простых, а, возможно, даже и в самом начале списка.

8. ВАРИАЦИИ НА ТЕМУ ЧИСЕЛ ПРОТА

Не то, чтобы мы сами серьезно интересовались такого типа вещами, но различные вариации на тему чисел Прота служили нам с Володей Халиным [8] неисчерпаемым источником задач разной сложности для домашних заданий и финальных тестов.

8.1. Числа Каллена и Вудалла

Вот специальный класс чисел Прота и аналогичные числа с заменой $+1$ на -1.

- Число $C_n = n \cdot 2^n + 1$ называется **числом Каллена**.
- Число $W_n = n \cdot 2^n - 1$ называется **числом Вудалла**.

Задача. Вычислите первые 140 чисел Каллена $C_n = n \cdot 2^n + 1$ и убедитесь, что все они, кроме $C_1 = 3$ составные. Достаточно ли этого, чтобы сформулировать гипотезу, что все числа C_n, $n > 1$, составные?

Ответ. Нет, как обнаружил Робинсон [332] число C_{141} простое. Кроме того, известны следующие простые Каллена [235, 237]:

$$C_{4713},\ C_{5795},\ C_{6611},\ C_{18496},\ C_{32292},\ C_{32469}, C_{59656},\ C_{90825},\ C_{262419},$$
$$C_{361275},\ C_{481899},\ C_{1354828},\ C_{6328548},\ C_{6679881},$$

их индексы образуют последовательность OEIS A005849. В самом большом из них, открытом в июле 2009 года Магнусом Бергманом, 2010852 миллиона цифр. Что-то делать с числами такого размера на бытовом компьютере без специализированных программ типа тех, которые устанавливает `PrimeGrid`, весьма сомнительное удовольствие.

Таким образом, среди чисел Каллена простых мало и их индексы довольно быстро растут. В то же время, в отличие от простых Каллена, среди простых Вудалла с небольшими индексами довольно много простых.

Задача. Найдите первые 15 простых чисел Вудалла $W_n = n \cdot 2^n - 1$.

Ответ. Вот они: $W_2 = 7$, $W_3 = 23$, $W_6 = 383$,

$W_{30} = 32212254719$,

$W_{75} = 283341988972178712821759 9$,

$W_{81} = 19584598277756992630240 0511$,

$W_{115} = 47769131098520414182480566228824883 19$,

$W_{123} = 13079603478523572189373461473158590627 83$,

и, кроме того, W_{249}, W_{362}, W_{384}, W_{462}, W_{512}, W_{751}, W_{822}. Но вот следующие простые Вудалла уже непомерно велики:

$$W_{5312},\ W_{7755},\ W_{9531},\ W_{12379},\ W_{15822},\ W_{18885},\ W_{22971},\ W_{23005},\ W_{98726},\ W_{143018},\ W_{151023},$$
$$W_{667071},\ W_{1195203},\ W_{1268979},\ W_{1467763},\ W_{2013992},\ W_{2367906},\ W_{3752948},\ W_{17016602},$$

их индексы образуют последовательность OEIS A002234. В самом большом из них 5122515 цифр и это в настоящий момент 30-е самое большое известное простое число.

8.2. Числа Серпиньского.

В 1960 году Вацлав Серпиньский [358] доказал, что существует бесконечно много таких нечетных натуральных k, что *все* числа $k \cdot 2^n + 1$ составные. Такие k называются **числами Серпиньского**, они образуют последовательность OEIS A076336, вот ее начало:

78557, 271129, 271577, 322523, 327739, 482719, 575041, 603713, 903983, 934909, 965431,
1259779, 1290677, 1518781, 1624097, 1639459, 1777613, 2131043, 2131099, 2191531,
2510177, 2541601, 2576089, 2931767, 2931991, 3083723, 3098059, 3555593, 3608251, …

Задача. Докажите утверждение Серпиньского.

Решение. Так как исходное рассуждение Серпиньского [358] самым непосредственным образом связано с числами Ферма, воспроизведем для начала именно его.

$$\begin{array}{llll}
n\equiv 1 \pmod 2, & k\equiv 1 \pmod 3 & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod 3,\\
n\equiv 2 \pmod 4, & k\equiv 1 \pmod 5 & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod 5,\\
n\equiv 4 \pmod 8, & k\equiv 1 \pmod{17} & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod{17},\\
n\equiv 8 \pmod{16}, & k\equiv 1 \pmod{257} & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod{257},\\
n\equiv 16 \pmod{32}, & k\equiv 1 \pmod{65537} & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod{65537},\\
n\equiv 32 \pmod{64}, & k\equiv 1 \pmod{641} & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod{641},\\
n\equiv 0 \pmod{64}, & k\equiv -1 \pmod{6700417} & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod{6700417}.
\end{array}$$

Обратите внимание, что первые пять из этих модулей — это простые Ферма F_0, F_1, F_2, F_3, F_4, а последние два — это найденные Эйлером простые делители F_5. Так как сравнения в первой колонке задают разбиение $\mathbb{N}$, то для каждого k, удовлетворяющего сравнениям во второй колонке, число $k\cdot 2^n+1$ делится хотя бы на одно из простых 3, 5, 17, 257, 65537, 641, 6700417. Чтобы гарантировать нечетность k, добавим еще сравнение $k\equiv 1 \pmod 2$. Теперь китайская теорема об остатках гарантирует, что любое k удовлетворяющее сравнению

$$k\equiv 15511380746462593381 \pmod{2\cdot 3\cdot 5\cdot 17\cdot 257\cdot 65537\cdot 641\cdot 6700417}$$

является числом Серпиньского. Таким образом, количество чисел Серпиньского не просто бесконечно, а имеет положительную плотность в множестве натуральных чисел.

Решение другим манером. Вот еще одно решение, основанное на той же идее, предложенное в 1962 году Джоном Селфриджем (неопубликовано, см. [170]). Обратите внимание, что это решение основано на использовании гораздо меньших простых:

$$\begin{array}{llll}
n\equiv 0 \pmod 2, & k\equiv 2 \pmod 3 & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod 3,\\
n\equiv 1 \pmod 4, & k\equiv 2 \pmod 5 & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod 5,\\
n\equiv 3 \pmod 9, & k\equiv 9 \pmod{73} & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod{73},\\
n\equiv 15 \pmod{18}, & k\equiv 11 \pmod{19} & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod{19},\\
n\equiv 27 \pmod{36}, & k\equiv 6 \pmod{37} & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod{37},\\
n\equiv 1 \pmod 3, & k\equiv 3 \pmod 7 & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod 7,\\
n\equiv 11 \pmod{12}, & k\equiv 11 \pmod{13} & \Longrightarrow & k\cdot 2^n+1\equiv 0 \pmod{13}.
\end{array}$$

Наименьшее нечетное решение получающейся системы сравнений равно 78557 и Селфридж считал, что это и есть наименьшее число Серпиньского. Однако в 2002 году все еще оставалось 17 меньших чисел, `Seventeen of Bust`[25], про которые на тот момент

[25] `http://www.seventeenofbust.com`

не было известно, являются они числами Серпиньского, или нет, что в значительной степени и стимулировало интерес к поиску простых Прота.

Ясно, что поиск дальнейших таких покрытий $\mathbb{N}$ сравнениями является замечательным упражнением на модулярную арифметику.

8.3. Числа Ризеля и варианты.

Если заменить в определении чисел Серпиньского $+1$ на -1, получается определение чисел Ризеля. Иными словами, k называется **числом Ризеля**, если *все* числа $k \cdot 2^n - 1$ составные. Числа Ризеля образуют последовательность OEIS A101036, вот ее несколько первых членов:

509203, 762701, 777149, 790841, 992077, 1106681, 1247173, 1254341, 1330207, 1330319, 1715053, 1730653, 1730681, 1744117, 1830187, 1976473, 2136283, 2251349, 2313487, 2344211, 2554843, 2924861, 3079469, 3177553, 3292241, 3419789, 3423373, 3580901, …

В 1998 году Эрик Брир доказал, что существует бесконечно много чисел, которые *одновременно* являются числами Серпиньского и числами Ризеля. Такие числа называются **числами Брира**. Они образуют последовательность OEIS A076335, вот несколько первых из них:

3316923598096294713661, 1043967989637478027637 3, 1161510327795570497 5673, 1260711058885450195 3787, 1785503665700759611 0949, 2144459816918157846 6233, 2896067497343610639 1349, 3209952244551587247 3461, 3290499556222085757 3541

Нечетное число k называется **двойственным числом Ризеля**, если для всех натуральных n число $|2^n - k|$ составное. Гипотеза состоит в том, что множества чисел Ризеля и двойственных чисел Ризеля. Например, $|2^n - 509203|$ составное для всех натуральных n, причем 509203 наименьшее с таким свойством.

9. ЦИКЛОТОМИЯ: ТЕОРИЯ

С числами Ферма связана и первая математическая работа Гаусса. А именно, 30 марта 1796 года Гаусс придумал построение правильного 17-угольника. Именно после этой работы он окончательно решил заниматься математикой, а не лингвистикой.

9.1. Построения циркулем и линейкой

Решение квадратичных уравнений при помощи циркуля и линейки было известно — или, по Шпенглеру, должно было быть известно — древним грекам, так как оно целиком находится в русле идей греческой “геометрической алгебры”, см. следующий пункт.

Однако в англоязычной литературе этот метод решения квадратичных уравнений принято называть окружностями Карлайла = Carlyle circles, по имени шотландского истерика Томаса Карлайла, 1795–1881. О чем, однако, древние греки могли лишь догадываться, так это о том, что при помощи циркуля и линейки можно решать

только квадратичные уравнения. Для решения кубических уравнений нужен еще один инструмент, например, трисектор или лекало, которое позволяет строить параболы.

Допустим, что мы хотим решить **квадратичное уравнение**[26] $x^2 - ax + b = 0$. Ограничимся для простоты случаем, когда $a, b \in \mathbb{R}$, хотя аналогичный метод применим и к случаю комплексных коэффициентов. Для этого изобразим на плоскости $\mathbb{R}^2$ точки $(0,1)$ и (a,b). Окружность C с диаметром $(0,1)$ — (a,b) называется **окружностью Карлайла** этого квадратичного уравнения. Иными словами, центр C равен $(a/2, b/2+1/2)$, а квадрат радиуса — $(a/2)^2 + (b/2-1/2)^2$.

Допустим вначале, что окружность Карлайла пересекает ось x в двух точках x_1 и x_2, причем $x_1 \geq x_2$. Ясно, что $(a/2, 0)$ является серединой отрезка $(x_1, 0)$, $(x_2, 0)$, так что $x_1 + x_2 = a$. С другой стороны, теорема о пересекающихся хордах (при $b \leq 0$) или секущих (при $b > 0$) показывает, что $x_1 x_2 = b$. Таким образом, *если* окружность Карлайла пересекает ось x, то он пересекает ее в корнях уравнения $x^2 - ax + b = 0$.

Что, если это уравнение не имеет вещественных корней, т.е. $b/2 + 1/2$ больше, чем радиус окружности Карлайла? Это происходит, если дискриминант отрицателен, $\Delta = a^2 - 4b < 0$. В этом случае *любая* окружность с центром на оси x ортогональная к окружности Карлайла пересекает вертикальную прямую $x = a/2$, проходящую через центр окружности Карлайла, в точках $(a/2, \sqrt{-\Delta/2})$, $(a/2, -\sqrt{-\Delta/2})$.

Полный ответ на вопрос о том, какие геометрические построения осуществимы при помощи циркуля и линейки, дает теория Галуа. Рассмотрим точки 0 и 1 на вещественной прямой. Все точки комплексной плоскости, которые можно построить отправляясь от 0 и 1 при помощи циркуля и линейки, образуют поле, которое называется **полем достижимых чисел** и обозначается $\mathbb{K}$.

Чисто алгебраически поле $\mathbb{K}$ определяется как наименьшее **квадратично замкнутое** подполе в $\mathbb{C}$. Иными словами, $\mathbb{K}$ содержит 1 и замкнуто относительно извлечения квадратных корней, для любого $x \in \mathbb{K}$ существует $y \in \mathbb{K}$ такое, что $y^2 = x$.

Доказанная в 1837 году **теорема Ванцеля** [393] утверждает, что элементы поля $\mathbb{K}$ и только они могут быть построены при помощи циркуля и линейки. Доказательство этой теоремы обсуждается, например, в учебниках Чеботарева [33] и Постникова [24]. Ниже мы обсудим классический частный случай этого результата, относящийся к **циклотомии**, т.е. делению круга на равные части.

Заметим, что *попутно* в той же работе Ванцель дал отрицательные ответы еще на две классические проблемы открытые до этого более 2000 лет, **проблему удвоения куба** и **проблему трисекции угла**.

Невозможность осуществить удвоение куба посредством циркуля и линейки означает в точности, что $\sqrt[3]{2}$ не является достижимым числом. Невозможность трисекции угла доказывается, например, тем, что, раз мы не можем построить правильный девятиугольник, то мы не можем поделить на 3 даже углы $\pi/3$ и $2\pi/3$. В самом деле, довольно сомнительно, чтобы больший корень $8x^3 - 6x + 1 = 0$, равный

$$\cos\left(\frac{2\pi}{9}\right) = \frac{1}{4}\left(\sqrt[3]{-4+4i\sqrt{3}} + \sqrt[3]{-4-4i\sqrt{3}}\right)$$

был достижимым числом, см. по этому поводу § 11. Вот что-то в таком духе и написано в статье Ванцеля [393].

[26] Я в курсе того, что школьный жаргон предписывает переводить `quadratic equation` как `квадратное уравнение` — или, в обратном переводе, `square equation`. Более того, квадратные уравнения действительно являются квадратичными, [2].

9.2. Есть ли у квадратичных уравнений греческие корни

В своей замечательной книге “История эмбриологии” [23] сэр Джозеф Нидэм замечает: “В древнем Египте были инкубаторы, но не было эмбриологии, а в древней Греции была эмбриология, но не было инкубаторов.” Даже не вдаваясь в подробности, в связи с предыдущим пунктом невозможно не упомянуть совершенно феерическую дискуссию, посвященную тому, умели ли греки решать квадратичные уравнения, тем более, что истоки этой дискуссии связаны с дискуссией о Ферма.

В конце XIX века Иероним Цейтен [34] и Поль Таннери [376] предложили концепцию, согласно которой греки владели, в частности, алгебраическими идеями, но выражали их на геометрическом языке, то что стало называться “греческой геометрической алгеброй”. Схожей позиции придерживались издатели и переводчики греческих математических текстов Йохан Гейберг [16] и сэр Томас Хис [211]. Сам термин “геометрическая алгебра” популяризировал, в частности, Отто Нойгебауэр [296], который утверждал, что именно в такой форме греки восприняли вавилонскую алгебру. На русском эта точка зрения изложена в чрезвычайно влиятельных книгах Бартеля ван дер Вардена [10] и самого Нойгебауэра [22].

В 1975 году Сабетай Унгуру [379] опубликовал совершенно *невероятную* по развязности статью против концепции геометрической алгебры в целом, содержавшую, в частности, грубые личные выпады против ван дер Вардена и Нойгебауэра. В дальнейшем Унгуру с учениками и соавторами опубликовал три больших текста на тему “does the quadratic equation have Greek roots?” [176, 382, 383], в которых доказывал, что греки **не** умели решать квадратичных уравнений!

Основной посыл исходной статьи состоял в том, что достигнув того возраста, когда они не могут более непосредственно заниматься своей наукой[27], математики начинают писать об истории математики. Но пишут *неправильно*, потому что для того, чтобы их читать, нужно знать математику: “It is in truth deplorable and sad when a student of ancient or medieval culture and ideas must familiarize himself first with the notions and operations of *modern* mathematics in order to grasp the meaning and intent of modern commentators dealing with ancient and medieval mathematical texts”, [379].

Вейль пересказывает эту позицию следуюшим образом: “According to some, little more is required than what was known to the authors one plans to write about; some go so far as to say that the less one knows, the better one is prepared to read those authors with an open mind[28].” Дальше всех в этом отношении пошел ученик Унгуру Майкл Фрид, который предложил аксиому **Tabula rasa**: “It is both possible and proper for historian of mathematics not to know any mathematics at all,” [174, 175].

На эту статью последовательно ответили по существу и воздерживаясь от личных оскорблений сам ван дер Варден [389] в 1976 году и Ханс Фрейденталь [173] в 1977 году. В следующем 1978 году Андре Вейль *дважды* вернулся к этой полемике, вначале в [396] и потом снова в своем докладе [397] на ICM-1978. Написаны эти тексты в обычной для Вейля язвительной манере, что дало Унгуру повод опубликовать в 1979 году еще более хамский ответ [381][29].

Если не знать более широкого контекста того времени, эти документы, начиная просто с самого факта публикации [379] в серьезном историческом журнале, представля-

[27] Унгуру пишет *буквально* ”professional impotence”.

[28] “If you open your mind too much, your brain will fall out”.

[29] Греческие переводы всех этих пяти статей вместе с занимательными комментариями собраны в книге Иоанниса Кристианидиса и Димитриса Диалитиса [119].

ются совершенно поразительными по вирулентности. *Часть* этого контекста эксплицируется в статье Мартины Шнайдер [342].

Этому предшествовало копившееся раздражение представителей humanities против того, что они воспринимали как попытки математиков покуситься на святое, их полную бесконтрольность. В частности, Шнайдер подробно обсуждает роль Вейля в “афере Белла”, когда предложенный экономистами и социологами в качестве постоянного члена Принстонского IAS Роберт Белла был провален на голосовании в соотношении 13/8, при 5 воздержавшихся. Известно, что среди голосовавших против были Арман Борель, Андре Вейль, Гедель, Дайсон, Милнор, Монтгомери, Сельберг, причем Борель и Вейль оркестровали широкую публичную кампанию против избрания Белла. О том, насколько остро это воспринималось гуманитариями, можно судить хотя бы по статье Фанга [160], где “афера Белла” прямо сравнивается с “аферой Дрейфуса”.

Второй острый конфликт, уже в Университете Принстона, возник в связи с тенюром историка математики Майкла Махони, ученика Томаса Куна (того самого Куна, “структура научных революций”). Для ускорения процесса Махони в очевидной спешке опубликовал научную биографию Ферма [282], в которой Андре Вейль [395] тут же обнаружил огромное количество фактических и математических ошибок. Рецензия Вейля выдержана в следующих тонах: Махони недостает “some knowledge of French”, “some knowledge of Latin”, “knowledge and sensitivity to mathematics”, “some historical sense”, “some knowledge of the work of Fermat’s contemporaries and of his successors”, “ordinary accuracy”, “the ability to express simple ideas in plain English”, и т.д. — “the ink is ugly and the paper is from the wrong kind of tree”.

Как замечает Стивен Ландсбург[30]: “Without a doubt, it was the most devastating book review in the history of literature”. Очень интересный личный пересказ этой истории можно найти в книге Нила Коблица [244], жена которого Анн как раз в то время училась у Махони.

Унгуру вспоминает, что Кун поручил ему написать одну из контр-рецензий на книгу Махони. Хотя фактически [380] вышла позже [379], работа над ней была начата раньше и [379] открывается эпиграфом Майкла Махони — именно из его биографии Ферма!! Так что нет сомнения, что инвективы Унгуру против “сенильных математиков” были адресованы Вейлю в еще большей степени, чем ван дер Вардену, на что Вейль и отреагировал в свойственной ему манере. Провокация удалась!

Разумеется, разборки в Лиге плюща на тему, кому быть живым и хвалимым, на этом не прекратились. Достаточно вспомнить дела “Ленг против Липсета” или “Ленг против Хантингтона”. Еще одна острая дискуссия того времени, отголоски которой можно найти в [242, 243, 360] посвящена использованию математики в политологии (взгляд на эту историю от первого лица можно найти в той же книге Коблица [244]). Все следы этой дискуссии подтерты в базах данных `MathSciNet` и `ZBMath`, вплоть до ссылок на [243, 360], в интересное время живем.

9.3. Теорема Гаусса—Ванцеля.

Циклотомией = делением (буквально “разрезанием”) круга, называется деление окружности на n равных частей.

Теорема Гаусса—Ванцеля утверждает, что для того, чтобы окружность можно было разделить на n частей при помощи циркуля и линейки, необходимо и достаточно, чтобы

[30] http://www.landsburg.com/weil.htm

n имело вид

$$n = 2^m p_1 \dots p_s, \quad \text{где } p_i \text{ — попарно различные простые числа Ферма.}$$

По модулю сформулированной выше теоремы Ванцеля это очевидно. В самом деле, так как порядок $(\mathbb{Z}/n\mathbb{Z})^*$ равен $\phi(n)$, то $(\mathbb{Z}/n\mathbb{Z})^*$ в том и только том случае является 2-группой, когда $n = 2^m p_1 \dots p_s$, где p_i — попарно различные числа Ферма.

Но ведь разделить окружность на n частей означает в точности построить первообразный корень $\zeta = e^{2\pi i/n}$ из 1 степени n. Круговое расширение $\mathbb{Q}(\zeta)$ является расширением Галуа поля $\mathbb{Q}$ с группой Галуа $G(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. С другой стороны, для того, чтобы число $a \in \mathbb{C}$ можно было построить циркулем и линейкой, оно должно принадлежать расширению $K/\mathbb{Q}$ такому, что группа Галуа $\mathrm{Gal}(K/\mathbb{Q})$ является 2-группой.

Достаточность условия была доказана Гауссом в 1796 году, но вот его *необходимость* — только Ванцелем в 1837 году. Разумеется, Гаусс не мог пользоваться теорией Галуа в своем доказательстве, потому что в то время, когда он установил свою часть теоремы, Галуа еще не родился! Да чего там Галуа, в 1799–1801 годах Гаусс не знал еще результатов Руффини и Абеля. Но ровно поэтому он, разумеется, и **не мог** доказать эту теорему в трудную сторону, это сделал Ванцель 40 лет спустя.

Интересно, что имя Пьера Лорана Ванцеля, 1814–1848, совершенно неизвестно широкой публике, хотя именно он решил классические проблемы **трисекции угла** и **удвоения куба** — в той же работе, в которой доказал теорему Гаусса—Ванцеля. Для начала, он не немецкий математик, а французский, и провел всю свою не слишком долгую жизнь в Париже, в École Polytechnique, вначале как élève-ingénieur des Ponts-et-Chaussées, я уж не знаю, как это перевести на русский, мостостроитель, или дорожный инженер, потом как ingénieur и répétiteur. Напомню, что примерно в то же время репетиторами в École Polytechnique служили люди типа Бертрана, Бонне, Каталана, Ле Веррье, Делоне,...

9.4. Верить нельзя никому не только в наше время.

Конечно, Гаусс в “Disquisitiones Arithmeticae” *говорил*, что он *доказал* необходимость — НУ ТАК И ВЫ ТОЖЕ ГОВОРИТЕ! Гаусс вообще много чего говорил, например, что в 1799 году доказал “основную теорему высшей алгебры”. Доказал, да, но в 1815 году, воспроизведя доказательство Эйлера—Лагранжа. А свое первое доказательство он и в 1849 году не смог исправить, потому что это гораздо труднее, чем исправить доказательство д’Аламбера.

В любом случае, ни в “Disquisitiones”, ни, насколько мне известно, в каких-либо других текстах Гаусса, нет никаких намеков на доказательство или, хотя бы, его идею. А ведь Гаусс, как раз, отличался *непревзойденными* основательностью и прилежанием, `Sitzfleisch`.

Для меня было ПОЛНЫМ ШОКОМ прочитать, в каких выражениях пересказывает это в своей книге Феликс Клейн: “Hierzu hat G a u s s noch andere Fälle hinzugefügt, indem er die Möglichkeit der Teilung in p Teile, wo p eine Primzahl von der Form $p = 2^{2^\mu} + 1$ ist, und die Unmöglichkeit für alle andern Zahlen bewiss”, [238], ср. также с французским и английским переводами [239, 240]. Тринадцатый удар часов ставит под сомнение все предыдущие, так что после этого я не знаю, как относиться ко всем остальным историческим изысканиям Клейна.

Следующая цитата показывает, *насколько* Диксон точнее и надежнее как исторический источник: “C. F. Gauss *proved* that a regular polygon of m sides can be constructed by

ruler and compasses if m is a product of a power of 2 and distinct odd primes each of the form F_n) and *stated* that the construction is impossible if m is not such a product".

Вот что, например, Гаусс говорит там же по поводу решения уравнений степени 5: "...quin hocce problema non tam analyseos hodiernae vires superet, quam potius aliquid impossibile proponat." Следуя логике Клейна, нужно провозгласить, что эта фраза содержит формулировку (и доказательство!) теоремы Руффини—Абеля и всей теории Галуа. Невозможность решения общего уравнения пятой степени была в то время очевидна всем, включая Гаусса, что он здесь и говорит.

Большинство же последующих авторов просто слепо копировали высказывание Клейна, что теорему Гаусса—Ванцеля доказал Гаусс в "Disquisitiones Arithmeticae". Раймонд Арчибальд [41, 42] пытался исправить утверждение Клейна, но он ошибочно приписывает первое доказательство необходимости Джеймсу Пирпойнту. Первым недвусмысленным изложением фактического положения дел была, насколько мне известно, небольшая заметка Николаса Казаринова [233].

10. ЦИКЛОТОМИЯ: ПРАКТИКА

Здесь будут описаны классические конструкции правильных 3-угольника и 5-угольника, конструкция Гаусса правильного 17-угольника и то, что мне удалось узнать про конструкции правильных 257-угольника и 65537-угольника.

10.1. Построение правильного 3-угольника и правильного 5-угольника

• **Корни 3-й степени из 1.** Пусть ω — первообразный корень 3-й степени из 1. Тогда ω является корнем квадратичного уравнения $x^2+x+1=0$. Корнями этого уравнения являются

$$\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \qquad \bar{\omega} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

Построить эти корни циркулем и линейкой совсем просто, ω и $\overline{\omega} = \omega^2$ будут точками пересечения окружностей радиуса 1 с центрами в 0 и в -1.

• **Корни 5-й степени из 1.** Корни 5-й степени из 1 являются корнями уравнения $x^5-1=0$. Так как один из корней этого уравнения равен 1, то мы можем разделить x^5-1 на $x-1$ так что первообразные корни степени 5 будут корнями уравнения $x^4+x^3+x^2+x+1=0$. Поскольку $x=0$ не является корнем, это уравнение равносильно уравнению $x^2+x+1+x^{-1}+x^{-2}=0$. Положив теперь $y=x+x^{-1}$, мы получаем относительно y следующее уравнение: $y^2+y-1=0$. Это уравнение имеет два различных корня $y_1=\dfrac{-1-\sqrt{5}}{2}$ и $y_2=\dfrac{-1+\sqrt{5}}{2}$. Решая теперь уравнения $x+x^{-1}=y_1$ и $x+x^{-1}=y_2$, получим 4 первообразных

корня[31] из 1 степени 5:

$$\epsilon_1 = \frac{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}}{4}, \qquad \epsilon_2 = \frac{-1-\sqrt{5}+i\sqrt{10-2\sqrt{5}}}{4},$$
$$\epsilon_3 = \frac{-1-\sqrt{5}-i\sqrt{10-2\sqrt{5}}}{4}, \qquad \epsilon_4 = \frac{-1+\sqrt{5}-i\sqrt{10+2\sqrt{5}}}{4},$$

Сравнивая эти формулы с формулой $\epsilon_k = \cos(2\pi k/n) + i\sin(2\pi k/n)$, видим, что

$$\cos(2\pi/5) = \frac{\sqrt{5}-1}{4}.$$

Метод деления окружности на 5 частей был известен в Древней Греции и описан, *например*, в “Альмагесте” Птолемея. Самый простой вариант этого метода состоит в следующем. Построим окружность с центром в точке $-1/2$, проходящую через точки $\pm i$. Эта окружность пересекает вещественную ось в точке $-1/2+\sqrt{5}/2$. Построим теперь окружность радиуса 1 с центром в точке $-1/2+\sqrt{5}/2$. Эта окружность пересечет единичную окружность с началом в центре координат в точках ϵ_1, ϵ_4. Теперь, зная сторону вписанного пятиугольника, совсем просто построить ϵ_2, ϵ_3.

10.2. Построение правильного 17-угольника

Первообразные корни степени 17 будут корнями уравнения

$$x^{16} + x^{15} + \ldots + x + 1 = 0.$$

Мультипликативная группа $\mathbb{F}_{17}^* = (\mathbb{Z}/17\mathbb{Z})^*$ поля $\mathbb{F}_{17}$ циклическая. Возьмем какой-нибудь **примитивный корень** m по модулю 17, т.е. такой элемент класс которого порождает эту группу. Это значит, что числа $1, m, m^2, \ldots, m^{15}$ принимают 16 различных значений по модулю 17.

Так как $\mathbb{F}_{17}^*$ циклическая групп порядка 16, имеется 8 таких примитивных корней, а именно, $3, 5, 6, 7, 20, 11, 12, 14$. Возьмем любой из них, например, $m = 3$. Выразим теперь все первообразные корни степени 17 из 1 через один из них, скажем, через

$$\zeta = \cos(\phi) + i\sin(\phi), \qquad \phi = 2\pi/17,$$

по степеням 3. Таким образом, мы располагаем все 16 первообразных корней в следующем порядке:

$$\zeta, \zeta^3, \zeta^9, \zeta^{10}, \zeta^{13}, \zeta^5, \zeta^{15}, \zeta^{11}, \zeta^{16}, \zeta^{14}, \zeta^8, \zeta^7, \zeta^4, \zeta^{12}, \zeta^2, \zeta^6.$$

[31] Отмечу, что на стр. 46 учебника Дмитрия Константиновича Фаддеева [30] имеется опечатка в знаке вещественной части корней ϵ_2 и ϵ_3. Сам я, в отличие от Д. К., разумеется, не умею решать квадратичных уравнений в уме и обнаружил эту опечатку с помощью `Mathematica`. При этом Д. К. был одним из самых понимающих, квалифицированных, тщательных и добросовестных людей, которых я вообще видел в своей жизни, с невероятно развитой, для математика, способностью к ментальным вычислениям. Я был свидетелем того, как он умножал на доске в реальном времени две матрицы 8×8, одновременно записывая ответ двумя руками. Это является еще одним доказательством правоты самураев в том, что осознавать и проверять всеми доступными нам средствами нужно **все и всегда** — ДАЖЕ ЖАРЕНОГО ЦЫПЛЕНКА НЕОБХОДИМО ПРИВЯЗЫВАТЬ.

Рассмотрим теперь следующие две суммы этих корней:

$$x_1 = \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2,$$

$$x_2 = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6.$$

Ясно, что $x_1 + x_2 = -1$. Сейчас мы убедимся, что $x_1 x_2 = -4$. Для этого, сгруппируем корни парами сопряженных,

$$\zeta + \zeta^{16},\ \zeta^9 + \zeta^8,\ \zeta^{13} + \zeta^4,\ \zeta^{15} + \zeta^2 \quad \text{и, соответственно,} \quad \zeta^3 + \zeta^{14},\ \zeta^{10} + \zeta^7,\ \zeta^5 + \zeta^{12},\ \zeta^{11} + \zeta^6.$$

Таким образом,

$$x_1 = 2(\cos(\phi) + \cos(8\phi) + \cos(4\phi) + \cos(2\phi)),$$

$$x_2 = 2(\cos(3\phi) + \cos(7\phi) + \cos(5\phi) + \cos(6\phi)).$$

Вспоминая формулу произведения косинусов

$$2\cos(m\phi)\cos(n\phi) = \cos((m+n)\phi) + \cos((m-n)\phi),$$

мы видим, что

$$x_1 x_2 = 8(\cos(\phi) + \ldots + \cos(8\phi)) = 4(x_1 + x_2) = -4.$$

Таким образом, мы знаем $x_1 + x_2 = -1$ и $x_1 x_2 = -4$ и можем теперь найти x_1, x_2 из квадратичного уравнения $x^2 + x - 4 = 0$. Так как

$$\cos(\phi) + \cos(2\phi) > 2\cos(\pi/4) = \sqrt{2} > -\cos(8\phi),$$

а $\cos(4\phi) > 0$, то $x_1 > 0$. Поэтому $x_2 = -4/x_1 < 0$.

Теперь, зная x_1 и x_2, мы можем сделать следующий шаг. Положим

$$y_1 = \zeta + \zeta^{13} + \zeta^{16} + \zeta^4 = 2(\cos(\phi) + \cos(4\phi),$$

$$y_2 = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2 = 2(\cos(8\phi) + \cos(2\phi),$$

$$y_3 = \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12} = 2(\cos(3\phi) + \cos(5\phi),$$

$$y_4 = \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6 = 2(\cos(7\phi) + \cos(6\phi).$$

Ясно, что $y_1 + y_2 = x_1$, а так как $\cos(\phi) > \cos(2\phi)$, $\cos(4\phi) > \cos(4\phi)$, то $y_1 > y_2$. Кроме того,

$$y_1 y_2 = 8(\cos(\phi) + \ldots + \cos(8\phi)) = -1.$$

Таким образом, y_1 и y_2 удовлетворяют уравнению $y^2 - x_1 y - 1 = 0$. Аналогично, y_3 и y_4 удовлетворяют уравнению $y^2 - x_2 y - 1 = 0$, причем $y_3 > y_4$.

Положим, наконец,

$$z_1 = \zeta + \zeta^{16} = 2\cos(\phi), \qquad z_2 = \zeta^{13} + \zeta^4 = 2\cos(4\phi).$$

Тогда $z_1 > z_2$, $z_1 + z_2 = y_1$ и

$$z_1 z_2 = 4\cos(\phi)\cos(4\phi) = 2(\cos(5\phi) + \cos(3\phi)) = y_3.$$

Поэтому z_1 — больший корень уравнения $z^2 - y_1 z + y_3 = 0$.

Таким образом, построение $2\cos(\phi)$, а значит и построение ζ, можно осуществить при помощи циркуля и линейки. Однако, насколько мне известно, сам Гаусс не дал такой конструкции, первая явная конструкция была описана в работе Егора Андреевича фон Паукера 1817 года, см. ссылку в [302]. Фактическое описание этой конструкции можно найти в книгах Чеботарева [33], либо Прасолова и Соловьева [26].

Однако, как и большинство русских работ того времени[32], работа Паукера была

[32] Даже написанных по-немецки! Не говоря про те, которые были написаны по-русски или по-французски!

неизвестна в Германии, где считали, что первая фактическая конструкция правильного 17-угольника была проведена фон Штаудтом [364] в 1842 году, т.е. ровно четверть века спустя! Во всяком случае, Шретер [344] называет свою статью недвусмысленно, “К конструкции фон Штаудта правильного семнадцатиугольника”. При этом сам Шретер слегка модифицирует набор инструментов, а именно рассматривает конструкцию при помощи линейки и *фиксированной* окружности.

Для ценителей конкретности приведем явную формулу. Не очень сложное непосредственное вычисление показывает, что

$$\cos\left(\frac{2\pi}{17}\right) = \frac{1}{16}\left(\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{170 + 38\sqrt{17}}}\right),$$

детали приведены в цитированной книге Клейна и воспроизведены, например, в книге Гиндикина, [17] стр.148–153. Пользуясь случаем, воспроизведу комментарий Семена Григорьевича по этому поводу: “В одном отношении формула для $\cos(2\pi/17)$ не оставляет сомнения. Прийти к ней в рамках традиционных геометрических идей времени Эвклида невозможно.”

10.3. Построение правильных n-угольников при $n = 257$ и $n = 65537$

Пользуясь методом Гаусса несложно построить и первообразный корень степени 257 из 1. Насколько мне известно, фактически это впервые сделал русский астроном и математик Егор Андреевич (alias Магнус-Георг) фон Паукер, 1787–1855, Курляндия (в настоящее время Латвия). Фон Паукер работал в обсерватории Дерпта а потом большую часть жизни был преподавателем математики в гимназии в Митаве (сегодня Елгава, Латвия). В 1822 году он был избран членом-корреспондентом Петербургской Академии Наук, в том же 1822 году вышла его работа [302] с вычислением $\cos(2\pi/257)$.

Занимающая всего лишь 194 страницы текста явная *геометрическая* конструкция правильного 257-угольника была опубликована Фридрихом Юлиусом Ришло[33,34] в 1832 году в Crelle [319].

[33] Friedrich Julius Richelot, 1808–1875, был профессором в университете Кенигсберга (сегодня Калининград, Россия). Чтобы поставить это в контекст, нужно вспомнить, что в XIX веке Кенигсберг был, наряду Берлином и Геттингеном, одной из столиц немецкой математики. С 1826 по 1843 год там работал Карл Густав Яков Якоби, 1804–1851. Построение првильного 257-угольника было темой диссертации Ришло, защищенной в 1831 году под руководством Якоби. В 1843 году Ришло стал преемником Якоби и нет никакого сомнения, что дальнейшие упомянутые в этом пункте работы выполнены под их непосредственным влиянием.

[34] Кстати, дочь Ришло Клара была замужем за Киркгофом, что является еще одним экспериментальным подтверждением следующего закона генетики: “Браки молодых математиков с дочерьми своих учителей — настолько характерное явление академической жизни Европы и Америки, что даже принято говорить о совершенно особой форме наследования математических способностей, передающихся обычно не от отца к сыну, а от тестя к зятю”, [13]. Например, в 1881 году Пикар женился на дочери Эрмита — и тут же доказал свои знаменитые теоремы о распределении значений аналитических функций и был избран в Парижскую Академию Наук (здесь для большей наглядности я слегка редактирую историю в духе Фоменко, но общая канва соблюдена). Впрочем, это далеко не единственный подобный случай: семейство Адамар — Поль Леви — Лоран Шварц — У. Фриш является еще более поразительным примером того, как МАТЕМАТИЧЕСКИЕ СПОСОБНОСТИ — И МЕСТО В ПАРИЖСКОЙ АКАДЕМИИ! — ПЕРЕДАВАЛИСЬ ОТ ТЕСТЯ К ЗЯТЮ В ТЕЧЕНИЕ ЧЕТЫРЕХ ПОКОЛЕНИЙ. Впрочем, не следует думать, что этот феномен ограничен Парижем и Парижской Академией наук. Аналогичное поразительное природное явление многократно наблюдалось в Берлине и Прусской Академии наук, например, Герман Шварц был зятем Куммера.

В 1834 году А. Фишер[35] опубликовал там же ЯВНОЕ ВЫРАЖЕНИЕ корней уравнения $x^{257} - 1 = 0$ через цепочку квадратичных уравнений [172]. Это всего 19 страниц вычислений в таком же духе как те, что проделаны выше для случаев $n = 3, 5, 17$, практически без текста, но полностью понятные, итогом которых является вычисление [вещественных частей] всех корней степени 257 из 1 с точностью до 10 десятичных знаков после запятой. Это *вручную*, без компьютера — широко жили люди XIX века.

Построение первообразного корня степени 65537 из 1, вероятно, займет у читателя несколько больше времени. Однако, как замечено [143], для этого достаточно построить *не более* 1332 окружностей Карлайла. Это было фактически осуществлено Йоганном Густавом Хермесом[36] [215], который построил правильный 65537-угольник *всего* за 10 лет БЕЗ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРА!.

Легенда гласит, что его статья занимает сундук, который до сих пор хранится на чердаке Математического Института Университета Геттингена. Краткое изложение этой работы, на 17 страницах, было опубликовано в 1894 году в Göttinger Nachrichten [215]. В этой связи уместно вспомнить девиз Хермеса “Geduld ist die Pforte der Freude” — ТЕРПЕНИЕ, ЭТО ВРАТА РАДОСТИ, [216].

Вот точные слова Клейна по этому поводу: “Auf das 65537-Eck hat Prof. Hermes in Lingen 10 Jahre seines Lebens verwandt[37], um alle nach der Gauss’schen Behandlundgsweise vorkommended Wurzeln etc., genau zu untersuchen. Das äusserst fleissige Diarium wird in der Sammlung des mathematischen Seminar zu Göttingen aufbewahrt. Man vergleiche eine Mitteilung von Prof. Hermes in Nr. 3 der Göttinger Nachrichten vom Jahre 1894”.

А вот анекдотическое изложение той же истории Литтлвудом: “A too-persistent research student drove his supervisor to say “Go away and work out the construction for a regular polygon of $65537 (= 2^{16} + 1)$ sides” The student returned 20 years later with a construction (deposited in the Archives at Göttingen)”.

11. ЦИКЛОТОМИЯ С ПОМОЩЬЮ ПАРАБОЛИЧЕСКОГО ЛЕКАЛА

Гаусс не доказывал необходимость в теореме Гаусса—Ванцеля, но зато он сделал гораздо больше, чем обычно упоминают, в другом направлении. А именно, в Disquisitiones Arithmeticae доказана достаточность в теореме Гаусса—Пирпойнта и явно описано вычисление корней 19-й и 73-й степеней.

11.1. Теорема Гаусса—Пирпойнта.

С классической древности изучался вопрос, что можно построить, если добавить к линейке и циркулю какие-то другие геометрические инструменты. Такого рода геометрическим конструкциям посвящена, например, книга [286].

[35] Это единственная его работа, которую я смог найти, там не указывается его имя, но зато указывается локация, Regiomontano, т.е. Кенигсберг — а не что-то там в Мексике, как полагают википедики. Из любопытства я полистал весь том. Из опубликованных там работ 24 написаны по-немецки, 11 по-французски и только 6, включая работы Фишера и Якоби, на латыни.

[36] Йоганн Густав Хермес, 1846–1912, учился в Кенигсберге, где в 1878 году защитил диссертацию по делению круга на $2^m + 1$ часть, [213, 214]. После этого преподавал математику в Кенигсберге и Лингене.

[37] Формально Клейн, вероятно, прав, в 1896 году Хермес действительно был профессором гимназии в Лингене (Оснабрюк). Но по существу издевательство. В самой статье Хермеса недвусмысленно говорится “Königsberg i. Pr.” — т.е. “Кенигсберг в Пруссии”.

Одна из самых популярных вариаций возникает при добавлении инструмента, позволяющего строить конические сечения. Следующий классический результат отвечает на вопрос, на сколько частей можно разделить окружность при помощи циркуля, линейки и **параболического лекала**. Этот вопрос сводится к тому, для каких степеней вычисление корней из 1 сводится к решению квадратных и кубических уравнений. Вместо параболического лекала здесь можно брать любой другой инструмент, позволяющий решать кубические уравнения, например, **трисектор** [186] — или **оригами** [128].

То, что это так для степеней 7 и 9, было известно арабам в IX веке (Бурбаки, Алгебра, т. II, стр. 221). В действительности, Сабит ибн-Корра (836–911) атрибутирует построение правильного семиугольника Архимеду. Греческий текст не сохранился, но Сабит сделал арабский перевод.

Полный ответ дается следующим результатом обобщающим теорему Гаусса—Ванцеля. Современное доказательство приведено в работе [388], впрочем, Видела не цитирует работу Пирпойнта и, видимо, считает этот результат новым!

Теорема Гаусса—Пирпойнта утверждает, что для того, чтобы окружность можно было разделить на n частей при помощи циркуля, линейки и параболического лекала, необходимо и достаточно, чтобы n имело вид

$$n = 2^k 3^l p_1 \dots p_s, \qquad \text{где } p_i \neq 2,3 \text{ — попарно различные простые такие, что каждое } p_i - 1 \text{ имеет вид } 2^r 3^s \text{ для подходящих } r \text{ и } s.$$

Вообще, точки на плоскости, которые можно построить при помощи циркуля, линейки и параболического лекала — это в точности наименьшее подполе в $\mathbb{C}$, замкнутое относительно извлечения квадратных и кубических корней.

11.2. Простые Пирпойнта

Фигурирующие в теореме Гаусса—Пирпойнта простые обычно называются простыми Пирпойнта. Иными словами, **простое Пирпойнта** это простое вида $2^r 3^s + 1$ для некоторых $r, s \geq 0$, включать ли сюда $p = 2, 3$, это вопрос вкуса. Например, последовательность OEIS A005109 начинается так:

$$2, 3, 5, 7, 13, 17, 19, 37, 73, 97, 109, 163, 193, 257, 433, 487, 577, 769, 1153, 1297, 1459, 2593, 2917,$$
$$3457, 3889, 10369, 12289, 17497, 18433, 39367, 52489, 65537, 139969, 147457, 209953, 331777,$$
$$472393, 629857, 746497, 786433, 839809, 995329, 1179649, 1492993, 1769473, 1990657, \dots$$

Ясно, что простые числа Ферма F_n являются простыми Пирпойнта. С другой стороны, обобщенные числа Ферма $F_n(3)$ с основанием 3 четны. Поэтому все простые Пирпойнта, не являющиеся числами Ферма, имеют вид $6m + 1$. Самое большое известное сегодня число Пирпойнта является числом Прота $3 \cdot 2^{16,408,818} + 1$ и открыто в октябре 2020 года. Основная гипотеза состоит, естественно, в том, что количество простых Пирпойнта бесконечно.

11.3. Построение правильных 7-угольника, 9-угольника, 13-угольника и 19-угольника.

• **Корни 7-й степени из 1.** Первообразные корни степени 7 будут корнями уравнения $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$. Поскольку $x = 0$ не является корнем, это уравнение

равносильно уравнению

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

Положив теперь $y=x+x^{-1}$, мы получаем относительно y следующее уравнение: $y^3+y^2-2y-1=0$. По формуле Кардано

$$y_{1,2,3}=\frac{1}{3}\left(-1+\sqrt[3]{\frac{-7+21\sqrt{-3}}{6}}+\sqrt[3]{\frac{-7+21\sqrt{-3}}{6}}\right)$$

Для того, чтобы найти корни степени 7, остается лишь решить три квадратичных уравнения $x^2-y_ix+1=0$, $i=1,2,3$. Фактическую геометрическую конструкцию правильного семиугольника можно найти, например, в мануале греческой математики Хиса [211], с. 340.

• **Корни 9-й степени из 1.** Действуем точно так же, как в предыдущем случае. Первообразные корни степени 9 будут корнями уравнения $x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1=0$. Поскольку $x=0$ не является корнем, это уравнение равносильно уравнению

$$x^4+x^3+x^2+x+1+x^{-1}+x^{-2}+x^{-3}+x^{-4}=0.$$

Положив теперь $y=x+x^{-1}$, мы получаем относительно y следующее уравнение: $y^4+y^3-3y^2-2y+1=0$. Решение уравнения степени 4 сводится к решению одного уравнения степени 3 и нескольких квадратичных уравнений. Если y_1,y_2,y_3,y_4 — корни этого уравнения, то для нахождения корней степени 9, остается лишь решить четыре квадратичных уравнения $x^2-y_ix+1=0$, $i=1,2,3,4$.

• **Корни 13-й степени из 1.** Этот пример детально разобран в учебнике алгебры Кохендёрфера [245], с. 196–197. Пусть ζ — первообразный корень степени 13 из 1. Положим

$$x_1=\zeta+\zeta^5+\zeta^8+\zeta^{12},\quad x_2=\zeta^2+\zeta^3+\zeta^{10}+\zeta^{11},\quad x_3=\zeta^4+\zeta^6+\zeta^7+\zeta^9.$$

Непосредственное вычисление показывает, что

$$x_1+x_2+x_3=-1,\qquad x_1x_2+x_1x_3+x_2x_3=-4,\qquad x_1x_2x_3=-1.$$

Поэтому x_1,x_2,x_3 являются корнями многочлена x^3+x^2-4x+1. Положим теперь

$$\begin{array}{lll} y_1=\zeta+\zeta^{12}, & y_3=\zeta^2+\zeta^{11}, & y_5=\zeta^4+\zeta^9,\\ y_2=\zeta^5+\zeta^8, & y_4=\zeta^3+\zeta^{10}, & y_6=\zeta^6+\zeta^7. \end{array}$$

Легко видеть, что y_1 и y_2 являются корнями уравнения $y^2-x_1y+x_3=0$; y_3 и y_4 являются корнями уравнения $y^2-x_2y+x_1=0$; и, наконец, y_5 и y_6 являются корнями уравнения $y^2-x_3y+x_2=0$. Теперь, чтобы найти ζ и $\zeta^{12}=\bar{\zeta}$, остается лишь решить уравнение $z^2-y_1z+1=0$. Все остальные корни получаются путем решения уравнений $z^2-y_iz+1=0$.

• **Корни 19-й степени из 1.** Следующую задачу из Disquisitiones мы с Володей Халиным рутинно предлагали студентам второго курса экономического факультета[38].

[38] С ностальгией вспоминается: “квантовую механику теперь преподают в младшей группе детского сада”, [18]

Задача. Проведите аналогичный анализ для случая корней степени 19 из 1. Сколько кубических уравнений Вам придется при этом решать? Почему?

Следующие простые числа, для которых мы теперь можем провести циклотомию, это 37, 73 и 97 — это именно те случаи, для которых проведены конструкции в статье Эрика Бэнвилля и Бернара Женеве [54], которые, кстати, обсуждают, как это сделать на компьютере.

11.4. Построения с помощью циркуля и линейки с засечками

Линейка с засечками = marked ruler или twice-notched straightedge, это линейка, на которой поставлены две метки на расстоянии 1. Такая линейка позволяет новую операцию, verging, состоящую в том, чтобы находить две точки на расстоянии 1 на двух кривых (ну, единственные кривые, которые мы умеем строить — это прямые и окружности) на прямой, проходящей через данную точку.

Архимед доказал, что этими новыми инструментами можно произвести трисекцию угла, а Никомед доказал, что при помощи них можно построить $\sqrt[3]{x}$ для любого x. Тем самым, при помощи этих инструментов можно построить все, что можно построить при помощи коник. Оказывается, однако, что они позволяют решать и некоторые уравнения степени 5.

Этот вопрос изучается в статьях Барагара, Робертсона—Снайдера и Бенджамина—Снайдера [56, 66, 67, 327]. В частности там введено понятие **ультрарадикала** a, это вещественный корень уравнения $x^5 + x - a = 0$. Оказывается, построение корней 11-й степени из 1 требует только вычисления ультрарадикала и, таким образом, становится возможным при помощи этого нового инструмента.

11.5. Посвящение

С Володей Гердтом мы познакомились довольно поздно, меньше 20 лет назад, но с тех пор постоянно плотно общались и профессионально и дружески. С ним было всегда интересно, наши встречи и беседы я вспоминаю с огромной благодарностью и восхищением. Я не знал других людей, которые так глубоко и всесторонне понимали бы роль компьютеров в математике во всех принципиальных и технических аспектах, и со стороны математики, и со стороны компьютеров, и со стороны физики.

Володя был одним из первых читателей и критиков всех моих текстов на эти темы и повлиял на мое собственное понимание компьютерной математики больше, чем кто-либо другой:

“Чжуан-цзы был на похоронах. Проходя мимо могилы Хуэй-цзы, он обернулся к спутникам и сказал:

— Однажды некий инец запачкал белой глиной кончик носа: пятнышко было — с мушиное крылышко. Он приказал плотнику Ши стесать его. Умелец так заиграл топором — аж ветер поднялся: только выслушал приказ — и все стесал. Снял дочиста всю глину, не задев носа. А инец — и бровью не повел. Услыхав об этом, сунский князь Юань позвал к себе плотника и сказал ему:

— Попробуй сделать это же самое и для меня,

А плотник ответил:

— Когда-то я сумел это сделать — да только нет уже в живых того материала!

Вот так и у меня не стало материала: с тех пор как умер Учитель — мне больше не с кем спорить.”, [25], “Чжуан-цзы”, гл. 24 “Сюй У-гуй”.

Я чрезвычайно благодарен Сергею Позднякову, который убедил меня написать этот цикл статей. Кроме того, я признателен Галине Ивановне Синкевич за ссылки по текстам XIX века.

References

1. *Буняковскій В. Я.* О новомъ случаѣ дѣлимости чиселъ вида $2^{2^m}+1$, сообщенномъ Академіи От. Первушинымъ (читано в заседании Физ.-мат.отд. 4 апреля 1878 г.), Записки Императорской Академіи Наукъ **31** (1878), no. 1, 223–224.
2. *Вавилов Н. А.* Нумерология квадратных уравнений, Алгебра и анализ, **20** (2008), no. 5, 9–40.
3. *Вавилов Н. А.* Компьютеры как новая реальность математики: I. Personal account. Компьютерные инструменты в Образовании, 2020. No 2, 5–26. doi:10.32603/2071-2340-2020-2-5-26
4. *Вавилов Н. А.* Компьютеры как новая реальность математики: II. Проблема Варинга. Компьютерные инструменты в Образовании, 2020, No. 3, 5–55. doi: 10.32603/2071-2340-2020-3-5-55
5. *Вавилов Н. А.* Компьютер как новая реальность математики: III. Числа Мерсенна и суммы делителей. Компьютерные инструменты в Образовании, 2020, No. 4, 5–58. doi.org/10.32603/2071-2340-2020-4-5-58
6. *Вавилов Н. А.* Компьютер как новая реальность математики: IV. Гипотеза Гольдбаха. Компьютерные инструменты в Образовании, 2021, No. 4, 5–72. doi.org/10.32603/2071-2340-2021-4-5-71
7. *Вавилов Н. А.* Компьютеры как новая реальность математики: V. Легкая проблема Варинга. Компьютерные инструменты в Образовании, 2022, No. 3.
8. *Вавилов Н. А., Халин В. Г.* Задачи по курсу “Математика и Компьютер”. Вып. 1. Арифметика и теория чисел. ОЦЭиМ, СПб, 2005, 180с.
9. *Вавилов Н. А., Халин В. Г., Юрков А. В.* Mathematica для нематематика, 2020, 484с.
10. *ван дер Варден Б. Л.* Пробуждающаяся наука. Математика Древнего Египта, Вавилона и Греции, М.: ГИФМЛ, 1959. 460с.
11. *Василенко О. Н.* О некоторых свойствах чисел Ферма, Вестн. Моск. ун-та. Сер. 1. Матем., мех., 1998, no. 5, 56–58
12. *Вершик А. М.* Асимптотическое распределение разложений натуральных чисел на простые делители, Докл. АН СССР, **289** (1986), no. 2, 269–272.
13. *Винер Н.* Я — математик. Ижевск: НИЦ “Регулярная и хаотическая динамика”, 2001. 336с.
14. *Гаусс К. Ф.* Труды по теории чисел. Пер. В. Б. Демьянова; Под ред. И. М. Виноградова; Комментарий Б. Н. Делоне; Классики Науки, М. Изд-во АН СССР, 1959, 978с.
15. *Гаусс К. Ф.* Пояснение возможности построения семнадцатиугольника. Перевод М. В. Крутиковой, публикация Е. П. Ожиговой. Историко-матем. исслед. **21** (1976), 285–291.
16. *Гейберг И. Л.* Естествознание и математика в классической древности. М.–Л., ОНТИ, 1936.
17. *Гиндикин С. Г.* Рассказы о физиках и математиках. Наука, М., 1981, с.1–191.
18. *Займан Дж.* Современная квантовая теория. М, Мир, 1971, 288с.
19. *Матвиевская Г. П., Ожигова Е. П., Невская Н. И., Копелевич Ю. Х.* Неопубликованные материалы Л. Эйлера по теории чисел. СПб, Наука, 1997, 256с.
20. *Мельников И. Г.* О некоторых вопросах теории чисел в переписке Эйлера с Гольдбахом. История и методология естественных наук, 1966, вып. 5, 15–30.
21. *Мельников И. Г.* Вопросы теории чисел в творчестве Ферма и Эйлера Историко-матем. исслед. **19** (1974), 9–38.
22. *Нейгебауэр О.* Точные науки в древности. М., Наука, 1968, 224с.
23. *Нидем Дж.* История эмбриологии, М., ИЛ, 1947, 342с.
24. *Постников М. М.* Теория Галуа, ГИФМЛ, М., 1963, 218с.
25. Поэзия и проза Древнего Востока. БВЛ, сер. I, т.1, “Художественная литература”, 1973, 736с.
26. *Прасолов В. В, Соловьев Ю. П.* Эллиптические функции и алгебраические уравнения. М., Факториал, 1997, 288с.

27. *Садовник Е. В.* Проверка на простоту некоторых чисел вида $N = 2kp^m - 1$, Дискрет. матем., **18** (2006), no. 1, 146–155.
28. *Садовник Е. В.* Проверка на простоту чисел вида $N = 2kp_1^{m_1}p_2^{m_2}\dots p_n^{m_n} - 1$, Дискрет. матем., **20** (2008), no. 2, 15–24.
29. *Стечкин С. Б.* Критерий Люка простоты чисел вида $N = h2^n - 1$, Матем. заметки, 10:3 (1971), 259–268
30. *Фаддеев Д. К.* Лекции по алгебре. М., Наука, 1984, 416с.
31. *Ферма П.* Исследования по теории чисел и диофантову анализу. Перевод с латыни и французского. М., Наука, 1992, 320с.
32. *Харди Г. Г.* Двенадцать лекций о Раманудже. — М., Ин-т Компьютерных Иссл., 2002, 335с.
33. *Чеботарев Н. Г.* Теория Галуа. ОНТИ, М.–Л., 1936, 154с.
34. *Цейтен Г. Г.* История математики в древности и в средние века. М.–Л.: ГТТИ, 1932, 230с.
35. *Adler F.* Theorie der geometrischen Konstruktionen, Sammlung Schubert **52**, Göschen (Leipzig, 1906).
36. *Affolter F, J.* Zur Staudt—Schröter'schen Construction des regulären Vielecks, Math. Ann., **6** (1873), 582–591.
37. *Agarwal R. C., Burrus C. S.* Fast digital convolution using Fermat transforms, Southwest IEEE Conf. Rec., Houston, Texas, 1973, 538–543.
38. *Agarwal R. C., Burrus C. S.* Fast convolution using Fermat number transforms with applications to digital filtering, IEEE Trans. Acoust. Speech Signal Processing **22** (1974), 87–97.
39. *Aigner A.* Über Primzahlen, nach denen (fast) alle Fermatschen Zahlen quadratische Nichtreste sind, Monatsh. Math. **101** (1986), no. 2, 85–93.
40. *Amiot B.* Mémoire sur les polygones réguliers, Nouv. Annales de Math., **4** (1844), 264–278.
41. *Archibald R. C.* The history of the construction of the regular polygon of seventeen sides. American M. S. Bull. **22** (1916), 239–246.
42. *Archibald R. C.* Gauss and the regular polygon of seventeen sides, Am. Math. Monthly **27** (1920), 323–326.
43. *Arnaudiès J. M., Delezoide P.* Nombres $(2,3)$-constructibles. Adv. Math. **158** (2001), no. 2, 169–252.
44. *Arya S. P.* Fermat numbers, Math. Ed. **6** (1989), 5–6.
45. *Arya S. P.* More about Fermat numbers, Math. Ed. **7** (1990), 139–141.
46. *Asadulla S.* A note on Fermat numbers, J. Natur. Sci. Math. **17** (1977), 113–118.
47. *Aygin Z. S., Williams K. S.* Why does a prime p divide a Fermat number? Math. Mag. **93** (2020), no. 4, 288–294.
48. *Bachmann P.* Die Lehre von der Kreistheilung und ihre Beziehungen zur Zahlentheorie. Leipzig, Germany: Teubner, 1872.
49. *Bardziahin D.* Finding special factors of values of polynomials at integer points. Int. J. Number Theory **13** (2017), no. 1, 209–228.
50. *Baek Seungjin, Choe Insong, Jung Yoonho, Lee, Dongwook, Seo, Junggyo* Constructions by ruler and compass, together with a fixed conic. Bull. Aust. Math. Soc. **88** (2013), no. 3, 473–478.
51. *Baille R.* New primes of the form $k \cdot 2^n + 1$. Math. Comput. **33** (1979), no. 148, 1333–1336.
52. *Baillie R., Cormack G., Williams H. C.* The problem of Sierpiński concerning $k \cdot 2^n + 1$. Math. Comp., **37** (1981), no. 155, 229–231; Corrigenda, ibid. **39** (1982), no. 159, 308.
53. *Baillie R., Wagstaff S. S.* Lucas pseudoprimes. Math. Comp. **35** (1980), no. 152, 1391–1417.
54. *Bainville E., Genevés B.* Constructions using conics. Math. Intelligencer **22** (2000), no. 3, 60–72.
55. *Ballinger R., Keller W.* Proth Search Page, 1997, `http://vamri.xray.ufl.edu/proths/`
56. *Baragar A.* Constructions using a compass and twice-notched straightedge, MAA Month. **109** (2002), 151–164.
57. *Barker C. B.* Proof that the Mersenne number M_{167} is composite, Bull. Amer. Math. Soc. **51** (1945), 389.
58. *Barner K.* Paul Wolfskehl und der Wolfskehl-Preis. Mitt. Dtsch. Math.-Ver. **5** (1997), no. 3, 4–11.
59. *Barner K.* How old did Fermat become? N.T.M., Internationale Zeitschrift für Geschichte und Ethik der Naturwissenschaften, Technik und Medizin. Neue Serie, 9 (2001), 209–228.
60. *Barner K.* Das Leben Fermats. Mitt. Deutsch. Math.-Ver. **9** (2001), no. 3, 12–26.

61. *Barner K.* Neues zu Fermats Geburtsdatum. Mitt. Deutsch. Math.-Ver. **15** (2007), no. 1, 12–14.
62. *Barner K.* Pierre Fermat. Sa vie privée et professionnelle. Ann. Fac. Sci. Toulouse Math. (6) **18** (2009), Fascicule Spécial, 119–135.
63. *Beeger N. G. W. H.* On even numbers m dividing $2^m - 2$, Amer. Math. Monthly **58** (1951), 553–555.
64. *Benjamin E.* On the constructibility of real 5th roots of rational numbers with marked ruler and compass. ISRN Algebra 2012, Article ID 487275, 6 p. (2012).
65. *Benjamin E.* On constructing real 5th roots by marked ruler and compass through verging between a line and a circle. JP J. Algebra Number Theory Appl. **30** (2013), no. 1, 35–46.
66. *Benjamin E., Snyder C.* On the construction of the regular hendecagon by marked ruler and compass, Math. Proc. Camb. Phil. Soc. **156** (2014), 409–424.
67. *Benjamin E., Snyder C.* On the construction of the regular hendecagon by marked ruler and compass. Math. Proc. Cambridge Philos. Soc. **156** (2014), no. 3, 409–424.
68. *Berrizbeitia P., Berry T. G.* Cubic reciprocity and generalised Lucas—Lehmer tests for primality of $A \cdot 3^n \pm 1$, Proc. Amer. Math. Soc. **127** (1999), no. 7, 1923–1925, doi 10.1090/S0002-9939-99-04786-3
69. *Berrizbeitia P., Berry T. G., Tena-Ayuso J.*, A generalization of Proth's theorem, Acta Arith. **110** (2003), 107–115.
70. *Berrizbeitia P., Iskra B.* Deterministic primality test for numbers of the form $A^2 \cdot 3^n + 1$, $n \geq 3$ odd, Proc. Amer. Math. Soc. **130** (2002), no. 2, 363–365 (electronic), doi 10.1090/S0002-9939-01-06100-7
71. *Bethune I.* PrimeGrid: A Volunteer Computing Platform for Number Theory, International Conference on Computational Mathematics, Computational Geometry & Statistics (CMCGS) 2015. DOI: http://dx.doi.org/10.5176/2251-1911_CMCGS15.43
72. *Bethune I., Gallot Y.* Genefer: programs for finding large probable generalised Fermat primes. J. Open Research Software, **3**, (2015), no. 1, doi:10.5334/jors.ca
73. *Bethune I., Goertz M.* Extending the generalized Fermat prime number search beyond one million digits using GPUs. In: Parallel processing and applied mathematics. Part I, 106–113, Lecture Notes in Comput. Sci., **8384**, Springer, Heidelberg, 2014.
74. *Bishop W.* How to construct a regular polygon, Amer. Math. Monthly **85** (1978), 186–188.
75. *Bickmore C. E.* Is the number 78875943472201 prime or composite?. Ed. Times **72** (1900), 99–101.
76. *Biermann K.-R.* T. Clausen, Mathematiker und Astronom. J. Reine Angew. Math. **216** (1964), 158–198. doi.org/10.1515/crll.1964.216.159
77. *Birkhoff G. D., Vandiver H. S.* On the integral divisors of $a^n - b^n$. Ann. Math., **5** (1904), 173–180.
78. *Bishop W.* How to Construct a Regular Polygon. Amer. Math. Monthly **85** (1978), 186–188.
79. *Björn A., Riesel H.* Factors of generalized Fermat numbers. Math. Comput. **67** (1998), no. 221, 441–446; Table errata, ibid. **74** (2005), no. 252, 2099; Table errata 2, ibid. **80** (2011), no. 275, 1865–1866.
80. *Blåsjö V.* A critique of the modern consensus in the historiography of mathematics, Journal of Humanistic Mathematics, **4** (2014), no. 2, 113–123.
81. *Blåsjö V.* In defence of geometrical algebra, Archive for History of Exact Sciences, **70** (2016), no. 3, 325–359.
82. *Bochow* Eine einfache Berechnung des 17 Ecks, Zeitschrift filr Math. u. Phys. (Schĺomilch), **38** (1893), 250–252.
83. *Boklan K. D., Conway J. H.* Expect at most one billionth of a new Fermat Prime! Math. Intelligencer, **39** (2017), no 1, 3–5. doi.org/10.1007/s00283-016-9644-3
84. *Borsos B., Kovács A., Tihanyi N.* Tight upper and lower bounds for the reciprocal sum of Proth primes. The Ramanujan J., published online 17 January 2022, https://doi.org/10.1007/s11139-021-00536-2
85. *Bosma W.* Explicit primality criteria for $h2^k + 1$, Math. Comp. **61** (1993), 97–109, S7–S9.
86. *Bosma W.* Cubic reciprocity and explicit primality tests for $h \cdot 3^k \pm 1$, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun., **41**, Amer. Math. Soc., Providence, RI, 2004, 77–89.
87. *Bouniakowsky V. Ya.* Nouveau cas de divisibilité des nombres de la forme $2^{2^m} + 1$ trouvé par le révérend père I. Pervouchine (Lu le 17 janvier 1878). Bull l'Acad. St.-Petersbourg, **24** (1878), no. 4,

559; republié: Mélanges math. et. astr. St.-Petersbourg, **5** (1879), no. 5, 505–506.
88. *Bouniakowsky V. Ya.* Encore un nouveau cas de divisibilité des nombres de la forme $2^{2^m}+1$ (Lu le 4/16 avril 1878). Bull l'Acad. St.-Petersbourg, **25** (1879), 63–64; republié: Mélanges math. et. astr. St.-Petersbourg, **5** (1879), no. 5, 519–520.
89. *Brent R. P.* Succinct proofs of primality for the factors of some Fermat numbers. Math. Comp. **38** (1982), no. 157, 253–255.
90. *Brent R. P.* Factorization of the eleventh Fermat number, Abstracts Amer. Math. Soc. **10** (1989), 176–177.
91. *Brent R. P.* Parallel algorithms for integer factorisation, Number theory and cryptography (Sydney, 1989), London Math. Soc. Lecture Note Ser., **154**, Cambridge Univ. Press, Cambridge, 1990, 26–37.
92. *Brent R. P.* Factorisation of the tenth and eleventh Fermat number. Technical report, Australian Nat. Univ. TR-CS-96-02 (1996), 27p.
93. *Brent R. P.* Factorisation of the tenth Fermat number. Math. Comput., **68** (1999), 429–451.
94. *Brent R. P., Crandall R. E., Dilcher K., van Halewyn C.* Three new factors of Fermat numbers. Math. Comp., **69** (2000), no. 231, 1297–1304.
95. *Brent R. P., Pollard J. M.* The factorisation of the eighth Fermat number. — Math. Comput., **36** (1981), 627–630.
96. *Bressoud D. M.* Factorization and primality testing, Springer, New York, 1989.
97. *Brillhart J.* Concerning the numbers $2^{2p}+1$, p prime, Math. Comput. **16** (1962), 424–430.
98. *Brillhart J.* Some miscellaneous factorizations, Math. Comput., **17** (1963), 447–450.
99. *Brillhart J.* On the factors of certain Mersenne numbers. II. Math. Comput. **18** (1964), 87–92.
100. *Brillhart J., Johnson G. D.* On the factors of certain Mersenne numbers, Math. Comput. **14** (1960), 365–369.
101. *Brillhart J., Lehmer D. H., Selfridge J. L.* New primality criteria and factorizations of $2^m \pm 1$, Math. Comp. **29** (1975), 620–647.
102. *Brillhart J., Lehmer D. H., Selfridge J. L. , Tuckerman B., Wagstaff S. S. Jr.* Factorizations of $b^n \pm 1$, $b = 2,3,5,6,7,10,11,12$ up to high powers, 2nd ed., Contemp. Math., vol. 22, Amer. Math. Soc., Providence, RI, 1988.
103. *Brillhart J., Selfridge J. L.* Some factorizations of $2^n \pm 1$ and related results. Math. Comput. **21** (1967), 87–96; Corrigendum, ibid. **21** (1967), 751.
104. *Buhler J. P., Harvey D.* Irregular primes to 163 million. Math. Comput. **80** (2011), no. 276, 2435–2444.
105. *Burda Y., Kadets L.* Construction of the heptadecagon and quadratic reciprocity. C. R. Math. Acad. Sci. Soc. R. Can. **35** (2013), no. 1, 16—21.
106. *Butters J. W.* On the solution of the equation $x^p - 1 = 0$ (p being a prime number), Proc. Edinb. Math. Soc, **7** (1888–89), pp. 10–22
107. *Cajori F.* Pierre Laurent Wantzel. Bull. Amer. Math. Soc. **24** (1918), no. 7, 339–347.
108. *Caldwell Ch. K.* The Largest Known Primes. `http://primes.utm.edu/primes/lists/all.txt`
109. *Caldwell Ch. K., Gallot Y.* On the primality of $n! \pm 1$ and $2 \times 3 \times 5 \times \ldots \times p \pm 1$. Math. Comp. **71** (2002), no. 237, 441–448.
110. *Canals I.*, Fermat numbers and the limitation of computers (Spanish), Acta Mexicana Ci. Tecn. 7 (1973), 29–30.
111. *Carmichael R. D.* On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. Ann. Math. **15** (1913), 30–70.
112. *Carslaw H. S.* Gauss's theorem on the regular polygons which can be constructed by Euclid's methods, Proc. Edinb. Math. Soc, **28** (1910), 121–128.
113. *Cayley A.* On the equation $x^{17} - 1 = 0$, Messenger of Math., **19** (1890), 184–188; Collected Papers, **13** (1897) 60–63.
114. *Chaumont A., M'uller T.*, All elite primes up to 250 billion. J. Integer Seq. **9** (2006), no. 3, Article 06.3.8, 5p.
115. *Chen Yong-Gao* On integers of the form $k2^n + 1$. Proc. Amer. Math. Soc. **129** (2001), no. 2, 355–361.
116. *Chen Yong-Gao* A note on the prime factors of Fermat numbers. Southeast Asian Bull. Math. **28** (2004), no. 2, 241–242.
117. *Chen Yong-Gao* On integers of the forms $k \pm 2^n$ and $k2^n \pm 1$. J. Number Theory **125** (2007), no. 1,

14–25.
118. *Chepmell H.* In a given circle to inscribe the regular polygon of thirty-four sides, Educ. Times, March, 1911; Educ. Times Repr. (2), **20** (1911), 51–55.
119. *Christianides G., Dialetis D.* Disputes on the history of Greek mathematics. Edited by Giannes Christianides and Dimitris Dialetis. Texts by S. Unguru, B. L. van der Waerden, H. Freudenthal, A. Weil, J. Christianidis, D. Dialetis. (Greek), Istor. Philos. Epistem., Panepistem. Ekdoseis Kretes, Heraklion, 2006, 147p.
120. *Clements D. L.* An historical contradiction. Missouri J. Math. Sci. **8** (1996), no. 2, 82–88.
121. *Collignon E.* Construction du polygone régulier de 17 côtés, Ass. Franc. Comptes R., **8** (1879), 162–169.
122. *Cormack G. V., Williams H. C.* Some very large primes of the form $k\cdot 2^m+1$. Math. Comput. **35** (1980), no. 152, 1419–1421.
123. *Cosgrave J. B., Dilcher K.* A role for generalized Fermat numbers. Math. Comp. **86** (2017), no. 304, 899–933.
124. *Cosgrave J. B., Dilcher K.* Gauss factorials, Jacobi primes, and generalized Fermat numbers. Punjab Univ. J. Math. (Lahore) **50** (2018), no. 4, 1–21.
125. *Costa E., Gerbicz R., Harvey D.* A search for Wilson primes. Math. Comput. **83** (2014), no. 290, 3071–3091.
126. *Costa E., Harvey D.* Faster deterministic integer factorization. Math. Comput. **83** (2014), no. 285, 339–345.
127. *Covanov S., Thomé E.* Fast integer multiplication using generalized Fermat primes. Math. Comp. **88** (2019), no. 317, 1449–1477.
128. *Cox D. A., Shurman J.* Geometry and number theory on clovers, Amer. Math. Monthly, **112** (2005), no. 8, 682–704.
129. *Crandall R. E., Dilcher K., Pomerance C.* A search for Wieferich and Wilson primes. Math. Comput., **66** (1997), no. 217, 433–449.
130. *Crandall R., Doenias J., Norrie C., Young J.* The twenty-second Fermat number is composite. Math. Comp. **64** (1995), no. 210, 863–868.
131. *Crandall R., Fagin B.* Discrete Weighted Transforms and Large-Integer Arithmetic, Math. Comp. **62** (1994), 305–324.
132. Crandall R. E., Mayer E. W., Papadopoulos J. S. The twenty-fourth Fermat number is composite, Math. Comp., **72** (2003), 1555–1572.
133. *Crandall R., Pomerance C.* Prime Numbers: A Computational Perspective, 2nd ed., Springer, New York, 2005.
134. *Creutzburg R., Grundmann H.-J.* Schnelle digitale Faltung mittels Fermattransformation. Elektron. Inform.-verarb. Kybernetik **21** (1985), 35–46.
135. *Csajbók T., Farkas G., Járai A., Járai Z., Kasza J.* Report on the largest known Sophie Germain and twin primes, Ann. Univ. Sci. Budapest. Sect. Comput. **25** (2005) 181–182
136. *Cunningham A., Western A. E.* On Fermat's numbers. Proc. Lond. Math. Soc. **1** (1904), 175. doi.org/10.1112/plms/s2-1.1.175
137. *Cunningham A. J. C., Woodall H. J.* Factorisation of $Q=(2^q\mp 1)$ and $(q\cdot 2^q\mp 1)$, Messenger Math. **47** (1917), 1–38.
138. *Cunningham A. J. C., Woodall H. J.* Factorisation of $y^n\mp 1$, $y=2,3,5,6,7,10,11,12$ up to high powers (n), Francis Hodgson, London, 1925.
139. *Delcourte M.* Indicateur d'Euler et nombres de Fermat. Mathesis **68** (1959), 350–356.
140. *Deng Yingpu, Huang Dandan* Primality test for numbers of the form $(2p)^{2^n}+1$. Acta Arith. **169** (2015), no. 4, 301–317.
141. *Deng Yingpu, Huang Dandan* Explicit primality criteria for $h\cdot 2^n\pm 1$. Journal de Theorie des Nombres de Bordeaux **28** (2016), no. 1, 55–74.
142. *Deng Yingpu, Lv Chang* Primality test for numbers of the form Ap^n+w_n. J. Discrete Algorithms **33** (2015), 81–92.
143. *DeTemple D. W.* Carlyle circles and the Lemoine simplicity of polygon constructions. Amer. Math. Monthly, **98** (1991), no. 2, 97–108.
144. *Deza E.* Mersenne numbers and Fermat numbers. Selected Chapters of Number Theory: Special

Numbers, 1. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, [2022], ©2022. xx+306p.
145. *Dickson L. E.* Constructions with ruler and compasses, in Monographs on Modern Mathematics (1911), 17-side: 371–373.
146. *Dickson L. E.* History of the theory of numbers. Vol. I: Divisibility and primality. Reprint of the 1919 original published by Carnegie Institution, Washington, DC; Mineola, NY: Dover Publications, 2005, 486p.
147. *Dilcher K.* Fermat numbers, Wieferich and Wilson primes: computations and generalizations. Public-key cryptography and computational number theory (Warsaw, 2000), 29–48, de Gruyter, Berlin, 2001.
148. *F. G. Dorais and D. Klyve* A Wieferich prime search up to 6.7×10^{15}, J. Integer Seq. **14** (2011), Article 11.9.2.
149. *Dubner H.* Generalized Fermat Primes. J. Recr. Math. **18** (1985), 279–280.
150. *Dubner H., Gallot Y.* Distribution of generalized Fermat prime numbers. Math. Comp. **71** (2002), no. 238, 825–832.
151. *Dubner H., Keller W.* Factors of generalized Fermat numbers. Math. Comput., **64** (1995), 397–405.
152. *Dyson F.* The sixth Fermat number and palindromic continued fractions. Enseign. Math. (2) **46** (2000), no. 3–4, 385–389.
153. *Eleuch H.* Notes on generalized Fermat numbers. Appl. Math. Inf. Sci. **6** (2012), no. 3, 491–493.
154. *Euler L.* Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus, Commentarii academiae scientiarum Petropolitanae **6** (1732/33), 1738, pp. 103–107. Reprinted in Opera Omnia I.2, pp. 1–5. Available online at EulerArchive.org.
155. *Euler L.* Theoremata circa divisors numerorum, Novi commentarii academiae scientiarum Petropolitanae **1** (1747/48), 1750, pp. 20–48. Reprinted in Opera Omnia I.2, pp. 62–85. Available online at EulerArchive.org.
156. *Euler L.* Leonhardi Euleri—Opera omnia. Series 4 A. Commercium epistolicum. Vol. 4.1. Leonhardi Euleri commercium epistolicum cum Christiano Goldbach. Pars I/Correspondence of Leonhard Euler with Christian Goldbach. Part I. Original texts in Latin and German. Edited by Franz Lemmermeyer and Martin Mattm'uller. Springer, Basel, 2015. xii+580 pp. ISBN: 978-3-0348-0892-7
157. *Euler L.* Leonhardi Euleri—Opera omnia. Series 4 A. Commercium epistolicum. Vol. 4.2. Leonhardi Euleri commercium epistolicum cum Christiano Goldbach. Pars II/Correspondence of Leonhard Euler with Christian Goldbach. Part II. Original text translated from the Latin and German. Edited by Franz Lemmermeyer and Martin Mattmüller. Springer, Basel, 2015. 5 unnumbered pages+pp. 583–1248. ISBN: 978-3-0348-0880-4
158. *Everest G., van der Poorten A., Shparlinski I., Ward T.*, Recurrence Sequences, Amer. Math. Soc., 2003.
159. *Everest G., Stevens Sh., Tamsett D., Ward T.* Primes Generated by Recurrence Sequences (or arXiv:math/0412079v2 [math.NT], 2006, 1–17.
160. *Fang J.* "J'Accuse": A politics of mathematics. Philosophia Mathematica, **12** (1975), 124–148.
161. *de Fermat P.* Œuvres de Fermat publiées par les soins de MM. Paul Tannery et Charles Henry sous les auspices du ministére de l'instruction publique. Tome premier. Oeuvres mathématiques diverses. Observations sur Diophante. Paris. Gauthier-Villars et Fils. XXXVII+440S, (1891).
162. *de Fermat P.* Œuvres de Fermat publiées par les soins de MM. Paul Tannery et Charles Henry sous les auspices du ministére de l'instruction publique. Tome deuxième. Correspondance. Paris. Gauthier-Villars et Fils. XII + 514p. 1894.
163. *de Fermat P.* Œuvres de Fermat publiées par les soins de MM. Paul Tannery et Charles Henry sous les auspices du ministére de l'instruction publique. Tome troisième. Traductions par M. Paul Tannery: 1. Des écrits et fragments latins de Fermat; 2. de l'Inventum novum de Jacques de Billy; 3. du Commercium epistolicum de Wallis. Paris: Gauthier-Villars et Fils. xvi, 611p. 1896.
164. *de Fermat P.* Œuvres de Fermat publiées par les soins de MM. Paul Tannery et Charles Henry sous les auspices du ministére de l'instruction publique. Tome quatrième. Compléments par M. Charles Henry. Supplément à la Correspondance. Appendice. Notes et Tables. Paris: Gauthier Villars. X u. 277p. 1912.
165. *de Fermat P.* Œuvres. Suppléments aux tomes 1–4, publiées par les soins de MM. Cornelis de Waard, Paul Tannery et Charles Henry sous les auspices du ministére de l'instruction publique. (French)

JFM 48.1104.03 Paris: Gauthier-Villars, XXV u. 188 S. 4 (1922).
166. *de Fermat P.* Mémoires scientifiques, vol. VI, Paul Tannery (ed.), Sciences modernes. Édouard Privat, Toulouse, et Gauthier-Villars, Paris, 1926.
167. *de Fermat P.* Bemerkungen zu Diophant. Aus d. Latein. Übersetzt und mit Anmerk. hrsg. v. Max Miller. Ostwalds Klassiker der exakten Wissenschaften, **234**. Leipzig: Akad. Verlagsges. 49S., 1932.
168. *de Fermat P.* Varia opera mathematica. Tolosae 1679; reprinted: Bruxelles, Culture et Civilisation, 210p., 1969.
169. *de Fermat P.* Œuvres de Pierre Fermat. I: La théorie des nombres. Collection Sciences dans l'Histoire. Paris: Tranduit par Paul Tannery, avec l'introduction et commentaires de R. Rashed, Ch. Houzel et G. Christol. Librairie Scientifique et Technique Albert Blanchard. xii, 503p. (1999).
170. *Filaseta M., Finch C., Kozek M.* On powers associated with Sierpinski numbers, Riesel numbers and Polignac's conjecture, Journal of Number Theory **128** (2008), 1916–1940.
171. *Finch C. E., Jones L.* A curious connection between Fermat numbers and finite groups. Amer. Math. Monthly **109** (2002), no. 6, 517–524.
172. *Fischer A.* Resolutio algebraica aequationis $x^{257} - 1 = 0$. J. Reine Angew. Math. 11 (1934), 201–218.
173. *Freudenthal H.* What is algebra and what has it been in history? Archive for History of Exact Sciences, **16** (1977), no. 3, 189–200.
174. *Fried M.* The discipline of history and the "Modern consensus in the historiography of mathematics". J. Humanist. Math. **4** (2014), no. 2, 124–136.
175. *Fried M.* Ways of relating to the mathematics of the past, J. Humanist. Math. **8** (2018), No. 1, 3–23.
176. *Fried M. Unguru S* Apollonius of Perga's Conica. Text, context, subtext. Mnemosyne. Bibliotheca Classica Batava. Supplementum, 222. Brill, Leiden, 2001. xii+499 pp.
177. *Gabard E., Riesel H.* Corrigenda: "Some factors of the numbers $G_n = 6^{2^n} + 1$ and $H_n = 10^{2^n} + 1$". Math. Comp. **24** (1970), 243.
178. *Gallot Y.* `Proth.exe`: a Windows program for finding very large primes, 1997, `http://www.utm.edu/research/primes/programs/gallot/`
179. *Gauss C. F.* Untersuchungen über höhere Arithmetik. Deutsch von H. Maser. Berlin. Julius Springer. VIII u. 695 S. (1889).
180. *Gauss C. F.* Untersuchungen über höhere Arithmetik. Deutsch herausgegeben von H. Maser Chelsea Publishing Co., New York 1965 xiii+695 pp.
181. *Gauss C. F.* Disquisitiones arithmeticae. Translated and with a preface by Arthur A. Clarke. Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse. Springer-Verlag, New York, 1986. xx+472 pp. ISBN: 0-387-96254-9
182. *Gauss C. F.* Mathematisches Tagebuch, 1796–1814. Fifth edition. With a historical introduction by Kurt-R. Biermann. Revised and with notes by Hans Wußing and Olaf Neumann. Translated from the Latin by E. Schuhmann. Ostwalds Klassiker der Exakten Wissenschaften, **256**. Verlag Harri Deutsch, Frankfurt am Main, 2005. 235p. ISBN: 3-8171-3402-9
183. *Gérard G.* Construction du polygone régulier de 17 côtés, Bull, de Math, élémentaires, **2** (mars, 1897), 164–167.
184. *Gibbins A., Smolinsky L.* Geometric constructions with ellipses. Math. Intell. **31** (2009), no. 1, 57–62.
185. *Giudice F.* Sulla divisione del circolo, Periodico di mat. (3), **9** (1912), 161–169.
186. *Gleason A. M.* Angle trisection, the heptagon and the triskaidecagon, Amer. Math. Monthly, **95** (1988), no. 3, 185–194.
187. *Goldenring R.* Die elementargeometrischen Konstruktionen des regelmäßigen Siebzehnecks, Teubner, Leipzig—Berfin, 1915.
188. *Goldstein C.* Un théorème de Fermat et ses lecteurs. Histoires de Science. Presses Universitaires de Vincennes (PUV), Saint-Denis, 1995. 232p.
189. *Goldstein C.* L'arithmétique de Pierre Fermat dans le contexte de la correspondance de Mersenne: une approche microsociale. Ann. Fac. Sci. Toulouse Math. (6) **18** (2009), Fascicule Spécial, 25–57.
190. *Gostin G. B.* A factor of F_{17}. Math. Comp., **35** (1980), no. 151, 975–976.
191. *Gostin G. B.* New factors of Fermat numbers, Math. Comp. **64** (1995), 393–395.
192. *Gostin G. B., McLaughlin Ph. B., Jr* Six new factors of Fermat numbers. Math. Comput. **38** (1982), no. 158, 645–649.

193. *Gottlieb Ch.* The simple and straightforward construction of the regular 257-gon. Math. Intell. **21** (1999), no. 1, 31–37.
194. *Grau J. M., Oller-Marcén A. M.* An $\widetilde{O}(\log^2(N))$ time primality test for generalized Cullen numbers, Math. Comp. **80** (2011), no. 276, 2315–2323, doi 10.1090/S0025-5718-2011-02489-0
195. *Grau J. M., Oller-Marcén A. M., Sadornil S.* A primality test for $k \cdot p^n + 1$ numbers, Math. Comp. **84** (2015), no. 291, 505–512.
196. Grime J., Knudson K., Pierce P., Veomett E., Whitney G. Beyond pi and e: a collection of constants. Math Horiz. **29** (2022), no. 1, 8–12.
197. *Grunert J. A.* Reguläre Siebzehneck im Kreise, Archiv. f. Math. u. Phys. (Grunert), **42** (1864), 361–374
198. *Güntsche R.* Geometrographische Siebzehnteilung des Kreises, Archiv f. Math. u. Phys. (3), **4** (1903).
199. *Grytczuk A.* Some remarks on Fermat numbers. Discuss. Math. **13** (1993), 69–73.
200. *Grytczuk A., Mądryk B.* Lower bound for the greatest prime divisors of the generalized Fermat numbers. Southeast Asian Bull. Math. **28** (2004), no. 2, 265–268.
201. *Grytczuk A., Wójtowicz, Luca F.* Another note on the greatest prime factors of Fermat numbers. Southeast Asian Bull. Math. **25** (2001), no. 1, 111–115.
202. *Gulliver T. A.* Self-reciprocal polynomials and generalized Fermat numbers, IEEE Trans. Inform. Theory **38** (1992), 1149–1154.
203. *Guthmann A.* Effective primality tests for integers of the forms $N = k3^n + 1$ and $N = k2^m3^n + 1$, BIT **32** (1992) 529–534.
204. *Hadamard J.* Sur la distribution des zéros de la fonction $\xi(s)$ et ses conséquences arithmétiques. Bull. Soc. Math. France, **24** (1896), 199–220.
205. *Hagge K.* Einfache Behandlung der Siebzehnteilung des Kreises, Zeitschr. math. nat. Unterr., **41** (1910), 320–325.
206. *Hagge K.* Einfache Behandlung der 257-teilung des Kreises, Zeitschr. math. nat. Unterr, **41** (1910), 448–458.
207. *Hallyburton J. C., Brillhart J.* Two new factors of Fermat numbers, Math. Comput., **29** (1975), 109–112; Correction, ibid. **30** (1976), 198.
208. *Hardy G. H., Wright E. M.* An introduction to the theory of numbers, 5th ed., Oxford University Press, Oxford, 1979.
209. *Harvey D., Gallot Y.* Distribution of generalized Fermat numbers, Math. Comp. **71** (2001), no. 238, 825–832.
210. *Harvey D., Keller W.* Factors of generalized Fermat numbers, Math. Comp. **64** (1995), no. 209, 397–408.
211. *Heath T. L.* A manual of Greek mathematics. Oxford: Clarendon Press, 1931; Reprinted by Dover Publications in 2003.
212. *Helm L., Moore P., Samidoost P., Woltman G.* Resolution of the mixed Sierpiński problem. Integers **8** (2008), A61, 8 pp.
213. *Hermes J. G.* Zurückführung des Problems der Kreistheilung auf lineare Gleichungen (für Primzahlen von der Form 2m+1). Borchardt J. **87** (1879), 84–114.
214. *Hermes J. G.* Symmetrische und complementäre Verteilung der Indexsummenreste r für Primzahlen von der Form $p = 2^{2^n} + 1$. Hoppe Arch. (2) **4** (1887), 207–218.
215. *Hermes J. G.* Über die Teilung des Kreises in 65537 gleiche Teile. Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse **3** (1894), 170–186.
216. *Hermes J. G.* Das ethische Moment im mathematischen Unterricht. Hoffmann Z. **28** (1897), 91–93.
217. *Hewgill D.* A relationship between Pascal's triangle and Fermat's numbers. Fibonacci Quart. **15** (1977), 183–184.
218. *Hilton P., Pedersen J.* On folding instructions for products of Fermat numbers. Southeast Asian Bull. Math. **18** (1994), no. 2, 19–27.
219. *Hofmann J. E.* Pierre de Fermat. Eine wissenschaftsgeschichtliche Skizze. Scientiarum Historia **13** (1971), 198–238.
220. *Hoüel J.* Sur le polygone régulier de 17 côtés, Nouv. Annales de Math., **16** (1857), 310–311.
221. *Høyrup* What is 'geometric algebra', and what has it been in historiography? (2016), preprint. See http://akira.ruc.dk/ jensh/Publications/ 2016_What%20is%20'Geometric%20Algebra'_S.pdf

222. *Hullyburton J. C., Brillhart J.* Two new factors of Fermat numbers, Math. Comp. **29** (1975), 109–112.
223. *Huron R.* L'aventure mathématique de Fermat. Pierre de Fermat, Toulouse et sa région. Actes du XXIe congrès d'études régionales tenu à Toulouse les 15 et 16 mai 1965. Fédération des Sociétés Académiques et Savantes de Languedoc—Pyrénées—Gascogne, Toulouse, 13–34 (1966).
224. *Indlekofer K.-H., Járai A.* Largest known twin primes and Sophie Germain primes. Math. Comp. **68** (1999), no. 227, 1317–1324.
225. *Itard J.* Les méthodes utilisées par Fermat en théorie des nombres. Rev. Histoire Sci. Appl. **3** (1950), 21–26.
226. *Izotov A. S.* A note on Sierpiński numbers, Fibonacci Quart. **33** (1995) 206–207.
227. *Jarden D.* Divisibility of terms by their subscripts in sequences of sums of powers, Riveon Lematematika, **12** (1958), 78–79, (Hebrew).
228. *Jaroma J. H.* Equivalence of Pepin's and the Lucas—Lehmer tests. Eur. J. Pure Appl. Math. **2** (2009), no. 3, 352–360.
229. *Jaroma J. H., Reddy K. N.* Classical and alternative approaches to the Mersenne and Fermat numbers. Amer. Math. Monthly **114** (2007), no. 8, 677–687.
230. *Jiménez Calvo I.* A note on factors of generalized Fermat numbers. Appl. Math. Lett. **13** (2000), no. 6, 1–5.
231. *Jones R., Pearce J.* A postmodern view of fractions and the reciprocals of Fermat primes. Math. Mag. **73** (2000), 83–97.
232. *Katayama S.* The construction of a regular 17-sided polygon, The Tôhoku Math. Journal, **4** (Feb., 1914), 197–202.
233. *Kazarinoff N. D.* On who first proved the impossibility of constructing certain regular polygons with ruler and compass alone. Amer. Math. Monthly **75** (1968), 647–648.
234. *Kazarinoff N. D.* Ruler and the round. Classic problems in geometric constructions. The Prindle, Weber and Schmidt complementary Series in Mathematics. Vol. 15. Boston—London—Sidney: Prindle, Weber and Schmidt, Inc. xi+138p., 1970; Reprinted Dover Publications, Inc., Mineola, NY, 2003. xii+138p.
235. *Keller W.* Factors of Fermat numbers and large primes of the form $k \cdot 2^n + 1$. Math. Comput., **41** (1983), 661–673.
236. *Keller W.* Prime factors $k \cdot 2^n + 1$ of Fermat numbers F_m and complete factoring status, `www.prothsearch.net/fermat.html`
237. *Keller W.* New Cullen primes. Math. Comput., **64** (1995), 1733–1741.
238. *Klein F.* Vorträge über ausgewählte Fragen der Elementargeometrie. Ausgearbeitet von F. Tägert. (German) JFM 26.0546.01 Leipzig. Teubner. 66S., 1895.
239. *Klein F.* Leçons sur certaines questions de géométrie élémentaire. (Possibilité des constructions géométriques; les polygones réguliers; transcendance des nombres e et π.) Rédaction française par J. Griess. Paris, 1896.
240. *Klein F.* Famous problems of elementary geometry: the duplication of the cube, the trisection of an angle, the quadrature of the circle. An authorized translation of F. Klein's Vorträge über ausgewählte Fragen der Elementar-Geometrie, ausgearbeitet von F. Tägert, by W. W. Beman and D. E. Smith. Boston: Ginn. X + 80, 1897.
241. *Klein F.* Elementarmathematik vom höheren Standpunkte aus, Teil I, Leipzig (1908).
242. *Koblitz N.* Mathematics as propaganda. In Mathematics tomorrow. N. Y.–Heidelberg–Berlin: Springer-Verlag. 1981, 111–120.
243. *Koblitz N.* A tale of three equations; or the emperors have no clothes. The Mathematical Intelligencer **10** (1988), 4–10.
244. *Koblitz N.* Random curves: journeys of a mathematician, Springer, 2008, 392p.
245. *Kochendörffer R.* Einführung in die Algebra. Deutscher Verlag der Wissenschaften, Berlin, 1974, 353S.
246. *Kommerell K.* Über die Konstruktion der regulären Polygone, Math. Annalen, **72** (1912), 588–592.
247. *Knauer J., Richstein J.* The continuing search for Wieferich primes, Math. Comput. **74** (2005), no. 251, 1559–1563 (electronic).
248. *Kraïtchik M.* Sur les nombres de Fermat. C. R. Acad Sci Paris, **180** (1925), 799–801.

249. *Kraitchik M.* Sur le nombre $N = \frac{1}{9}(10^{23} - 1)$ Mathesis **42** (1928), 386–388.
250. *Kraitchik M.* Sur le nombre $N = \frac{1}{9}(10^{23} - 1)$ Mathesis **43** (1929), 154–156.
251. *Kraitchik M.* Les grands nombres premiers, Mathematica, **7** (1933), 92–94.
252. *Kraitchik M.* Les grands nombres premiers, Sphinx **3** (1933), 99–101.
253. *Kraitchik M.* Factorisation de $2^n \pm 1$, Sphinx **8** (1938), 148–150.
254. *Kraitchik M.*, On the factorization $2^n \pm 1$, Scripta Mathematica, **18** (1952), 39–52.
255. *Křížek M.*, O Fermatových číslech. Pokroky Mat. Fyz. Astronom. **40** (1995), no. 5, 243–253.
256. *Křížek M.* Od Fermatových prvočísel ke geometrii. Pokroky Mat. Fyz. Astronom. **46** (2001), no. 3, 179–191.
257. *Křížek M., Chleboun J.* A note on factorization of the Fermat numbers and their factors of the form $3h2^n + 1$. Math. Bohem. **119** (1994), no. 4, 437–445
258. *Křížek M., Chleboun J.* Is any composite Fermat number divisible by the factor $5h2^n + 1$? Number theory (Liptovský Ján, 1995). Tatra Mt. Math. Publ. **11** (1997), 17–21.
259. *Křížek M., Křížek P.* Kouzelný dvanáctistěn pětiúhelníkový. Rozhledy Mat.-Fyz. **74** (1997), 234–238.
260. *Křížek M., Luca F., Somer L.* 17 lectures on Fermat numbers. From number theory to geometry. With a foreword by Alena Šolcová. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, **9**. Springer-Verlag, New York, 2001. xxiv+257p. 2nd edition 2011.
261. *Křížek M., Luca F., Somer L.* On the convergence of series of reciprocals of primes related to the Fermat numbers. J. Number Theory **97** (2002), no. 1, 95–112.
262. *Křížek M., Luca F., Somer L.* Desde los números de Fermat hasta la geometría. Gac. R. Soc. Mat. Esp. **10** (2007), no. 2, 471–483.
263. *Křížek M., Somer L.* A necessary and sufficient condition for the primality of Fermat numbers. Math. Bohem. **126** (2001), no. 3, 541–549.
264. *Křížek M., Somer L.* 17 necessary and sufficient conditions for the primality of Fermat numbers. Math. Inform. Univ. Ostraviensis **11** (2003), no. 1, 73–79.
265. *Landry F.* Aux mathématiciens de toutes les parties du monde. Communication sur la décomposition des nombres en leurs facteurs simples, Librairie Hachette, Paris, 1867.
266. *Landry F.* Décompositions des nombres $2^n \pm 1$ en leurs facteurs premiers de $n = 1$ à $n = 64$ (moins quatre), Librairie Hachette, Paris, 1869.
267. *Landry F.* Sur la décomposition du nombre $2^{64} + 1$. C. R. Acad. Sci. Paris. **91** (1880), 138.
268. *Larras J.* Sur la primarité des nombres de Fermat. C. R. Acad. Sci. Paris **242** (1956), 2203–2204.
269. *Le Maohua* A note on the greatest prime factors of Fermat numbers. Southeast Asian Bull. Math. **22** (1998), no. 1, 41–44.
270. *Lehmer D. H.* Tests for primality by the converse of Fermat's theorem, Bull. Amer. Math. Soc., **33** (1927), 327–340.
271. *Lehmer D. H.* A further note on the converse of Fermat's theorem, Bull. Amer. Math. Soc., **34** (1928), 54–56.
272. *Lehmer D. H.* An extended theory of Lucas' functions, Ann. of Math., **31** (1930), 419–448.
273. *Lehmer D. H.* D. H. Lehmer, Hunting big game in the theory of numbers, Scripta Math., 1933, pp. 229–235.
274. *Lehmer D. H.* The converse of Fermat's theorem. I, II. Amer. Math Monthly, **43** (1936), 347–354; **56** (1949), 300–309.
275. *Lehmer D. H.* On the factors of $2^n \pm 1$, Bull. Amer. Math. Soc. **53** (1947), 164–167
276. *Lenstra A. K., Lenstra H. W., Manasse M. S., Pollard J. M.* The factorisation of the ninth Fermat number. Math. Comput., **61** (1993), 319–149.
277. *Ligh S., Jones P.* Generalized Fermat and Mersenne numbers. Fibonacci Quart. **20** (1982), no. 1, 12–16.
278. *Littlewood J. E.* Littlewood's miscellany. Edited and with a foreword by Béla Bollobás. Cambridge University Press, Cambridge, 1986. vi+200p. ISBN: 0-521-33058-0; 0-521-33702-X
279. *Lucas E.* Sur la recherche des grands nombres premiers, Association Française pour l'Avancement des Sciences, Comptes Rendus, **5** (1876), 61–68.
280. *Lucas E.* Théorèmes d'arithmétique. Atti Reale Accad. Scienze Torino **13** (1878), 271–284.

281. *van Maanen J.* Euler en Goldbach over de getallen van Fermat: $F_n = 2^{2^n} + 1$. Euclides (Groningen) **57** (1981/82), no. 9, 347–356.
282. *Mahoney M. S.* Fermat's mathematics: Proofs and conjectures. Science **178** (1972), no. 4056, 30–36.
283. *Mahoney M. S.* The mathematical career of Pierre de Fermat, 1601–1665. Second edition. Princeton Paperbacks. Princeton University Press, Princeton, NJ, 1994. xxii+432p.
284. *Mahoney M. S.* The histories of computing(s). Interdis. Sci. Rev., **30** (2005), 119–135.
285. *Mahoney M. S.* What makes the history of software hard and why it matters. IEEE Ann. Hist. Comput. **30** (2008), no. 3, 8–18.
286. *Martin G. E.* Geometric constructions, Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1998. xii+203p.
287. *Matthew G., Williams H. C.* Some new primes of the form $k \cdot 2^n + 1$, Math. Comput., **31** (1977), 797–798.
288. *Maywald G. A. R.* Das reguläre 34- und 514-Eck, Vierundzwanzigster Jahresbericht über die Realschule zu Görlitz (Görlitz, 1861), 3–19.
289. *McIntosh R.* A necessary and sufficient condition for the primality of Fermat numbers. Amer. Math. Monthly **90** (1983), no. 2, 98–99.
290. *Montgomery H. L., Wagon S.* A heuristic for the prime number theorem. Math. Intelligencer **28** (2006), no. 3, 6–9.
291. *Morehead J. C.* Note on Fermat's numbers, Bull. Amer. Math. Soc., **11** (1905), 543–545.
292. *Morehead J. C.* Note on the factors of Fermat's numbers, Bull. Amer. Math. Soc., **12** (1906), 449–451.
293. *Morehead J. C., Western A. E.* Note on Fermat's numbers, Bull. Amer. Math. Soc. **16** (1909), 1–6.
294. *Morimoto V.* On prime numbers of Fermat type, Sûgaku **38** (1986), 350–354, (Japanese).
295. *Morrison M. A., Brillhart J.* The factorization of F_7. Bull. Amer. Math. Soc. **77** (1971), 264.
296. *Neugebauer O.* Zur geometrischen Algebra (Studien zur Geschichte der antiken Algebra III). Quellen und Studien zur Geschichte der Mathematik, Astronomie und Physik, **3** (1936), 245–259.
297. *Neukom H.* The Second Life of ENIAC. IEEE Ann. Hist. of Comput., **28** (2006), 4–16.
298. *Odoni R. W. K.* On the prime divisors of the sequence $w_{n+1} = 1 + w_1 w_2 \dots w_n$. J. London Math. Soc., **32** (1985), 1–11.
299. *Ondrejka R.* More on large primes. J. Recreational Math. **11** (1978/79), no. 2, 112–113.
300. *Padoa A.* Poligoni regolari di 34 lati. Trattazione elementare, Boll, di Mat, Bologna, **2** (1903), 2–10.
301. *Pascal E.* Sulla costruzione del poligono regotare di 257 lati, Rend. Acc. Napoli, (2) **1** (1887), 33–39.
302. *Pauker M. G.* Geometrische Verzeichnung des regelmäßigen Siebzehn-Ecks und Zweyhundersiebenundfünfzig-Ecks in den Kreis. Jahresverhandlungen der Kurländischen Gesellschaft für Literatur und Kunst **2** (1822), 160–219.
303. *Paxson G. A.* The compositeness of the thirteenth Fermat number, Math. Comput. **15** (1961), 420
304. *Pepin T.* Sur la formule $2^{2^n} + 1$, C. R. Acad. Sci. Paris, **85**, 1878, 329–331.
305. *Pierpoint J.* On an undemonstrated theorem of the Disquisitiones Arithmeticae. Bull. Amer. Math. Soc., **2** (1895), 77–83.
306. *Pocklington H. C.* The determination of the prime or composite nature of large numbers by Fermat's theorem, Proc. Cambridge Philos. Soc., **18** (1914), 29–30.
307. *Pomerance C., Selfridge J. L., Wagstaff S. S.* The pseudoprimes to $25 \cdot 10^9$. Math. Comput. **35** (1980), no. 151, 1003–1026.
308. *Pomey L.* Sur les nombres de Fermat et de Mersenne. Ann. Fac. Sci. Toulouse Sci. Math. Sci. Phys. (3) **16** (1924), 135–138.
309. *Popelier P. L. A.* The heptadecagon: a curious object . . . . Math. Ed. **9** (1993), no. 3, 154–158.
310. *Popelier P. L. A.* The heptadecagon: a curious object. . . . Math. Student **66** (1997), no. 1–4, 217–223.
311. *Proth F.* Théorèmes sur les nombres premiers, C. R. Acad. Sci. Paris **87** (1878), 926.
312. *Reich K.* Die Entdeckung und frühe Rezeption der Konstruierbarkeit des regelmäßigen 17-Ecks und dessen geometrische Konstruktion durch Johannes Erchinger (1825). Mathesis, 101–118, Verl. Gesch. Nat.wiss. Tech., Berlin, 2000.
313. *Ribenboim P.* 1093. Math. Intelligencer **5** (1983), no. 2, 28–34.
314. *Ribenboim P.* The book of prime number records. 2nd edition. Springer-Verlag, New York, 1989. xxiv+479 pp
315. *Ribenboim P.* The new book of prime number records. Springer-Verlag, New York, 1996. xxiv+541p.

316. *Ribenboim P.* My numbers, my friends. Popular lectures on number theory. Springer-Verlag, New York, 2000. xii+375p.
317. *Ribenboim P.* The little book of bigger primes. 2nd edition. Springer-Verlag, New York, 2004. xxiv+356p.
318. *Ribenboim P.* Die Welt der Primzahlen. Geheimnisse und Rekorde. 2nd revised and updated edition. Translated from the 2004 English original by Jörg Richstein. Updated by Wilfrid Keller. Springer, Heidelberg, 2011. xxv+366 pp.
319. *Richelot F. J.* De resolutione algebraica aequationis $x^{257} = 1$, sive de divisione circuli per bisectionem anguli septies repetitam in partes 257 inter se aequales commentatio coronata. J. reine angew. Math. **9** (1832), 1–26, 146–161, 209–230, 337–358. doi 10.1515 / crll.1832.9.337.
320. *Riesel H.* A note on the prime numbers of the forms $N = (6a+1)2^{2n-1} - 1$ and $M = (6a-1)2^{2n} - 1$, Ark. Mat. **3** (1956), 245–253.
321. *Riesel H.* A factor of the Fermat number F_{19} Math. Comput. **17** (1963), 458.
322. *Riesel H.* Some factors of the numbers $G_n = 6^{2^n} + 1$ and $H_n = 10^{2^n} + 1$. Math. Comput. **23**, 413-415 (1969);
323. *Riesel H.* Common prime factors of the numbers $A_n = a^{2^n} + 1$. Nordisk Tidskr. Informationsbehandling (BIT) **9** (1969), 264–269.
324. *Riesel H.* Lucasian criteria for the primality of $M = h \cdot 2^n - 1$. Math. Comput. **23**, 869-875 (1969).
325. *Riesel H.* Prime numbers and computer methods for factorization. Reprint of the 2nd ed. 1994. Modern Birkhäuser Classics. New York, NY: Birkhäuser/Springer 464 p. (2012).
326. *Riesel H., Björn A.* Generalized Fermat numbers. In Gautschi, Walter (ed.), Mathematics of computation, 1943–1993: a half- century of computational mathematics. Mathematics of computation 50th anniversary symposium, August 9–13, 1993, Vancouver, Canada. Providence, RI: American Mathematical Society. Proc. Symp. Appl. Math. **48** (1994), 583–587.
327. *Robertson J., Snyder C.* A simple geometric construction involving ultraradicals. J. Aust. Math. Soc. **91** (2011), no. 1, 103–124.
328. *Robinson R. M.* Mersenne and Fermat numbers, Proc. Amer. Math. Soc. **5** (1954), 842–846.
329. *Robinson R. M.* Factors of Fermat numbers, Math. Tables Aids Comput., **11** (1957), 21–22.
330. *Robinson R. M.* Some factorizations of numbers of the form $2^n \pm 1$, Math. Tables Aids Comput. **11** (1957) 265–268,
331. *Robinson R. M.* The converse of Fermat's theorem, Amer. Math. Monthly, **64** (1957) 703–710.
332. *Robinson R. M.* A report on primes of the form $k \cdot 2^n + 1$ and on factors of Fermat numbers, Proc. Amer. Math. Soc **9**, 1958, 673–681.
333. *Rödseth O. J.* A note on primality tests for $N = h \cdot 2^n - 1$. BIT **34** (1994), no. 3, 451–454.
334. *Rose A.* Lightning strikes mathematics: ENIAC. Popular Sci., **148** (1946), 83–86.
335. *Rotkiewicz A.* Remarque sur un théorème de F. Proth. Mat. Vesnik **1** (1964), no. 16, 244–245.
336. *Sadornil D., Tena J.* A Lucas—Lehmer primality test for the numbers $n = Ap_1^{s_1} p_2^{s_2} \dots p_t^{s_t} + \omega$. (Spanish. English summary) Fifth Conference on Discrete Mathematics and Computer Science (Spanish), 437–444, Ciencias (Valladolid), 23, Univ. Valladolid, Secr. Publ. Intercamb. Ed., Valladolid, 2006.
337. *Sandifer C. W.* The early mathematics of Leonhard Euler. MAA Spectrum. Mathematical Association of America, Washington, DC, 2007. xx+393p.
338. *Sandifer C. W.* How Euler did it. MAA Spectrum. Mathematical Association of America, Washington, DC, 2007. xiv+237p.
339. *Sandifer C. W.* How Euler did even more. With a preface by Rob Bradley. With chapters by Bradley and Dominic Klyve. Mathematical Association of America, Washington, DC, 2015. xiv+237p.
340. *Schinzel A.* On primitive prime factors of $a^n - b^n$. Proc. Cambridge Philos. Soc. **58** (1962), 555–562.
341. *Schlafly A., Wagon S.* Carmichael's conjecture on the Euler function is valid below 1010,000,000. Math. Comput. **63** (1994), no. 207, 415–419.
342. *Schneider M.* Contextualizing Unguru's 1975 attack on the historiography of ancient Greek mathematics, in: Volker Remmert, Martina Schneider, Henrik Kragh Sörensen (ed.), Historiography of Mathematics in the 19th and 20th centuries, Birkhäuser 2016 245–267.
343. *Schoenborn W.* Elementare Beweise fur einige Gleichungen, die Statt haben zwischen dem Radius eines Kreises, der Seite und der Diagonale der eingeschriebenen regulâren 10-, 14-, 18-, 26-, 34-ecke,

Pr. Krotoschin, 1873
344. *Schröter H.* Zur v. Staudt'schen Construction des regulären Siebenzehnecks. Borchardt J. **75** (1872), 13–24.
345. *Schwendenwein H.* Das regelmä|ßige 257eck, Programm des k. k. (vereinigten) StaatsGimnasiums in Teschen für das Schuljahr 1891//92 (Teschen, 1892), 1–22.
346. *Seelhoff P.* Die Zahlen von der Form $k\cdot 2^n+1$, Zeitschrift für Mathematik und Physik, **31** (1886) 380.
347. *Seelhoff P.* Die Auflösung grosser Zahlen in ihre Factoren, Zeitschrift für Mathematik und Physik, **31** (1886), 166–174.
348. *Seelhoff P.* Die neunte vollkommene Zahl, Zeitschrift für Mathematik und Physik, **31** (1886) 174–178.
349. *Selberg A.* An elementary proof of the prime number theorem. Ann. Math., **85** (1951), 203–362.
350. *Selfridge J. L.* Factors of Fermat numbers, Mathematical Tables and Other Aids to Computation 7 (1953) 274–275.
351. *Selfridge J. L., Hurwitz A.* Fermat numbers and Mersenne numbers. Math. Comput. **18** (1964), 146–148.
352. *Shanks D.* Solved and Unsolved Problems in Number Theory. AMS Chelsea, New York, 2002.
353. *Shevelev V., Gacría-Pulgarín G., Velásquez-Soto J. M., Castillo J. H.* Overpseudoprimes, and Mersenne and Fermat numbers as primover numbers. J. Integer Seq. **15** (2012), no. 7, Article 12.7.7, 10 pp.
354. *Shippee D. E.* Four new factors of Fermat numbers, Math. Comput., **32** (1978), 941.
355. *Shiu P.* Fermat's method of factorisation. Math. Gaz. **99** (2015), no. 544, 97–103.
356. *Shiu P.* Cyclotomy and the heptadecagon. Math. Gaz. bf 100 (2016), no. 548, 288–297.
357. *Shorey T. N., Stewart C. L.* On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. II. J. London Math. Soc. (2) **23** (1981), no. 1, 17–23.
358. *Sierpiński W.* Sur un probl'eme concernant les nombres $k\cdot 2^n+1$, Elem. Math. **15** (1960) 73–74.
359. *Sierpiński W.* Sur un théorème de F. Proth. Mat. Vesnik **1** (1964), no. 16, 243–244.
360. *Simon H. A.* Unclad emperors: A case of mistaken identity The Mathematical Intelligencer, **10** (1988), 11–14.
361. *Smith L. L.* Problems and Solutions: A Construction of the Regular Polygon of Seventeen Sides. Amer. Math. Monthly **27** (1920), no. 7–9, 322–323.
362. *Šolcová A., Křížek M.* Fermat and Mersenne numbers in Pepin's test. Demonstratio Math. **39** (2006), no. 4, 737–742.
363. *Somer L.* My twelve years of collaboration with Michal Křížek on number theory. Applications of mathematics 2012, 267–277, Acad. Sci. Czech Repub. Inst. Math., Prague, 2012.
364. *von Staudt Ch.* Construction des regulären Siebenzehnecks. J. Reine Angew. Math. **24** (1842), 251.
365. *Steggall* The value of $\cos 2\pi/17$ expressed in quadratic radicals, Proc. Edinb. Math. Soc, bf 7 (1888–89), 4–5.
366. *Stein A., Williams H. C.* Explicit primality criteria for $(p-1)p^n-1$. Math. Comput. **69** (2000), no. 232, 1721–1734.
367. *Stewart C. L.* The greatest prime factor of a^n-b^n. Acta Arith. **26** (1974/75), no. 4, 427–433.
368. *Stewart C. L.* On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers. Proc. London Math. Soc. (3) **35** (1977), no. 3, 425–447.
369. *Stewart C. L.* On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. III. J. London Math. Soc. (2) **28** (1983), no. 2, 211–217.
370. *Strommer Gy.* Konstruktion des regulären Siebzehnecks mit Lineal und Streckenübertrager, Acta Math. Hungar., **59** (1992), 217–226; Berichtigung dazu, ibid., **60** (1992), no. 3–4, 269–270.
371. *Strommer Gy.* Konstruktion des regulären Siebzehnecks mit Lineal und Streckenübertrager. Period. Polytech., Mech. Eng. **36** (1992), No. 3–4, 181–190.
372. *Strommer Gy.* Zur Konstruktion des regulären Siebzehnecks. Stud. Sci. Math. Hung. **30** (1995), no. 3–4, 433–441.
373. *Strommer Gy.* Konstruktion des regulären 257-Ecks mit Lineal und Streckenübertrager. Acta Math. Hung. **70** (1996), no. 4, 259–292.
374. *Sun Z.-H.* Primality tests for numbers of the form $K\cdot 2^m\pm 1$. Fibonacci Q. **44** (2006), no. 2, 121–130.
375. *Sze Tsz-Wo.* Deterministic Primality Proving on Proth Numbers arXiv:0812.2596v5 [math.NT], 4 July 2011, 18p.

376. *Tannery P.* Pour l'Histoire de la Science Hellène. De Thalès à Empédocle 2-me éd. par A. Diès, avec une préface de M. Federigo Enriques. Paris, Gauthier-Villars, 1930. 435p.
377. *Trott M.* $\cos(2\pi/257)$ à la Gauss. `Mathematica` Educ. Res. **4** (1995), 31–36.
378. *Trott M.* $\cos(2\pi/257)$ à la Gauss. §1.10.2 in The `Mathematica` GuideBook for Symbolics. New York: Springer-Verlag, 312–321, 2006. `http://www.mathematicaguidebooks.org/`
379. *Unguru S.* On the need to rewrite the history of Greek mathematics, Archive for History of Exact Sciences, **15** (1975/76), no. 1–2, 67–114.
380. *Unguru S.* Fermat revivified, explained, and regained, Francia, Vol. **4** (1976), 774–789.
381. *Unguru S.* History of ancient mathematics: Some reflections of the state of the art. Isis **70** (1979), no. 4, 555–565.
382. *Unguru S., Rowe D.* Does the quadratic equation have Greek roots? A study of 'geometric algebra', 'application of areas', and related problems, Libertas Math., **1** (1981), 1–49.
383. *Unguru S., Rowe D.* Does the quadratic equation have Greek roots? A study of 'geometric algebra', 'application of areas', and related problems. II. Libertas Math., **2** (1982), 1–62.
384. *Uspensky J. V., Heaslet M. A.* Elementary Number Theory, McGraw-Hill, New York, 1939, 317–323.
385. *de la Vallée-Poussin* Recherches analytiques sur la théorie des nombres premiers. — Ann. Soc. Sci. Bruxelles, **202** (1986), 183–256, 281–297
386. *Varshney A. K.* An extension of Fermat's numbers. Proc. Math. Soc. **7** (1991), 163–164.
387. *Vélez P., Luis O.* A Chord Approach for an Alternative Ruler and Compasses Construction of the 17-Side Regular Polygon. Geom. Dedicata **52** (1994), 209–213.
388. *Videla C. R.* On points constructible from conics. Math. Intelligencer, **19** (1997), no. 2, 53–57.
389. *B. L. van der Waerden B. L.* Defence of a 'shocking' point of view, Archive for History of Exact Sciences, **15** (1976), no. 3, 199–210.
390. *Wagstaff S. S.* Computing Euclid's primes. Bull. Inst. Combin. Appl. **8** (1993), 23–32.
391. *Wagstaff S. S. Jr.* The joy of factoring. Student Mathematical Library, 68. Amer. Math. Soc., Providence, RI, 2013. xiv+293p.
392. *Wagstaff S. S. Jr.* The Cunningham project. High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, 367–378, Fields Inst. Commun., 41, Amer. Math. Soc., Providence, RI, 2004.
393. *Wantzel P. L.* Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas, Journal de Mathématiques Pures et Appliquées, **1** (1837), no. 2, 366–372.
394. *Warren L. J., Bray H. G.* On the square-freeness of Fermat and Mersenne numbers. Pacific J. Math. **22** (1967), 563–564.
395. *Weil A.* Review of "The mathematical career of Pierre de Fermat", M. S. Mahoney. Bulletin of the AMS, **6** (1973), 1138–1149.
396. *Weil A.* Who betrayed Euclid? Extract from a letter to the editor. Archive for History of Exact Sciences **19** (1978), no. 2, 91–93.
397. *Weil A.* The History of Mathematics: Why and How. Proceedings of the International Congress of Mathematics, Helsinki 1978. Academia Scientiarum Finnica **1** (1980), 227–236.
398. *Weil A.* Number theory. An approach through history from Hammurapi to Legendre. Reprint of the 1984 edition. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. xxii+377p.
399. *Williams H. C.* The primality of $N = 2A3^n - 1$, Can. Math. Bull. **15** (1972) 585–589.
400. *Williams H. C.* Primality testing on a computer. Ars Combin. **5** (1978), 127–185.
401. *Williams H. C.* The primality of certain integers of the form $2Ar^n - 1$. Acta Arith. **39** (1981), no. 1, 7–17.
402. *Williams H. C.* Factoring on a computer, Math. Intelligencer, **6** (1984), 29–36.
403. *Williams H. C.* Effective primality tests for some integer of the form $A5^n - 1$ and $A7^n - 1$. Math. Comput. **48** (1987), 385–403.
404. *Williams H. C.* A note on the primality of $6^{2^n} + 1$ and $10^{2^n} + 1$, Fibonacci Quart. **26** (1988), no. 4, 296–305.
405. *Williams H. C.* How was F_6 factored? Math. Comp. **61** (1993), 463–474.
406. *Williams H. C.* Édouard Lucas and Primality Testing. Wiley, 1998.

407. *Williams H. C., Seah E.* Some primes of the form $(a^n - 1)/(a - 1)$. Math. Comput. **33** (1979), no. 148, 1337–1342.
408. *Williams, H. C., Shallit J. O.* Factoring integers before computers. In Mathematics of Computation, 1943–1993: A Half-Century of Computational Mathematics (edited by W. Gautschi). Proc. Symp. Appl. Math., **48**, 481–531. Amer. Math. Soc., Providence, RI, 1994.
409. *Williams H. C., Zarnke C. R.* Some prime numbers of the forms $2A3^n + 1$ and $2A3^n - 1$, Math. Comp. **26** (1972), 995–998.
410. *Witno A.* Primes modulo which almost all Fermat numbers are primitive roots. Note Mat. **30** (2010), no. 1, 133–140.
411. *Witno A.* On generalized Fermat numbers $3^{2^n} + 1$. Applied Math. & Information sciences, **4** (2010), no. 3, 307–313.
412. *Witno A.* Hypothetical elite primes for Mersenne numbers and repunits. J. Integer Seq. **24** (2021), no. 1, Article 21.1.7, 11p.
413. *Wolfart J.* Primzahltests und Primfaktorzerlegung. Yearbook: Surveys of mathematics 1981, 161–188, Bibliographisches Inst., Mannheim, 1981.
414. *Wrathall C. P.* New factors of Fermat numbers, Math. Comp. **18** (1964), 324–325.
415. *Yates S.* Sylvester primes. J. Recreational Math. **8** (1975/76), no. 3, 215–217.
416. *Yates S.* Prime divisors of repunits. J. Recreational Math. **8** (1975/76), no. 1, 33–38.
417. *Yates S.* Cofactors of repunits. J. Recreational Math. **8** (1975/76), no. 2, 99–107.
418. *Yates S.* The mystique of repunits. Math. Mag. **51** (1978), no. 1, 22–28.
419. *Yates S.* Repunits and repetends. With a foreword by D. H. Lehmer. Delray Beach, Fla., 1982. vi+215 pp.
420. *Young J.* Large primes and Fermat factors, Math. Comp. **67** (1998), 1735–1738.
421. *Young J., Buell D. A.* The twentieth Fermat number is composite, Math. Comp., **50** (1988), 261–263.
422. *Zeuthen H.G.* Die geometrische Construction als 'Existenzbeweis' in der antiken Geometrie, Math. Ann. **47** (1896), 222–228.
423. *Zsigmondy K.* Zur Theorie der Potenzreste. Monatshefte Math. Phys., **3** (1892), 265–284.

ГРНТИ 00000

Поступила в редакцию 2 января 2014, окончательный вариант 24 января 2016 г.

Computer tools in education, 2023
№ -: 2–55
http://ipo.spb.ru/journal
doi:10.1000/182

Computers as novel mathematical reality. VI. Fermat numbers and their relatives

N. A. Vavilov
SPbU

Abstract

In this part, which constitutes a pendent to the part dedicated to Mersenne numbers, I continue to discuss the fantastic contributions towards the solution o classical problems of number theory achieved over the last decades with the use of computers. Specifically, I address primality testing, factorisations and the search of prime divisors of the numbers of certain special form, primarily Fermat numbers, their friends and relations, such as generalised Fermat numbers, Proth numbers, and the like. Furthermore, we discuss the role of Fermat primes and Pierpoint primes in cyclotomy.

Keywords: *Fermat numbers, generalised Fermat numbers, Proth numbers, Pierpoint numbers, cyclotomy*

Citation: N. A. Vavilov. Computers as novel mathematical reality.
VI. Fermat numbers and their relatives. Computer tools in education, 2023. № -. P. 2–55 :
DOI: http://dx.doi.org/10.1000/182.

Received February 29, 2022, The final version: February 30, 2022

Nikolai Alexandrovich Vavilov, Dr. Sci., Professor SPbU nikolai-vavilov@yandex.ru

**Николай Александрович Вавилов,
д.ф.-м.н, профессор математики
Факультета МКН СПбГУ
nikolai-vavilov@yandex.ru**

© Наши авторы, 2023.
Our authors, 2023.