Компьютерные инструменты в образовании, 2020
№ -: 2–47
УДК: 621.320
http://ipo.spb.ru/journal
doi:10.1000/182

КОМПЬЮТЕР КАК НОВАЯ РЕАЛЬНОСТЬ МАТЕМАТИКИ: III. ЧИСЛА МЕРСЕННА И СУММЫ ДЕЛИТЕЛЕЙ*

Н. А. Вавилов

СПбГУ

Аннотация

Нигде в математике прогресс, связанный с возникновением компьютеров, не является столь зримым, как в аддитивной теории чисел. В этой части будет рассказано о роли компьютеров в исследованиях поведения древнейшей функции, суммы делителей, свойства которой пифагорейцы начали систематически изучать больше 2500 лет назад. Описание траекторий этой функции — совершенные числа, дружественные числа, общительные числа, and the like — составляет содержание нескольких поставленных два–три тысячелетия назад задач, которые не решены до сих пор. Теорема Эвклида—Эйлера сводит описание *четных* совершенных чисел к простым числам Мерсенна. После 1914 года ни одно новое простое число Мерсенна не было открыто вручную, с 1952 года все они открыты при помощи компьютеров. При помощи компьютеров сегодня *каждый день* строится в сотни и тысячи раз больше новых пар дружественных чисел, чем было до этого открыто вручную за несколько тысячелетий. В конце статьи обсуждается гипотеза Каталана—Диксона.

Ключевые слова: *Простые Мерсенна, суммы делителей, совершенные числа, дружественные числа, общительные числа, аликвотные последовательности, гипотеза Каталана—Мерсенна, гипотеза Каталана—Диксона, гипотеза Гая—Селфриджа*

Цитирование: Н. А. Вавилов Компьютер как новая реальность математики // Компьютерные инструменты в образовании, 2020. № -. С. 2–47 .

1. ВВЕДЕНИЕ

Настоящая статья является непосредственным продолжением [3, 4]. В этой части я продолжу обсуждать роль компьютеров в исследованиях по теории чисел, на примере двух следующих классических тем.

• Проверка простоты и факторизация больших чисел, а именно, чисел Мерсенна $M_p = 2^p - 1$, где p простое.

• Задачи о суммах делителей: известные с глубокой древности задачи о совершенных и дружественных числах, их обобщения и варианты.

*Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта N.19-29-14141 изучение взаимосвязи концептуальных математических понятий, их цифровых представлений и смыслов, как основы трансформации школьного математического образования.

Как и в исследованиях по проблеме Варинга [4], в этих темах “особенно отчетливо видно, как трудно дается каждое *реальное* продвижение, и можно непосредственно сравнить результаты усилий разных поколений”. Появление компьютеров изменило здесь *все*. Вот две конкретных и чрезвычайно наглядых иллюстрации этого.

• За примерно 2500 лет вручную было открыто 12 простых Мерсенна, последнее из них в 1914 году, в самом большом из них 39 десятичных цифр. В 1952–2018 годах с помощью компьютеров было открыто еще 39 простых Мерсенна, в самом большом из них, известном сегодня, 24862048 цифр. Почти все самые большие известные сегодня простые числа — все в первой десятке! — это либо числа Мерсенна, либо их старшие делители.

• За всю многотысячелетнюю историю задачи о дружественных парах по состоянию на 1971/72 годы было найдено всего 1108 таких пар, и все, кто их открыл, известны поименно [205–207]. С тех пор с помощью компьютеров были открыты $> 1.2 \cdot 10^9$ таких пар[1].

В то же время, именно появление компьютеров заставило нас осознать *физические* пределы наших вычислительных возможностей. Так, например, мы не в состоянии ответить на вопрос о простоте чисел Мерсенна с большими показателями, подразумевавшийся Мерсенном и явно сформулированный Каталаном, см. § 4. Мы понимаем, что появление новых алгоритмов и новой техники отодвинет сегодняшнюю границу, но теперь мы отчетливо видим и то место, дальше которого мы *никогда* не сможем продвинуться грубой силой, без каких-то совершенно новых математических *идей*.

Все цитируют *начало* фразы, которую Эйнштейн сказал Веблену в 1921 году: "Gott würfelt nicht…" и "Raffiniert ist der Herr Gott doch, aber boshaft ist Er nicht." И редко кто цитирует ее окончание: "Ich habe noch einmal darüber nachgedacht. Vielleicht ist Er doch boshaft." Или, как по-простому выразил ту же мысль Стивен Хокинг: “God not only plays dice. He also sometimes throws the dice where they cannot be seen.” Это дистеистическое наблюдение постоянно приходит в голову при знакомстве с результатами аддитивной теории чисел. Обидно не то, что нам бросают кости[2], обидно, что бросают кости туда, где мы их не можем увидеть. Если гипотезы Каталана—Мерсенна и Каталана—Диксона неверны, то мы имеем все шансы об этом никогда не узнать. Но тогда напрашивается вопрос, что *именно* могло бы значить утверждение, что эти гипотезы неверны? Для кого именно они неверны?

С другой стороны, появление компьютеров в очередной раз полностью изменило представление о полезном и бесполезном, в частности, о том, что такое прикладная математика. Как я уже упоминал в [4], в течение столетий теория чисел выступала как чистая игра ума, как эталон *бесполезности*. Именно это, впрочем, и делало теорию чисел “королевой математики” в глазах Эйлера, Гаусса, Харди, и многих других: “Die Mathematik ist die Königin der Wissenschaften und die Zahlentheorie ist die Königin der Mathematik”.

Примерно в то же время, когда пифагорейцы формулировали свои гипотезы о совершенных и дружественных числах, на другом конце ойкумены было сказано: “Все знают о пользе полезного, но никто не знает о пользе бесполезного”. На самом деле, не только в длительной, но даже и в средней перспективе нет ничего полезнее

[1] Я сознательно не указываю точное значение: сегодня открывают *сотни тысяч* новых таких пар *каждый день*, так что точное количество известных пар наверняка изменится просто за период редакционной подготовки настоящей статьи.

[2] Йан Стюарт [327] поставил вопрос иначе, “do dice play God”?

“бесполезного” знания. Задача о факторизации чисел Мерсенна внезапно стала важнейшей *прикладной* задачей, на которой тестировались все новые процессоры. Именно в процессе подобных теоретико-числовых тестов[3] были обнаружены ошибки в делении чисел с плавающей запятой на первых Пентиумах.

Вот, что, например, пишет по этому поводу Кейт Девлин: “But why does a large supercomputer manufacturer like Cray Research invest so much money in what, from its perspective, is surely little more than a game? The answer is that the computation required to search for large Mersenne primes is a heavy one, stretching over days or weeks, and so it provides an excellent way to test the efficiency and accuracy of a new computer system. The question that interests Cray is, Does their latest computer perform the way it is supposed to? Computer chip manufacturer Intel also uses a Mersenne prime-hunting program to test every Pentium chip before it ships it” [97].

Как и предыдущая статья серии [4], этот текст имеет не научный и не исторический, а именно *методологический* и *методический* характер. Цель ее троякая:

• Проиллюстрировать на простом, доступном и интересном материале как *невероятный масштаб* изменений в математике, вызванных распространением компьютеров, так и возникшие при этом новые ограничения. Граница между осуществимым и неосуществимым никуда не исчезла, она просто несколько сдвинулась.

• Прорекламировать *широчайшие* возможности использования этого материала (и различных его вариантов и обобщений!) в преподавании математики и информатики на всех уровнях и проиллюстрировать эти возможности подборками задач.

• Еще раз привлечь внимание к двум замечательным задачам, сформулированным Эженом Каталаном в 1876 и 1878 годах, по продвижениям в решении которых мы могли бы измерять наш прогресс в вычислительной математике.

В частности, я включил сюда подборку задач, основаных на курсе “Математика и Компьютер”, который мы с Володей Халиным разработали в 2004–2006 годах, и который Саша Юрков полностью обновил в 2018–2020 годах, см. [8] по поводу описания всего проекта. Первая часть, относящаяся к числам Мерсенна, выросла из [6], § 6.4, а вторая, относящаяся к суммам делителей, из [6], §§ 8.1–8.4 и [7], § 4.3. Однако первая часть почти полностью написана заново, а вторая значительно обновлена и расширена.

В части, посвященной числам Мерсенна, гораздо больше исторического и современного *фактического материала*. С другой стороны, часть, посвященная задачам про суммы делителей носит чисто практический характер и, кроме последнего параграфа, состоит главным образом из обработки задач, которые мы с Володей Халиным фактически предлагали студентам. Код в Mathematica в основном просто воспроизведен оттуда, иногда с чуть измененными по сравнению с [6, 7] параметрами.

Количество текстов *непосредственно* относящихся к этим и близким направлениям теории чисел измеряется многими тысячами и даже главные из них невозможно отразить в рамках журнальной статьи[4]. Поэтому, кроме книг, обзоров и текстов общего характера, я включаю в библиографию только несколько ключевых классических текстов и рандомные статьи, которые мы использовали для составления задач. Последние 2–3 десятилетия текущее состояние меняется так быстро, что прогресс можно отслеживать только по специализированным сайтам, которые будут упомянуты непосредственно в соответствующих местах текста.

[3] В действительности Томас Найсли обнаружил в 1994 году FDIV bug в процессе вычисления константы Бруна, суммы обратных величин к простым близнецам.

[4] Это совсем небанально сделать даже в формате компендиума [311, 312].

Имеется огромное количество текстов общего характера по теории чисел, самого различного уровня, в которых обсуждаются простые Мерсенна и суммы делителей. Фактически при составлении этих задач в [6] мы пользовались книгами Эрика Баха и Джеффри Шаллита [17], Анри Коэна [79], Ричарда Крэндалла и Карла Померанса [89][5], Ричарда Гая [140], Владыслава Наркевича [239], Пауло Рибенбойма [289] и Вацлава Серпиньского [320][6].

Известная с библейских времен поговорка утверждает, что “нет ничего нового под Солнцем, но есть много старых вещей, которых мы не знаем.” В частности, при работе над [6] мы не учитывали большое количество интересных текстов, в том числе и таких, где специально рассматриваются факторизации чисел специального вида, например, брошюру Карлоса Морейро и Николау Салданья [237] и книгу Хью Уилльямса [359], специально посвященные тесту Люка и его вариантам. Номинально книга Альберта Бейлера [24] относится к рекреативной математике, но фактически это весьма содержательный текст, содержащий ссылки на оригинальные работы.

К счастью, в том, что касается истории всех рассматриваемых здесь вопросов до начала 1920-х годов есть циклоп[ед]ический по охвату текст Леонарда Диксона [101], где упомянуты, хотя и в телеграфном стиле, *все* классические тексты. Книга Харольда Эдвардса [12] содержит очень интересную историческую реконструкцию того, как Ферма, Мерсенн и их современники искали простые делители чисел Мерсенна. Полными и надежными источниками о том, что было известно о числах Мерсенна в 1920-е и 1930-е годы служат статьи Деррика Лемера и Ральфа Арчибальда [15, 213, 218]. В брошюре Гая Хэуорта [167] информация с той же полнотой доведена до начала 1990-х, после чего это стало уже физически невозможно. В статьях Хью Уилльямса и Джеффри Шаллита [360] и Сэмюэла Уогстаффа [351] детально описываются методы, использовавшиеся для факторизации чисел специального вида до 1947 года и в компьютерную эпоху, соответственно.

Разумеется, с тех пор появилось огромное количество новых текстов. Среди более новых книг, где приводятся интересные утверждения и формулируются новые гипотезы в этом направлении, упомяну книги Эндрю Гранвилля [134], Сэмюэла Уогстаффа [352][7] и Джона Уоткинса [356].

Вот еще несколько замечательных научно популярных текстов, которые можно использовать для приобщения к математике детей, широких народных масс и любознательных пенсионеров[8]: Мартин Гарднер [127], Джон Конвей и Ричард Гай [83], Кейт Девлин [97], Йан Стюарт [326] и Маркус дю Сотой [313], последние три содержат популярные, но аккуратные и подробные обзоры использования компьютеров в задачах факторизации. Книга Констанс Рид [284] предсказуемым образом[9] содержит

[5] Не удержусь от того, чтобы процитировать следующий живописный фрагмент из рецензии Роберта Юричевича на эту книгу: “It seems that we will only begin to seriously understand the sequence of prime numbers when we are freely able to work with prime numbers which are at least 1 million digits in length. It would certainly be fantastic to discover a trick in order to do arithmetic with such huge fundamental building numbers without the aid of a computing machine. It would also be nice to be able to fly without the aid of a flying machine. Plainly, the computer is an indispensible tool to the research mathematician studying the sequence of prime numbers, as well as to the mathematician applying prime number theory in industry.” — “Кабы мне такие перья, да такие крылья,. . . ”

[6] Фактически, как для [89] и [140], мы, к сожалению, пользовались предыдущим изданием. Второе издание существенно расширено и обновлено именно в части, относящейся к факторизации чисел Мерсенна и роли в этом компьютеров.

[7] "Multiply $2071723 \times 5363222357$ by hand. Feel the joy.”

[8] “There is much pleasure to be gained from useless knowledge.”

[9] Констанс Рид сестра Джулии Робинсон.

описание открытия новых простых Мерсенна Рафаэлем Робинсоном.

Непрерывный текст Рибенбойма [286–289] — а здесь он процитирован далеко не с самого начала! — служил заменой интернета в докомпьютерную эпоху, особенно с учетом авторских обновлений в русских, французских, немецких и португальских переводах. Отдельно отмечу последний немецкий перевод [290], где с момента выхода английского издания многое добавилось. Книги Рибенбойма элементарные, но все же относятся не к научно-популярному жанру, а к математическому просвещению. В них приводятся простые, но настоящие доказательства большого количества фактов.

2. РУКОТВОРНЫЕ ПРОСТЫЕ ЧИСЛА МЕРСЕННА

В этом и следующем параграфе мы обсудим важнейший класс простых, возникающий во многих вопросах теории чисел, алгебры и комбинаторики.

2.1. Простые Мерсенна

Если m — собственный делитель n, то x^n-1 делится на x^m-1. Поэтому если $M_n=2^n-1$ простое, то n простое. Числа вида $M_p=2^p-1$, где p простое, называются **числами Мерсенна**. Почти все самые большие известные простые числа являются **простыми числами Мерсенна**.

• Простота первых трех из чисел

$$M_2=3,\qquad M_3=7,\qquad M_5=31,\qquad M_7=127$$

известна с глубокой древности, простота четвертого из них явно упоминалась не позже III века до Н.Э. В середине XV века была установлена также простота числа

$$M_{13}=8191.$$

Поэтому большинство ранних авторов были уверены, что верно и обратное, т.е. если p простое, то M_p тоже простое.

• Это заблуждение было развеяно в 1536 году Худальрикусом Региусом, который заметил, что $M_{11}-1=2047=23\cdot 89$, как мы скоро увидим, эта факторизация не случайна, $23=2\cdot 11+1$.

• В 1588 году Пьетро Катальди[10], проверил, что

$$M_{17}=131071,\qquad M_{19}=524287$$

простые, при этом он заявил, что M_{23}, M_{29}, M_{31} и M_{37} тоже простые.

• В 1640 году Пьер де Ферма проверил, что в действительности M_{23} и M_{37} составные. Позже Леонард Эйлер заметил, что и M_{29} тоже составное, а в 1772 году показал, что

$$M_{31}=2147483647$$

[10] Формально книга *Trattato dè Numeri Perfetti* [57], содержащая эти результаты, опубликована в 1603 году. Но, первая ее фраза такова: “Nel trattato dè numeri perfetti, che giàsino dell’anno 1588 composi,…”. На странице 40 воспроизведена таблица всех простых чисел $p<750$. Поскольку $727^2=528529>M_{19}$, даже не особенно вчитываясь в текст понятно, как именно действовал Катальди. Он пробовал в качестве возможных делителей M_{13}, M_{17}, M_{19} все простые, не превосходящие целую часть их квадратных корней — “sua prossima radice quadra”. Сомнительно, чтобы Катальди довел такого рода прямые вычисления до $2897^2=8392609>M_{23}$.

простое. При этом оба они пользовались сравнениями для делителей чисел M_p, которые мы напоминаем в § 4.

• Во всех обычных текстах по теории чисел говорится, что в связи с проблемой четных совершенных чисел Марин Мерсенн в 1644 году утверждал в предисловии к своей книге *Cogitata Physica-Mathematica* [230], что числа

$$M_p, \qquad p = 2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 67,\ 127,\ 257$$

просты, а все остальные числа M_p для $p \le 257$ составные. Как позже выяснилось, этот список верен до $p = 31$, но дальше содержал ошибки. Однако эти ошибки были исправлены только в конце XIX и начале XX веков.

Так примерно это излагается и в нашем задачнике [6]. Однако с тех пор я прочел первоисточники и в следующем пункте скорректирую эту популярную картинку. В действительности Мерсенн утверждал лишь, что до M_{31} нет других новых простых Мерсенна. А числа M_{67}, M_{127} и M_{257} возникли в процессе попытки сформулировать гораздо более трудную и интересную гипотезу.

2.2. Что на самом деле утверждал Мерсенн

В издании 1644 года [230] я не нашел ничего про числа Мерсенна, кроме пункта XIX введения, где говорится про *совершенные* числа. А именно, Мерсенн отмечает, что из 28 чисел, которые указаны в трактате Пьетро Бонго как совершенные, в действительности 20 совершенными не являются: “solos octo perfectos habeat videlicet 6, 28, 496, 8128, 23550336, 8589869056, 137438691328, 2305843008139952128”. Так в тексте. Очевидно, опечатка. Пятое число должно быть 33550336, *все* остальные, включая 2305843008139952128, совершенность которого была доказана Эйлером, верны.

Далее Мерсенн утверждает следующее: “Porro numeri perfecti adeo rari sunt, vt vndecim dumtaxat potuerint hactenus inueniri: hoc est, alii tres à Bongianis differentes: neque enim vllus est alius perfectus ab illis octo, nisi superes exponentem numerum 62, progressionis duplae ab 1 incipientis.” А именно, что совершенные числа *настолько* редки, что со времени Бонго удалось открыть всего три новых, причем ни одного из них меньшего чем. . . — и вот тут происходит нечто совершенно загадочное. Если читать 62 так же, как 68, 128 и 258 в дальнейшем тексте, то речь здесь идет именно о числе $2^{60}M_{61}$.

Однако продолжение не оставляет возможности такого толкования: “Nonus enim perfectus est potestas exponentis 68 minus 1. Decimus, potestas exponentis 128 minus 1. Vndecimus denique, potestas 258 minus 1, hoc est potestas 257, vnitate decurtata, multiplicata per potestatem 256”. Здесь прямо утверждается, что $2^{66}M_{67}$, $2^{126}M_{127}$ и $2^{256}M_{257}$ еще три совершенных числа, девятое, десятое и одинадцатое — в порядке обнаружения, а не в порядке величины. Я не вижу здесь утверждения, что других совершенных чисел нет.

До конца пункта XIX Мерсенн продолжает рассуждать на эту тему. В качестве вызова он предлагает найти еще 11 совершенных чисел, но заявляет, что это будет чрезвычайно трудно, поскольку существуют огромные интервалы степеней, где простых Мерсенна вообще нет. При этом он делает удивительные конкретные предсказания, в частности, предполагает отсутствие простых Мерсенна M_p в интервале $1050000 < p < 2090000$. Как мы вскоре увидим, даже с использованием суперкомпьютеров вычисления с числами такого размера стали нам доступны только начиная с середины 1990-х годов.

И действительно, после этого он утверждает, что предъявить бесконечное[11] количество совершенных чисел будет чрезвычайно трудно. Это связано с тем, что даже для нескольких чисел, у которых всего-то 15–20 знаков(!!) чтобы проверить, являются они простыми или составными, может потребоваться столетие вычислений[12].

В научно-популярных книгах высказывается мнение, что он просто воспроизвел этот список из писем Ферма и Френикля, сделав при переписывании *опечатку*, 67 вместо 61. С другой стороны, сам список и точность догадки относительно числа M_{127} совершенно удивительны и требуют объяснения. Обе эти точки зрения присутствуют в следующем фрагменте из Диксоновской “Истории”: “In a letter to Tannery[13] Lucas stated that Mersenne (1644, 1647) implied that a necessary and sufficient condition that $2^p - 1$ be a prime is that p be a prime of one of the forms $2^{2n} + 1$, $2^{2n} \pm 3$, $2^{2n+1} - 1$. Tannery expressed his belief that the theorem was empirical and due to Frenicle, rather than to Fermat[14] . . . ”, [101].

Воспроизведу тот фрагмент текста 1647 года [231], на который здесь ссылаются Люка и Диксон. Мерсенн явно выписывает все цифры числа M_{67}, в количестве 21 штуки, что делает заявление об “опечатке” *абсурдным*. Очевидно, что он пытается здесь формулировать ОБЩЕЕ ПРАВИЛО простоты чисел Мерсенна. При этом он не отмечает отдельно случай M_{257}, и не говорит ничего про конкретный интервал.

Вот что в точности говорится: “Sequens Regula numeris primis agnoscendis admodum vtilis videlicet numerum binarii analogicum vnitate decurtatum, cuius exponens primus, ternario, vel minore numero ab aliquo binarii analogi, cuius exponens sit par, est numerus primus. Verbi gratiâ, 7 est exponens 128, nam 7 differt ternario à 4 binarii analogo, cuius exponens est par, ideoque 127, est primus. Præterea si 64, ternarius addatur, surget primus 67, adque adeo 67, potestas plus 1, erit numerus, qui sequitur, primus 147573952589676412927: quorum hæc est proprietas, vt in sui medium ducti numeros perfectos generent: quod intellige de solis numeris primis, qui sunt vnitate minores numero binarii analogo, eapropter non conuenit hæc proprietas numero primo 5, sed numeris 3, 7, 31, 127, 8191, 131071, 524287, 2147483647, & omnibus alius eiusmodi generis”, [231], страница 182.

В конце отрывка снова воспроизводится список первых *восьми* чисел Мерсенна, относительно которых он не имел сомнения. Предшествующий текст может быть истолкован в таком духе, как пишет Люка, что простота M_p определяется близостью p к степени двойки. В дальнейшем многие, в частности, Ральф Арчибальд, Стиллман Дрейк, Малколм Хейуорт [15, 103, 169], предлагали свои интерпретации, но, как мне кажется, никому не удалось объяснить список Мерсенна таким образом, чтобы включить M_{13} и исключить при этом M_{61}. Поэтому отсутствие упоминания M_{61} действительно представляет собой загадку и я начинаю верить, что увидев рядом в тексте M_{61} и M_{67} перво[о]печатники сочли это повтором и выбросили M_{61} при редактировании текста.

[11] В соответствии с обычаем того времени он говорит “любое предписанное количество”.

[12] Оба эти фрагмента текста полностью воспроизведены на латыни в статье Уолтера Уильяма Роуз Болла [310], где их, конечно, несколько легче читать, чем в оригинальном издании XVII века. Последняя фраза этого пункта в оригинале выглядит так: “agnoscere num dati numeri 15, aut 20 caracteribus constantes, sint primi necne, cùm nequidem saeculum integrum huic examini, quocumque modo hactenus cognito, sufficiat.” Отсюда Роуз Болл выводит следующее заключение: “From the last clause it would appear that he did not know how the result was demonstrated”.

[13] Из общих соображений очевидно, что имеется в виду Поль Таннери, который примерно в это время занимался подготовкой изданий трудов Ферма и Декарта, а не его брат Жюль Таннери.

[14] “. . . valeurs qu’il tenait, supposent certains, de Fermat lui-même”, [274].

2.3. Критерий Люка—Лемера

Простоту первых чисел Мерсенна легко установить пробными делениями — используя для сокращения перебора сравнения для делителей, как это делали Ферма и Эйлер, см. § 4. В то же время, проверка подобными прямыми методами простоты следующих чисел из списка Мерсенна, вот хотя бы M_{67}, представляла по тем временам уже довольно серьезную вычислительную задачу.

Поэтому следующие простые Мерсенна были открыты только в конце XIX века. Как уже упоминалось, почти все самые большие известные сегодня простые числа являются числами Мерсенна. Это связано с тем, что проверять простоту числа M_p *значительно* проще, чем простоту других чисел того же порядка.

А именно, для чисел Мерсенна имеется следующий критерий простоты, открытый в 1876 году Эдуаром Люка [224] и упрощенный в 1930 году Дерриком Лемером[15] [210, 214]. Чтобы сформулировать этот критерий, определим прежде всего **числа Люка** L_n. Положим $L_1 = 4$ и зададим следующие числа рекуррентно посредством $L_{n+1} = L_n^2 - 2$.

Так вот, **критерий Люка—Лемера** утверждает, что для того, чтобы выяснить, является ли число Мерсенна M_p простым, необходимо выполнить всего *одно деление*, а именно, M_p в том и только том случае простое, когда оно делит L_{p-1}, см. книгу Хью Вилльямса [359] по поводу истории этой идеи и ее развития. Простые доказательства приведены в статьях [54, 189, 309, 358].

До 1876 года простота чисел Мерсенна доказывалась строго в порядке их возрастания. А именно, обозначим n-е простое число Мерсенна через $M(n)$. Тогда изложенная в предыдущем пункте история может быть резюмирована как

$$M(1) = M_2 = 3, \quad M(2) = M_3 = 7, \quad M(3) = M_5 = 31, \quad M(4) = M_7 = 127,$$
$$M(5) = M_{13} = 8191, \quad M(6) = M_{17} = 131071, \quad M(7) = M_{19} = 524287,$$
$$M(8) = M_{31} = 2147483647.$$

Однако, начиная с Люка простые числа Мерсенна открывались не обязательно в порядке возрастания номера.

• В 1876 году пользуясь своим критерием Эдуар Люка доказал, что число M_{67} составное (по этому поводу см. § 4) и подтвердил, что число M_{127} простое:

$$M(12) = M_{127} = 170141183460469231731687303715884105727,$$

девятое в порядке открытия, но *двенадцатое* по величине.

Рекордное на то время число M_{127} у которого 39 цифр, оставалось *самым большим известным простым числом* на протяжении 75 лет! Мы расскажем об этом чуть больше в § 4.

Открытие трех *предшествующих* простых чисел Мерсенна $M(9)$, $M(10)$ и $M(11)$, опровергающих то, что обычно называется гипотезой Мерсенна, потребовало еще 38 лет. Интересно, что все они были открыты *любителями*!

[15] Дерриком *Генри* Лемером (1905–1991), мужем Эммы Марковны Лемер (1906–2007), которого не следует путать с его отцом Дерриком *Нортоном* Лемером (1867–1938), тоже профессором Университета Калифорнии в Беркли, который тоже занимался *ровно* такого же рода теорией чисел. Впрочем их систематически смешивают и основные базы данных: в MatSciNet работы Д. Н. Лемера не определяются, а в ZBMath приписываются Д. Г. Лемеру. Поэтому единственный способ состоит в том, чтобы смотреть сами тексты статей. Упомянутые далее обобщения совершенных чисел, это Д. Н. Лемер. Но в данном случае речь идет именно о работах Д. Г. Лемера, составивших содержание его Ph. D. в 1930 году.

• *Девятое* число Мерсенна

$$M(9) = M_{61} = 2305843009213693951$$

открыл в 1883 году Иван Михеевич Первушин[16],[17],[18].

• *Десятое* и *одинадцатое* числа Мерсенна

$$M(10) = M_{89} = 618970019642690137449562111,$$
$$M(11) = M_{107} = 162259276829213363391578010288127$$

открыл Ральф Эрнест Пауэрс в 1911 году [278, 279] и в 1914 году [280, 281], соответственно.

Число M_{107} было *последним* числом Мерсенна, открытым вручную. Впрочем, в своих вычислениях сам Пауэрс пользовался *арифмометром*! Следующие два простых числа Мерсенна M_{521} и M_{607} были открыты уже с использованием компьютера, ровно за день до его смерти[19].

Сам Лемер в 1927–1932 годах завершил проверку первоначального предположения Мерсенна, доказав, что M_{257} составное. В дальнейшем выяснилось, что ни одного нового простого числа вида M_p, $p \le 257$, нет, а следующие простые Мерсенна уже гораздо больше и вряд ли могли быть когда-либо обнаружены без компьютера.

2.4. Задачи для студентов экономистов

Впрочем, сегодня на бытовом компьютере можно повторить не только все эти результаты, но и ранние компьютерные вычисления за несколько секунд. Воспроизведем несколько задач из [6], которые мы с Володей Халиным фактически предлагали студентам направлений “информационные системы в экономике” и “экономическая кибернетика”.

Задача. Найдите первые 17 простых чисел Мерсенна и исправьте все ошибки в списке Мерсенна.

Ответ. Можно, например, так:

[16] Сельский священник Иван Первушин был старшим из 17 детей в семье, что с детства вызвало у него интерес к простым числам. Впрочем, Википедия утверждает, что в семье его родителей было всего 16 детей, что, конечно, объясняло бы его интерес к степеням двойки. До открытия простого Мерсенна M_{61} в 1877 году он нашел простой делитель у числа Ферма F_{12}, а в 1878 году у числа Ферма F_{23}. До него найти новые делители у чисел Ферма получалось только у Эйлера и Клаузена, и одновременно с ним — у Люка.

[17] Я не смог найти оригинальную публикацию Первушина, а только упоминание его результата в Бюллетене Петербургской Академии. Вот живописный фрагмент из доклада Имшенецкого и Буняковского: “Tout en laissant à la charge de l’auteur la responsabilité pour l’exactitude du résultat qu’il a obtenu au bout de ses longs et fatigants calculs, — nous devons constater, pour sauvegarder son droit de priorité, que 1^o Le manuscrit du père P e r v o u c h i n e contenant sa communication de l’année 1883, est déposé aux Archives de notre Académie; ce document est accompagné de quelques tables, calculées par l’auteur, et destinées a faciliter la vérification du résultat qu’il a obtenu.”, [178].

[18] “Кроме того была еше статья (C a t a l a n) по этому вопросу, но с этой статьей я, к сожалению, был лишен возможности познакомиться, так как я этого журнала не мог в Москве нигде достать.”, [11].

[19] Воспроизведу некролог Пауэрса, написанный Лемером для AMS, в котором упоминаются оба эти обстоятельства: “This amateur mathematician died on Jan. 31, 1952, at Puente, California. He would have been 77 years old on April 27. Mr. Powers was more responsible than any other man for the demonstration of the failure of Mersenne’s conjecture. He proved that $2^{89} - 1$ and $2^{107} - 1$ were primes, and that several other Mersenne numbers were composite by long and laborious desk machine calculations. He was not aware of the discovery, the night before his death, of two new Mersenne primes (MTAC, v. 6, p. 61). Mr. Powers was born in Fountain, Colorado, and spent most of his life in Denver”.

```
Select[Table[2^Prime[n]-1,{n,1,400}],PrimeQ]
```

Топорно, но для столь маленьких чисел это не имеет никакого значения. Напомним, что функция `Select[list,crit]` осуществляет выбор элементов из списка `list`, удовлетворяющих критерию `crit`. В данном случае из списка первых 400 чисел вида $2^p - 1$, где p простое, выбираются числа, удовлетворяющие критерию `PrimeQ`, осуществляющему проверку на простоту.

Кроме всех чисел открытых вручную при этом получатся и первые пять новых простых чисел Мерсенна открытых в Рафаэлем Робинсоном в 1952 году уже с помощью компьютера, в том числе те два открытых в январе, которые упоминает Лемер. У них 157 цифр

$$M(13) = M_{521} = 68\,64797\,66013\,06097\,14981\,90079\,90813\,93217\,26943\,53001\,43305\,40939$$
$$44634\,59185\,54318\,33976\,56052\,12255\,96406\,61454\,55497\,72963$$
$$11391\,48085\,80371\,21987\,99971\,66438\,12574\,02829\,11150\,57151$$

и, соответственно, 183 цифры:

$$M(14) = M_{607} = 531\,13799\,28167\,67098\,68958\,82065\,52468\,62732\,95931\,17727\,03192$$
$$31994\,44138\,20040\,35598\,60852\,24273\,91625\,02265\,22928\,56688\,89329\,48624\,65010$$
$$15346\,57933\,76527\,07239\,40951\,99787\,66587\,35194\,38312\,70835\,39321\,90317\,28127$$

Ясно, что простоту этих чисел было бы *крайне* затруднительно проверить вручную. В следующих трех числах $M(15) = M_{1279}$, $M(16) = M_{2203}$ и $M(17) = M_{2281}$, открытых Робинсоном в июне–октябре 1952 года, уже 386, 664 и 687 цифр, соответственно, и я не буду воспроизводить их здесь. Мы вернемся к их обсуждению в следующем параграфе.

Задача. Напишите программу для вычисления чисел Люка.

Ответ. Поскольку рекуррентная программа очевидна, ограничимся перечислением нескольких первых L_n:

$$L_2 = 14, \quad L_3 = 194, \quad L_4 = 37634, \quad L_5 = 1416317954,$$
$$L_6 = 2005956546822746114,$$
$$L_7 = 4023861667741036022825635656102100994.$$

Числа Люка довольно быстро растут, уже у L_{100} больше, чем 10^{27} цифр.

Задача. Напишите тест простоты чисел Мерсенна, основанный на критерии Люка—Лемера и сравните скорость его работы с `PrimeQ`.

3. НЕРУКОТВОРНЫЕ ПРОСТЫЕ ЧИСЛА МЕРСЕННА

Между 1914 и 1952 годами не было открыто ни одного нового простого Мерсенна, а все, которые были открыты после этого, были открыты с использованием компьютеров.

3.1. Новые простые числа Мерсенна: 1952–1996

История открытия простых чисел Мерсенна от начала компьютерной эпохи до проекта GIMPS детально изложена в первой главе книги Кейта Девлина “Золотой

век математики”, [97]. Первые попытки найти новые простые Мерсенна при помощи компьютеров, впрочем безуспешные, предприняли Максвелл Ньюман 1949 году и Алан Тьюринг в 1951 году. Большинство из тех, кто отрывал числа Мерсенна в те годы, были в игре, они профессионально занимались либо теорией чисел, либо компьютерными вычислениями.

• Как уже упомянуто в предыдущем параграфе, 30 января 1952 года Рафаэль Робинсон[20] открыл на компьютере SWAC (= Standards Western Automatic Computer) Национального Бюро Стандартов в Лос Анжелесе следующие два простых Мерсенна, а позже в том же году еще три:

$M(13) = M_{521}$	157 цифр	30.01.1952
$M(14) = M_{607}$	183 цифр	30.01.1952
$M(15) = M_{1,279}$	386 цифр	25.06.1952
$M(16) = M_{2,203}$	664 цифр	07.10.1952
$M(17) = M_{2,281}$	687 цифр	09.10.1952

Это были самые большие простые числа известные в то время. На самом деле Робинсон проверил на простоту все числа Мерсенна M_p для $p \le 2297$. Для числа $M_{2,281}$ собственно вычисление (после написания и отладки программы) заняло на SWAC около часа. Для сравнения, Макдивитт [225] прикидывает, что от человека вооруженного карманным калькулятором, вычисление подобного объема потребовало бы около 50 нормальных рабочих лет. Смешно даже думать, что какое-то из больших чисел Мерсенна могло бы *когда-либо* быть открыто человеком — unless. . .

Открытие после 75-летнего перерыва больших простых чисел было, несомненно, сенсацией. В историческом контексте это событие обсуждают Лемер [215, 216], Хорас Улер [346–348], Тёгер Банг [18] и Ханс Ризель [302] Основные идеи и некоторые детали вычислений представлены в чрезвычайно интересной статье самого Робинсона [307].

• В 1957 году Ханс Ризель[21] нашел на первом шведском *ламповом* компьютере BESK (= Binär Elektronisk Sekvens Kalkylator), на котором он работал с 1953 года, следующее простое Мерсенна, [303, 304]:

$M(18) = M_{3,217}$	969 цифр	08.09.1957

• В 1961 году Александр Гурвиц на IBM 7090 в UCLA открыл следующие два простых Мерсенна [174]. По тем временам это был вполне серьезный компьютер, уже *на транзисторах*, который создавался специально для научных вычислений и стоил 2–3M USD. Тем не менее, проведение теста Люка—Лемера для $M(20)$ потребовало на нем 50 минут машинного времени — сегодня, конечно, любое карманное устройство справляется с этим за секунды.

$M(19) = M_{4,253}$	1,281 цифр	03.11.1961
$M(20) = M_{4,423}$	1,332 цифр	03.11.1961

В статье Селфриджа и Гурвица [316] можно найти описание встретившихся при этом проблем. Понятно, что само умножение многозначных чисел в то время было проблемой

[20] Тот самый Рафаэль Робинсон, знаменитый логик, муж Джулии Робинсон.

[21] Тот самый Ханс Ризель, который известен своими работами по факторизации чисел вида $k \cdot 2^n \pm 1$: тест Люка—Лемера—Ризеля, числа Ризеля, решето Ризеля и т.д.

и потребовало разработки новых алгоритмов, основанных на FFT. Но были и совершенно неожиданные для наших сегодняшних понятий проблемы, например, возникновение машинных сбоев и расхождений в ответах между разными компьютерами!

• В 1963 году Дональд Джиллис на ILLIAC II открыл еще три числа Мерсенна [128]:

$M(21) = M_{9,689}$	2,917 цифр	11.05.1963
$M(22) = M_{9,941}$	2,993 цифр	16.05.1963
$M(23) = M_{11,213}$	3,376 цифр	02.06.1963

В действительности Дональд Джиллис был одним из разработчиков ILLIAC II и поиск чисел Мерсенна был частью *тестирования* только что собранной в университете Иллинойса, Урбана—Шампань, системы, которое продолжалось примерно три недели. Машинные сбои продолжали свирепствовать, Джиллис нашел ошибки в таблицах Гурвица, позже Такерман найдет ошибки в таблицах Джиллиса [338],. . .

• Только в 1971 году Брайант Такерман на IBM 360/91 нашел 24-е число Мерсенна [337]:

$M(24) = M_{19,937}$	6,002 цифр	04.03.1971

Такерман по образованию тополог, но за пять лет работы в IAS с Джоном фон Нейманом переучился на Computer Science и к моменту открытия $M(24)$ много лет работал в исследовательском отделе IBM. Параллельно с ним поисками $M(24)$ занимались Майкл Спесинер и Ричард Шреппель в MIT. Они придумали более быстрый алгоритм для умножения больших чисел (он описан во втором томе Кнута), но лучший алгоритм проиграл лучшему оборудованию: “don’t force it, take a larger hammer”. Следующие два десятилетия были соревнованием больших машин.

• В 1978 году Ландон Курт Нолл и Лора Никель на CDC Cyber 174 нашли 25-е число Мерсенна, а вскоре в феврале 1979 года Нолл нашел и 26-е, [244]:

$M(25) = M_{21,701}$	6,533 цифр	30.10.1978
$M(26) = M_{23,209}$	6,987 цифр	09.02.1979

Это событие попало во все газеты, так как Нолл[22] и Никель в то время были 18-летними школьниками. К моменту открытия $M(25)$ они три года работали над этим проектом и получили 350 часов машинного времени на Cyber 174 в кампусе Университета Калифорнии в Ист Бэй (Хейуорд)[23].

• В 1979 году Харри Нельсон и Дэвид Словинский на Cray 1 нашли 27-е число Мерсенна, [323], а через три с половиной года, все еще на Cray 1, Словинский нашел еще одно такое число:

$M(27) = M_{44,497}$	13,395 цифр	08.04.1979
$M(28) = M_{86,243}$	25,962 цифр	25.09.1982

Харри Нельсон был одним из ключевых разработчиков низкоуровневых операционных систем для суперкомпьютеров. При установке Cray-1 в Ливерморской Национальной

[22] Нолл продолжил заниматься факторизацией и дальше, на его странице http://www.isthe.com/chongo/index.html можно найти интересные ссылки, посвященные этому делу.

[23] Представьте себе, сколько стоил месяц работы такой машины в то время — у меня есть гипотезы о том, как школьники могли получить к ней доступ, но я стесняюсь их высказывать.

Лаборатории он привлек программиста Cray Research Inc. Дэвида Словинского для разработки рутин приемочного тестирования. В качестве субстрата для такой рутины Словинский выбрал поиск больших простых Мерсенна. При этом возникла масса технических моментов, типа быстрого умножения многозначных чисел, для этого был имплементирован алгоритм Шенхаге—Штрассена 1971 года и т.д. В дальнейшем эти рутины использовались при тестировании всех суперкомпьютеров Cray и сам Словинский, частично совместно с Полем Кейджем, открыл, кроме $M(27)$ и $M(28)$, еще *пять* новых простых Мерсенна, что является мировым рекордом. Основанные на этих идеях программы под другие платформы, написанные Ричардом Крэндаллом и Джорджем Вольтманом, привели к открытию *всех* остальных известных сегодня простых Мерсенна. Мир уже никогда не станет прежним.

• Следующее число сильно выпадает из хронологии, его открыли Уолтер Колквитт и Люк Уэлш только в 1988 году на суперкомпьютере NEC SX-2 в Исследовательском Центре Хьюстона, [82]:

$$M(29) = M_{110,503} \qquad 33,265 \text{ цифр} \qquad 28.01.1988$$

К этому моменту были уже известны гораздо большие числа $M(30)$, $M(31)$, открытые Словинским при тестировании новых моделей Cray.

• Дэвид Словинский на Cray X-MP и на Cray X-MP/24, соответственно:

$$M(30) = M_{132,049} \qquad 39,751 \text{ цифр} \qquad 19.09.1983$$
$$M(31) = M_{216,091} \qquad 65,050 \text{ цифр} \qquad 01.09.1985$$

Ну и, наконец, последний аккорд, одна машина, одно число, с периодичностью два года.

• Три последних простых Мерсенна найденных на больших машинах были открыты в 1992–1996 Дэвидом Словинским и Полем Кейджем на Cray-2, Cray C90, Cray T94:

$$M(32) = M_{756,839} \qquad 227,832 \text{ цифр} \qquad 19.02.1992$$
$$M(33) = M_{859,433} \qquad 258,716 \text{ цифр} \qquad 04.01.1994$$
$$M(34) = M_{1,257,787} \qquad 378,632 \text{ цифр} \qquad 03.09.1996$$

При открытии $M(32)$ использовался буквально Maple! Но в этот момент динозавров вытеснили млекопитающие.

3.2. Great Internet Mersenne Prime Search: 1996 onwards

В январе 1996 года Джордж Вольтман организовал проект распределенных вычислений GIMPS[24] = “Great Internet Mersenne Prime Search”, см. [364–366]. Душой этого проекта является написанная Вольтманом программа Prime95, тестирующая числа на простоту[25]. Кроме самых быстрых на сегодня алгоритмов умножения больших чисел и

[24] См. официальный сайт https://www.mersenne.org/, название проекта произносится “гимпс”.

[25] Я не знаю, имелось ли это в виду изначально, но Prime95 стало любимым средством для тестирования стабильности систем: “Prime95 has been a popular choice for stress/torture testing a CPU since its introduction, especially with overclockers and system builders. Since the software makes heavy use of the processor’s integer and floating point instructions, it feeds the processor a consistent and verifiable workload to test the stability of the CPU and the L1/L2/L3 processor cache. Additionally, it uses all of the cores of a multi-CPU/multi-core system to ensure a high-load stress test environment”.

собственно критерия Люка—Лемера, в ней имплементированы пробное деление, тесты псевдопростоты, алгоритм Ленстры, алгоритм Полларда и куча других вещей.

В проекте принимает участие примерно 250 тысяч человек и около 2.5 миллионов компьютеров, с используемой для целей проекта суммарной производительностью около 1.5 экзафлопсов[26], которые получают текущую версию программы Prime95 (в настоящее время версию `30.3`), необходимые инструкции и интервал простых экспонент p, в котором они ищут простые числа Мерсенна M_p, либо верифицируют предыдущие вычисления. Все последние новые простые Мерсенна начиная с ноября 1996 года в количестве 17 штук были открыты именно в рамках проекта GIMPS.

Вот резюме с их официального сайта `https://www.mersenne.org/primes/` с краткими комментариями.

$M(35) = M_{1,398,269}$	420,921	13.11.1996	Joel Armengaud	`90MHz Pentium`
$M(36) = M_{2,976,221}$	895,932	24.08.1997	Gordon Spence	`100MHz Pentium`
$M(37) = M_{3,021,377}$	909,526	27.01.1998	Roland Clarkson	`200MHz Pentium`
$M(38) = M_{6,972,593}$	2,098,960	01.06.1999	Nayan Hajratwala	`350MHz Pentium 2 IBM Aptiva`

Чтобы лучше понимать величину этих чисел, напомню, что на странице книжки стандартного формата около 2000 знаков. Это значит, что просто для десятичной записи числа $M(38)$ нужна книжка толщиной 1000 страниц. Тем не менее, мы можем проверить простоту этого числа и делать о нем другие осмысленные высказывания. При этом дальнейшие числа еще гораздо гораздо больше — ведь количество десятичных знаков растет как логарифм числа, а не как само это число.

После этого наступил Y2K и простое Мерсенна $M(39)$ стоит несколько особняком. Кстати, оно единственное из всех открыто на PC с процессором AMD.

$M(39) = M_{13,466,917}$	4,053,946	14.11.2001	Michael Cameron	`800MHz Athlon Thunderbird`

Следующие пять простых Мерсенна если рассматривать количество цифр как функцию от времени их открытия почти идеально ложатся на прямую:

$M(40) = M_{20,996,011}$	6,320,430	17.11.2003	Michael Shafer	`2GHz Dell Dimension`
$M(41) = M_{24,036,583}$	7,235,733	15.05.2004	Josh Findley	`2.4GHz Pentium 4`
$M(42) = M_{25,964,951}$	7,816,230	18.02.2005	Martin Nowak	`2.4GHz Pentium 4`
$M(43) = M_{30,402,457}$	9,152,052	15.12.2005	Curtis Cooper Steven Boone	`2GHz Pentium 4`
$M(44) = M_{32,582,657}$	9,808,358	04.09.2006	Curtis Cooper Steven Boone	`3GHz Pentium 4`

При этом простое Мерсенна $M(43)$ последнее, о котором мы с Володей Халиным знали во время работы над [6], следующее число $M(44)$ туда уже не попало. Между тем, это чрезвычайно интересное число. Купер и Бун стали первыми участниками

[26] Экзафлопс = квинтиллион = миллион миллионов миллионов операций с плавающей точкой в секунду.

GIMPS, которые открыли больше одного нового простого Мерсенна. Для вычислений они использовали кластер из примерно 850 компьютеров.

После этого произошла очередная историческая аномалия, простое Мерсенна $M(47)$ было обнаружено раньше, чем два предыдущих:

$M(45) = M_{37,156,667}$	11,185,272	06.09.2008	Hans-Michael Elvenich	2.83GHz Core2Duo
$M(46) = M_{42,643,801}$	12,837,064	04.06.2009	Odd M. Stridmo	3GHz Core2
$M(47) = M_{43,112,609}$	12,978,189	23.08.2008	Edson Smith	Dell OptiPlex 745

Последние четыре простых Мерсенна открыты в 2013–2018 годах, но их номера пока не подтверждены, так как не все меньшие числа Мерсенна проверены на простоту. Поэтому их номера могут измениться.

$M(48*) = M_{57,885,161}$	17,425,170	25.01.2013	Curtis Cooper	Intel Core2Duo E8400 @3.00GHz
$M(49*) = M_{74,207,281}$	22,338,618	07.01.2016	Curtis Cooper	Intel i7-4790 @3.60GHz
$M(50*) = M_{77,232,917}$	23,249,425	26.12.2017	Jon Pace	Intel i5-6600 @3.30GHz
$M(51*) = M_{82,589,933}$	24,862,048	07.12.2018	Patrick Laroche	Intel i5-4590T @2.0GHz

Забавно, что все это было сделано на самых демократичных бытовых компьютерах, иногда со слегка разогнанным процессором.

4. ФАКТОРИЗАЦИИ ЧИСЕЛ МЕРСЕННА

Обратимся теперь к разложению на простые множители тех чисел Мерсенна, которые не являются простыми. Для чисел такого размера установление того, что они не являются простыми, совершенно не означает возможности предъявить хотя бы один простой делитель. Более того, даже знание одного или нескольких простых делителей какого-то числа совершенно не означает возможность разложить это число на множители. Мне совершенно неясно, что могла бы означать основная теорема арифметики в чисто финитном мире. Легко представить себе ситуацию, когда мы можем записать само число и проверить, что оно не проходит какой-то тест простоты, но при у этого числа нет никаких простых делителей, так как их невозможно никаким образом выразить СРЕДСТВАМИ ИСПОЛЬЗУЕМОГО НАМИ ЯЗЫКА.

4.1. Факторизации чисел Мерсенна

История ранних факторизаций чисел Мерсенна очень детально изложена у Диксона [101] и Арчибальда [15], где можно найти ссылки на оригинальные работы.

В связи с тем упражнением, которое мы предлагаем проделать в следующем пункте, интересно, что еще в 1935 году — т.е. уже после основных работ Деррика Лемера на эту тему! — не было известно, являются ли числа M_{157}, M_{167}, M_{193}, M_{199}, M_{227}, M_{229}

простыми или составными. Про числа M_{101}, M_{103}, M_{109}, M_{137}, M_{139}, M_{149}, M_{241}, M_{257} было известно, что все они составные, но при этом для них не было известно ни одного простого делителя! Только в 1944–1947 годах Хорас Улер при помощи теста Люка—Лемера установил, что все остававшиеся до этого нерассмотренными числа составные, не предъявляя, впрочем, их разложения на множители.

Поэтому для выработки чувства исторической перспективы я коротко воспроизведу историю *факторизаций* чисел Мерсенна M_p, $p \le 257$, выполненных *вручную* до 1947 года. Эти результаты не были систематически проверены, исправлены и доведены до конца до середины 1960-х годов, уже на компьютере.

• Первое принципиальное продвижение принадежит де Ферма, который заметил сравнения для степеней (“малая теорема Ферма”) и руководствуясь этим нашел в 1640 году младшие простые делители чисел M_{23} и M_{37}, равные 47 и 223, соответственно.

• В дальнейшем к этой задаче многократно возвращался Эйлер. Так в 1732 году развивая идею Ферма он установил, что числа M_{29}, M_{43}, M_{73} составные и нашел их младшие простые делители, равные 233, 431 439, соответственно, для этого ему пришлось каждый раз произвести всего *два* деления!

• В том же году он проверил, что числа M_{83}, M_{131}, M_{179}, M_{191}, M_{239}, M_{251} тоже все составные и предъявил их младшие простые делители 167, 263, 359, 383, 479, 503.

• Потом он возвращался к этой задаче еще два раза с интервалом девять лет. Так, в 1741 году он нашел младший простой делитель M_{47}, равный 2351.

После 1750 года наступило затишье, и поиски факторизаций больших чисел Мерсенна возобновились только в 1856 году работами Ройшле и Плана и продолжались в таком духе еще 90+ лет. Укажем только авторов и даты открытия младших простых множители для чисел Мерсенна M_p, $p \le 247$.

• M_{79}, M_{113} и M_{233}, Карл Густав Ройшле, 1856.

• M_{41}, Джованни Антонио Амедео Плана, 1856.

• M_{53} и M_{59}, Фортюн Ландри, 1867 и 1878.

• $M_{97}, M_{151}, M_{211}, M_{223}$, А. Ле Лассер, 1883.

• M_{197}, Аллан Каннингем, 1895.

• M_{67}, Френк Нельсон Коул[27] [81], 1903 — к этому моменту из работ Люка 1876 и Фокемберга 1894 уже было известно, что M_{67} составное, но они не предъявили ни одного простого делителя.

• M_{163}, M_{71}, Аллан Каннингем, 1908 и 1909.

• M_{181}, Херберт Вудалл, 1911.

• M_{173}, Аллан Каннингем, 1912.

Как мы уже упоминали, в 1876 году Люка объявил, что число M_{67} является составным. В 1894 году Фокемберг объявил это снова, а потом еще раз два или три [115, 116]. После этого Пауэрс, Каннингем, Лемер, Улер, Баркер [19, 91–93, 208, 209, 211, 212, 215, 282, 283, 340–345, 362, 363] к 1947 постепенно доказали, что все остальные числа M_p, $p \le 257$, составные. Таким образом, даже решение узко понимаемой задачи Мерсенна без полного разложения этих чисел на множители заняло РОВНО ТРИСТА ЛЕТ.

[27] С этим разложением связан известный исторический анекдот про лекцию Коула на митинге Американского Математического Общества 31 октября 1903 года, во время которой он не произнес ни одного слова, а просто перемножил на доске 193707721 на 761838257287. Позже он упоминал, что для того, чтобы найти эти делители, ему потребовались "three years of Sundays."

Потом те же авторы, а также Бикмор, Андре Жерардан, Морис Борисович Крайчик, Поль Пуле [28, 29, 199, 200] и другие строили новые простые делители, исправляли ошибки в предыдущих текстах и т.д. В общем, все это превратилось в маленькую индустрию, которая занимала всех этих достойных людей несколько десятков лет[28]. Для разнообразия, в следующем пункте мы предлагаем повторить все эти вычисления за несколько минут.

В действительности, даже Робинсон в 1952 году перепроверил только простоту чисел Мерсенна, но не занимался их фактическим разложениям на множители. Такие вычисления были проведены только к началу 1960-х годов. Насколько я понимаю, *окончательный* ответ получен только к середине 1960-х годов. В работах Робинсона, Лемера, Бриллхарта, Джонсона, Карста, Кравица, Ризеля, Селфриджа, Эрмана, Уогстафа [48–53, 105, 190–193, 201, 305, 308, 317, 350] факторизации были продолжены до $p < 20000$. В то время это было совсем непростым делом. Так, первая факторизация числа M_{101} потребовала 10 часов машинного времени [50]. Но это, конечно, уже совершенно другая история, к которой я собираюсь вернуться в статье, посвященной факторизациям чисел специального вида. Ясно, что в дальнейшем проверка простоты чисел Мерсенна шла сплошняком — хотя и не всегда с первого прохода — а факторизации шли следом, но часто с довольно большим отставанием.

4.2. Критерий Ферма—Эйлера

Поиск простых делителей чисел M_p по сравнению с другими числами того же размера резко упрощается следующим **критерием Ферма—Эйлера**. Пусть p и q — нечетные простые. Тогда если $p|M_q$, то

$$p \equiv 1 \pmod{q}, \qquad p \equiv \pm 1 \pmod{8}.$$

Задача. Разложите на множители все остальные числа Мерсенна до M_{257}

Ответ. Поскольку все эти числа не слишком велики, можно обойтись внутренней функцией `FactorInteger`. Вот факторизации всех составных чисел Мерсенна до M_{67}. Кроме уже известного нам $M_{11} = 2047 = 23 \cdot 89$ факторизация остальных чисел вручную занятие не для слабых духом.

$$M_{23} = 8388607 = 47 \cdot 178481,$$
$$M_{29} = 536870911 = 233 \cdot 1103 \cdot 2089,$$
$$M_{37} = 137438953471 = 223 \cdot 616318177,$$
$$M_{41} = 2199023255551 = 13367 \cdot 164511353,$$
$$M_{43} = 8796093022207 = 431 \cdot 9719 \cdot 2099863,$$
$$M_{47} = 140737488355327 = 2351 \cdot 4513 \cdot 13264529,$$
$$M_{53} = 9007199254740991 = 6361 \cdot 69431 \cdot 20394401,$$
$$M_{59} = 576460752303423487 = 179951 \cdot 3203431780337,$$
$$M_{67} = 147573952589676412927 = 193707721 \cdot 761838257287.$$

Взглянув на факторизацию M_{67} сразу ясно, что сделать это докомпьютерную эпоху без какой-то серьезной математики было бы просто *невозможно*. Во времена Мерсенна даже

[28] Это даже не обсуждая вопрос, какие из исторических вычислений проверялись или повторялись, сколько там было ошибок и пр. — “And that leaves five — Well, six actually. But the idea is the important thing!”

хотя бы проверить простоту этих множителей уже было изрядным упражнением. Так что если Мерсенн и ошибся с простотой M_{67}, то совсем ненамного.

Вот еще порция факторизаций. Видно, что паттерны разные, но у всех чисел Мерсенна есть хотя бы один достаточно большой множитель.

$$M_{71} = 228479 \cdot 48544121 \cdot 212885833,$$
$$M_{73} = 439 \cdot 2298041 \cdot 9361973132609,$$
$$M_{79} = 2687 \cdot 202029703 \cdot 1113491139767,$$
$$M_{83} = 167 \cdot 57912614113275649087721,$$
$$M_{97} = 11447 \cdot 13842607235828485645766393,$$
$$M_{101} = 7432339208719 \cdot 341117531003194129,$$
$$M_{103} = 2550183799 \cdot 3976656429941438590393,$$
$$M_{109} = 745988807 \cdot 870035986098720987332873,$$
$$M_{113} = 3391 \cdot 23279 \cdot 65993 \cdot 1868569 \cdot 1066818132868207,$$

Вот еще одна чрезвычайно интересная серия. У числа M_{131} есть огромный простой множитель, но следующие три в каком-то смысле еще интереснее, у них нет маленьких простых множителей! Напомню, что это именно те числа, про которые было известно, что они составные, но для которых долго не удавалось предъявить ни одного простого делителя. В дальнейшем этот паттерн становится доминирующим, с чем и связана трудность факторизации чисел Мерсенна общегражданскими алгоритмами.

$$M_{131} = 263 \cdot 1035079443105516238671861923746823 4569,$$
$$M_{137} = 32032215596496435569 \cdot 5439042183600204290159,$$
$$M_{139} = 5625767248687 \cdot 1238761322052083357622784236 01,$$
$$M_{149} = 86656268566282183151 \cdot 8235109336669084672398 6161,$$
$$M_{151} = 18121 \cdot 55871 \cdot 165799 \cdot 2332951 \cdot 7289088383388253664437433,$$
$$M_{157} = 852133201 \cdot 60726444167 \cdot 1654058017289 \cdot 2134387368610417,$$
$$M_{163} = 150287 \cdot 704161 \cdot 110211473 \cdot 27669118297 \cdot 36230454570129675721,$$
$$M_{167} = 2349023 \cdot 79638304766856507377778616296087448490695649,$$
$$M_{173} = 730753 \cdot 1505447 \cdot 70084436712553223 \cdot 155285743288572277679887,$$

Ближе к концу списка Мерсенна прямая факторизация становится довольно затратным делом и я не буду воспроизводить ее результаты целиком. Так, в применении к числу $M_{257} = 2^{257} - 1$ исполнение команды `FactorInteger` занимает *ужасающие* 253.604 секунды[29]:

$$M_{257} = 535006138814359 \cdot 1155685395246619182673033 \cdot 37455059850181093658177663009631318139 3$$

Разумеется, трудность здесь состоит в том, что *все* простые множители большие, по общегражданским стандартам, в самом маленьком из них все равно 15 цифр. Можно только поразиться дерзновению Мерсенна, который заявлял, что это число *простое* — для него оно простым и было! Для человека, не владеющего теорией чисел

[29] `Mathematica 11.3` на `HP EliteBook 830GS` с процессором `Intel Core i7-8550U 1.99GHz`.

или не вооруженного компьютером, никаких шансов найти эти множители нет. Конечно, с нашей сегодняшней точки зрения это значит, что простые множители чисел специального вида нужно искать при помощи алгоритмов, созданных специально для факторизации чисел этого вида!

Задача. А теперь напишите программу поиска делителей M_p, использующую критерий Ферма—Эйлера, которая работает быстрее, чем `FactorInteger`.

Бросается в глаза наличие у некоторых M_p совсем маленьких простых делителей, скажем $23|M_{11}$, $47|M_{23}$, $167|M_{83}$ и $263|M_{131}$. Оказывается, это не случайность. А именно, **критерий Эйлера—Лагранжа** утверждает, что если $p \equiv 3 \pmod 4$, то $q = 2p+1$ в том и только том случае является простым, когда $q|M_p$.

Задача. Найдите все $p < 1000$ такие, что $q = 2p+1$ делит M_p.

Напомним, что в связи с теоремой Ферма Софи Жермен ввела следующий класс простых. Число p называется **простым Жермен**, если p и $2p+1$ оба просты. Таким образом, критерий Эйлера—Лагранжа утверждает, что числа Мерсенна, показатели которых являются простыми Жермен дающими остаток 3 при делении на 4, не являются простыми.

4.3. Prime records

Только в 1951 году рекорд Люка был побит[30]. и удалось найти простое число большее, чем M_{127}. Причем это не было число Мерсенна! А именно, пользуясь *арифмометром* Эме Феррье нашел простое число

$$(2^{148}+1)/17 = 209889366574405864861512642566102225938639 21,$$

у которого 44 цифры и которое не является числом Мерсенна.

Кстати, делить на 17 Феррье учился довольно упорно. До этого он посвятил этому делу целую книгу [117] и в результате в 1949 году нашел

$$(2^{92}+1)/17 = 291280009243618888211558641,$$

Таким образом, Феррье побил и еще один рекорд, который продержался еще дольше, а именно рекорд простого числа, *не являющегося числом Мерсенна*. Предыдущее такое число было найдено Фортюном Ландри в 1867 году:

$$M_{59}/179951 = 3203431780337.$$

см. `https://primes.utm.edu/notes/FirstIn1951.html`,

Как правило, самые большие известные простые числа являются числами Мерсенна. Как правило, но не всегда. Это могут быть старшие делители чисел Мерсенна или Ферма или какие-то другие числа подобного специального вида, сравнимые с ± 1 по модулю большой степени 2.

Так 6 августа 1989 года группа товарищей, известная как `Amdahl 6`, состоявшая из Джона Брауна, Ландона Курта Нолла, Бодо Паради, Джина Смита, Джоэля Смита и Серджио Дзарантонелло доказала простоту следующего числа

$$391581 \cdot 2^{216193} - 1, \qquad 65087 \text{ цифр.}$$

[30] Впрочем, некоторые считают, что первое *безукоризненное* доказательство простоты M_{127} было дано только в 1894 году Фокембергом, но даже и в этом случае рекорд простоял 57 лет! Я не высказываю никаких суждений по этому поводу, но у многих авторов еще большие сомнения относительно вычислений самого Фокемберга, см., например, [167].

На момент открытия это было самое большое известное простое число.

Из 10 самых больших известных сегодня простых чисел девять являются простыми Мерсенна. Единственное число другого вида, 9-е по рангу, это открытый в 2016 году старший делитель равный

$$10223 \cdot 2^{31172165} + 1, \qquad 9383761 \text{ цифр.}$$

Остальные соревнования проходят в совершенно другой весовой категории. Например, в самой большой известной сегодня паре близнецов

$$p = 2996863034895 \cdot 2^{1290000} - 1, \qquad p + 2 = 2996863034895 \cdot 2^{1290000} + 1$$

всего по 388342 цифры и среди всех простых эти числа находятся ближе к середине *десятой тысячи*.

Если еще 3–4 десятилетия назад эти рекорды можно было публиковать в статьях [247, 248, 369–371], то сегодня в них миллионы цифр и учет им ведется только на специализированных сайтах.

4.4. Гипотезы о числах Мерсенна

Вне всякого сомнения мы знаем, что ответ на три следующих вопроса утвердительный[31]. Мы только совершенно не знаем, как это доказывать. В классификации Дьедонне [102] эти проблемы фигурируют как **неприступные**.

Проблема. Бесконечно ли количество простых Мерсенна M_p?

Проблема. Бесконечно ли количество составных чисел Мерсенна M_p?

По отношению к двоичной системе числа Мерсенна являются в точности **репъюнитами** (= repeated unit), т.е. числами, все цифры которых равны 1. В самом деле,

$$2^p - 1 = 2^{p-1} + 2^{p-2} + \ldots + 2 + 1,$$

так что числа Мерсенна имеют вид $11, 111, 11111, 1111111, \ldots$ Репъюнитам в различных базах посвящена довольно значительная литература, см. [10].

Репъюниты являются частным случаем **палиндромических чисел**, которые читаются одинаково из начала в конец и из конца в начало. Другим известным примером палиндромов являются **числа Ферма** $11, 101, 10001, 100000001, \ldots$

Чтобы проиллюстрировать, насколько сложна проблема о бесконечности количества простых чисел Мерсенна, отметим, что не решена даже следующая гораздо более простая классическая задача, которую мы не будем здесь даже обсуждать, как и различные более общие гипотезы Шинцеля и Серпиньского, см. [140].

Проблема. Бесконечно ли количество простых палиндромов в двоичной системе?

Вот еще одна классическая задача.

Проблема. Верно ли, что все числа Мерсенна M_p бесквадратные?

Если не требовать здесь простоты p, то это, очевидно, неверно. В самом деле, уже $M_6 = 2^6 - 1 = 63 = 3^2 \cdot 7$. Можно было бы думать, что это связано с тем, что показатель четен, но и это не так:

$$M_{21} = 2^{21} - 1 = 2097151 = 7^2 \cdot 127 \cdot 337.$$

[31] Единственный известный мне источник, где всерьез высказывается мнение, что число простых Мерсенна конечно, это статья Василия Антоновича Голубева [131].

С другой стороны, если $q^2|M_p$, для некоторых *простых* p и q, то q должно быть **простым Вифериха**, т.е. q^2 должно делить $2^{q-1}-1$. Такие числа впервые рассмотрел Артур Виферих в 1909 году в связи с теоремой Ферма. Более чем за век удалось найти всего два таких числа, а именно 1093 и 3511, но ни одно из них не может быть делителем чисел Мерсенна, см. [322, 355].

Относительно следующей гипотезы я бы уже не был так уверен. Одно из истолкований исходной гипотезы Мерсенна состоит в том, что он делал предсказание, для каких показателей числа Мерсенна просты. То, что post factum эта гипотеза оказалась неверна, ближе к концу списка, не делает ее менее великой, *для того времени*. Бейтман, Селфридж и Уогстафф [20] предложили следующее исправление первоначальной гипотезы Мерсенна. Однако сегодня мы можем подозревать, что и здесь дело идет просто о ранних совпадениях, [137–139]. По поводу простоты чисел вида $(2^p+1)/3$ см. [319].

Новая гипотеза Мерсенна. Пусть p — нечетное натуральное число. Тогда если выполняются два из следующих условий, то выполняется и третье:

- $p = 2^k \pm 1$ или $p = 4^k \pm 3$,
- $M_p = 2^p - 1$ простое,
- $(2^p+1)/3$ простое.

Текст Мерсенна 1647 года я первоначально прочел именно как ГИПОТЕЗУ О БЕСКОНЕЧНОСТИ КОЛИЧЕСТВА ПРОСТЫХ ЧИСЕЛ МЕРСЕННА, точнее, как явную конструкцию *бесконечной серии* простых Мерсенна. Совсем явно это было сформулировано Эженом Каталаном уже в конце XIX века.

Определим **двойное число Мерсенна** как число Мерсенна, показатель которого сам является числом Мерсенна для какого-то простого p,

$$M_{M_p} = 2^{2^p-1} - 1.$$

Определим теперь **числа Каталана—Мерсенна** рекурсивно как двойные числа Мерсенна, начинающиеся с 3: $p_1 = 3$, $p_{n+1} = M_{p_n}$, см. . Как мы знаем, первые четыре числа Каталана—Мерсенна

$$p_1 = 2^2 - 1 = 3, \quad p_2 = 2^{2^2-1} - 1 = 7, \quad p_3 = 2^{2^{2^2-1}-1} - 1 = 127, \quad p_4 = 2^{2^{2^{2^2-1}-1}-1} - 1 = M_{127},$$

простые. Узнав о доказательстве Люка простоты M_{127} Эжен Каталан тут же в 1876 году прямо на полях работы Люка высказал следующую гипотезу[32].

Гипотеза Каталана—Мерсенна. Все числа Каталана—Мерсенна p_n просты.

Однако уже число $p_5 = M_{M_{127}}$ настолько велико, что если оно не является простым, то мы имеем шансы никогда этого не узнать. Однако еще смешнее было бы, если бы оно внезапно оказалось простым, потому что еще за пару итераций мы окажемся в области чисел, для которых у нас может вообще не быть возможности каким-либо образом выразить их простые делители.

[32] На самом деле, это позднейшая реинтерпретация. Сам Каталан гораздо осторожнее: “Si l’on admet ces deux propositions, et si l’on observe que 2^2-1, 2^3-1, 2^7-1 sont aussi des nombres premiers, on a ce théorème empirique: Jusqu’à une certaine limite, si 2^n-1 est un nombre premier p, 2^p-1 est un nombre premier p', $2^{p'}-1$ est un nombre premier p", etc. Cette proposition a quelque analogie avec le théorème suivant, énoncé par Fermat, et dont Euler a montré l’inexactitude: Si n est une puissance de 2, 2^n+1 est un nombre premier.” Сравнивая эту гипотезу с гипотезой Ферма о простоте чисел Ферма он прямо намекает, что она может быть неверна уже на следующем шаге, см. [114, 132].

Перейдем теперь к асимптотическим результатам. Морально результаты работ Эрдеша, Кисса, Померанса, Ленстры, Энгберга, Поллака, Ригера и других [106, 108, 111, 238, 240, 270, 291] о делителях чисел Мерсенна означают, что:

• простых Мерсенна очень мало,

• простые делители у больших составных чисел Мерсенна как правило тоже очень большие.

Это объясняет, почему простые Мерсенна так трудно искать и почему их еще труднее раскладывать на множители. На основе этих результатов, а также эвристических и статистических соображений, Ленстра, Померанс и Уогстафф высказали следующую количественную гипотезу.

Гипотеза Ленстры—Померанса—Уогстаффа. Асимптотически количество чисел Мерсенна меньших, чем x равно

$$e^{\gamma} \cdot \log_2 \log_2(x),$$

где γ — константа Эйлера—Маскерони.

Иными словами, утверждается, что количество простых чисел Мерсенна *бесконечно*, но встречаются они *крайне редко* — количество чисел Мерсенна с экспонентой p меньшей y асимптотически равно $e^{\gamma} \cdot \log_2(y)$. Впрочем, некоторые специалисты считают, что в действительности простых Мерсенна гораздо больше.

Самая правдоподобная гипотеза о числах Мерсенна была сформулирована в 1978 году Дэвидом Словинским [323].

Гипотеза Словинского. В любой момент будет больше открытых гипотез о числах Мерсенна, чем известных простых Мерсенна.

5. СУММЫ ДЕЛИТЕЛЕЙ

На этой оптимистической ноте перейдем теперь ко второй основной теме, суммам делителей.

Пусть каноническое разложение числа n имеет вид $n = p_1^{k_1} \dots p_s^{k_s}$. Тогда **количество делителей** n равно

$$d(n) = (k_1 + 1) \dots (k_s + 1),$$

а **сумма делителей** n задается формулой

$$\sigma(n) = \sum_{i \le k_1, \dots, i_s \le k_s} p_1^{i_1} \dots p_s^{i_s} = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \dots \frac{p_s^{k_s+1} - 1}{p_s - 1}$$

(сумма геометрической прогрессии).

Задача. Задайте функции $d(n)$ и $\sigma(n)$ на основе внутренней функции `FactorInteger` и сравните скорость их работы с `Length[Divisors[n]]` и `DivisorSigma[1,n]`.

Из формулы для $d(n)$ вытекает, что

• $d(n)$ зависит не от самого n, а от его арифметической структуры, иными словами, от того, с какими степенями в n входят различные простые;

• значение $d(n)$ может быть абсолютно любым.

Задача. Для любого простого числа q найдите наименьшее число, имеющее ровно q делителей.

Ответ. Небольшой компьютерный эксперимент убедит Вас в том, что это 2^{q-1}. Вообще, любое примарное число p^{m-1} имеет ровно m делителей, но в случае, когда m раскладывается на множители, как правило, удается построить много меньшее, чем 2^{m-1} число с тем же количеством делителей.

Задача. Составьте таблицу, в которой для каждого числа $m \le 100$ указано наименьшее число, имеющее ровно m делителей.

Задача. Вот начало этой таблицы:

1	2	3	4	5	6	7	8	9	10
1	2	4	6	16	12	64	24	36	48

Задача. Задайте функцию, сопоставляющую каждому натуральному m наименьшее натуральное n имеющее ровно m делителей.

Задача. Убедитесь, что для любого натурального числа $n > 1$ найдется такое m, что $d^m(n) = 2$. Сколь велико может быть это m?

Ответ. Поэкспериментировав с функцией d, легко убедиться, что для любого $n > 2$ имеем $d(n) < n$, поэтому применение d может оборваться только на значении 2. С другой стороны, мы только что заметили, что $d(2^{n-1}) = n$, поэтому если от n можно дойти до 2 за m шагов, то от 2^{n-1} требуется уже $m+1$ шаг.

Обратимся теперь к функции σ. Ясно, что σ возрастающая функция, $\sigma(n) > n$ для всех $n > 1$, причем $\sigma(n) = n+1$ только в случае, когда $n = p$ простое.

Задача. Убедитесь, что если n составное, то $\sigma(n) > n + \sqrt{n}$.

Задача. Любое ли m может быть значением функции σ?

Задача. Найдите все решения уравнения $\sigma(n) = \sigma(n+1)$ при $n \le 100000$.

Лео Мозер привел примеры, показывающие, что в отличие от арифметической функции $n \mapsto n\varphi(n)$, функция $n \mapsto n\sigma(n)$ не инъективна, иными словами, равенство

$$m\sigma(m) = n\sigma(n)$$

возможно и при $m \ne n$. А именно, при $m = 12$, $n = 14$ обе части здесь равны 336. Ясно, что умножая обе части этого равенства на любое число k взаимно простое с 2, 3 и 7, мы получим новую тройку чисел $m = 12k$, $n = 14k$ удовлетворяющую этому условию. Поэтому интересно искать примитивные пары, для которых $(m/k, n/k)$ не являются решениями этого уравнения ни при каком $k > 1$.

В действительности пример Мозера является первым из примеров следующего типа: $m = 2^{p-1}M_q$, $n = 2^{q-1}M_p$, где M_p и M_q различные простые числа Мерсенна.

Задача. Постройте еще несколько сотен примитивных решений уравнения $m\sigma(m) = n\sigma(n)$.

Задача. Задайте функцию, сопоставляющую паре (m, n) сумму их общих делителей.

Во многих задачах возникают различные варианты функции σ, например, функция сопоставляющая n сумму его *собственных* делителей, традиционно она обозначалась $\widehat{\sigma}$, но из типографских соображений мы будем обозначать ее s. Следующая функция σ^* естественно возникает в задаче о количестве представлений натурального числа как суммы четырех квадратов.

Задача. Задайте функцию σ^*, которая сопоставляет каждому натуральному числу сумму тех его делителей, которые не делятся на 4.

Задача. Пусть $p_1, \dots, p_s$ суть все различные простые делители числа n, а

$$m = \frac{n}{p_1 \dots p_s}$$

Для нескольких десятков n вычислите сумму $\psi(n)$ делителей числа n, являющихся кратными числа m, и угадайте формулу для этой суммы в общем случае.

Ответ. Искомая формула лишь знаком отличается от формулы для функции Эйлера:

$$\psi(n) = n\left(1 + \frac{1}{p_1}\right)\dots\left(1 + \frac{1}{p_s}\right).$$

6. СОВЕРШЕННЫЕ ЧИСЛА

Совершенные числа, это неподвижные точки функции, сопоставляющей натуральному числу сумму его собственных делителей.

6.1. Четные совершенные числа

Числа Мерсенна играют абсолютно исключительную роль в одной из *старейших* нерешенных проблем математики, относящейся к *четным* совершенным числам. Число n называется **совершенным**, если оно равно сумме своих собственных делителей. Иными словами, $\sigma(n) = 2n$. В терминах функции $s(n) = \sigma(n) - n$ это условие записывается еще естественнее, $s(n) = n$.

Задача. Найдите совершенные числа $\le 10^7$.

Ответ. Можно просто полным перебором с использованием `DivisorSigma`. Вот они:

$$6 = 2\cdot 3 = 1+2+3,$$
$$28 = 2^2\cdot 7 = 1+2+4+7+14,$$
$$496 = 2^4\cdot 31 = 1+2+4+6+16+31+62+124+248,$$
$$8128 = 2^6\cdot 127 = 1+2+4+8+16+32+64+127+254+508+1016+2032+4064,$$
$$\begin{aligned}33550336 = 2^{12}\cdot 8191 = {} & 1+2+4+8+16+32+64+128+256+512+1024+2048+\\ & 4096+8191+16382+32764+65528+131056+262112+\\ & 524224+1048448+2096896+4193792+8387584+16775168.\end{aligned}$$

Три первых были известны уже в VI веке до Н.Э., а четвертое нашел Никомах из Герасы около 100 года Н.Э. В книге Блаженного Августина “De Civita Dei” содержится поразительное рассуждение, что число 6 совершенное не потому, что Б-г создал Мир за 6 дней, а наоборот, Б-г потому создал мир за 6 дней, что число 6 совершенное[33],[34].

[33]“Haec autem propter senarii numeri perfectionem eodem die sexiens repetito sex diebus perfecta narrantur, non quia Deo fuerit necessaria mora temporum, quasi qui non potuerit creare omnia simul, quae deinceps congruis motibus peragerent tempora; sed quia per senarium numerum est operum significata perfectio. Numerus quippe senarius primus completur suis partibus, id est sexta sui parte et tertia et dimidia, quae sunt unum et duo et tria, quae in summam ducta sex fiunt”, XI–XXX.

[34]Увидев эти числа в таком контексте любой специалист по исключительной нумерологии не может не вздрогнуть. Ведь на самом деле $56 = 2\cdot 28$ — это размерность наименьшего представления E_7, а $248 = 496/2$ — это размерность наименьшего представления E_8.

Уже в “Элементах” Эвклида содержалось наблюдение (Книга IX, теорема 36), что если $2^p - 1$ простое, то $2^{p-1}(2^p - 1)$ совершенное. Эйлер показал, что *все* четные совершенные числа имеют такой вид. Точнее, имеет место следующая **теорема Эвклида—Эйлера**: множество четных совершенных чисел совпадает с множеством чисел вида $2^{p-1}M_p$, где M_p — простое число Мерсенна.

Задача. А теперь найдите еще 46 совершенных чисел.

Теорема Эвклида—Эйлера сводит вопрос о бесконечности множества четных совершенных чисел к вопросу о бесконечности множества простых чисел Мерсенна. Таким образом теперь мы можем переформулировать вопрос Мерсенна так, как он был исходно сформулирован более, чем за два тысячелетия до него.

Проблема. Бесконечно ли количество четных совершенных чисел?

6.2. Нечетные совершенные числа

До сих пор неизвестен и ответ на следующую задачу. Вероятно, эта задача была известна еще древним, но в любом случае она была явно сформулирована Жаком Лефевром не позднее 1496 года. Эти две задачи, видимо, являются, вместе с проблемой о бесконечности количества дружественных пар, *самыми* старыми нерешенными проблемами в математике,

Проблема. Существуют ли *нечетные* совершенные числа.

Не пытайтесь искать нечетные совершенные числа вручную. Еще Бенджамин Пёрс[35] доказал, что у нечетного совершенного числа не меньше 4 различных простых делителей. В 1888 году Джеймс Джозеф Сильвестр[36] вначале повторил этот результат, а потом [334] улучшил его до 5. В 1925 году Израиль Соломонович Градштейн[37] [11] довел количество различных делителей до 6, в 1974 году Карл Померанс [266] до 7, в 1980 году Питер Хагис [151] до 8, и в 2007 году Пэйс Нильсен [241] до 9, см. по этому поводу [129].

Кроме того, известно много других условий и ограничений на нечетные совершенные числа, которые шаг за шагом усиливались на протяжении многих десятилетий. Я не буду приводить по ним такого же типа исторический обзор, а просто перечислю некоторые из работ, где получены такие ограничения: [27, 43–46, 59, 68, 84, 95, 98, 119, 135, 148, 150–153, 160, 162–164, 166, 168, 170, 172, 179, 183, 184, 194, 195, 197, 202, 227–229, 241, 255, 306, 324, 328, 335, 338, 357, 361, 367]. Сейчас я резюмирую, следуя обзору Хенрика те Риле [300], лучшие полученные там оценки, с учетом дальнейших усилений, предложенных в [62, 74, 82, 133, 175–177, 243, 245, 246, 367, 374]:

- Нечетное совершенное число $> 10^{1500}$,
- Оно имеет по крайней мере 10 различных простых делителей[38],
- Количество его простых сомножителей с учетом кратности ≥ 101,
- Его старший простой делитель $> 10^8$,
- Его второй по старшинству простой делитель $> 10^4$,
- Его третий по старшинству простой делитель $> 10^2$,

[35] Во избежание недоразумений, Benjamin Peirce, 1809–1880, отец Чарльза Пёрса, 1839–1914. По-русски обычно беззастенчиво пишут “Пирс”, так, как будто исходно было “Pierce”.

[36] Тот самый Сильвестр! В преклонном возрасте он внезапно начал экспериментировать с классическими неприступными проблемами теории чисел, в том числе проблемой Гольдбаха.

[37] Тот самый Градштейн, больше известный советским математикам как Градштейн—Рыжик.

[38] Больше при некоторых дополнительных предположениях.

- Его старший примарный сомножитель $> 10^{62}$.

В упомянутых выше работах есть и *много* других ограничений: оценки на простые делители сверху, сравнения, условия на кратности различных простых делителей и т.д. Очевидно, что с учетом всех этих ограничений найти нечетное совершенное число в этом мире нет *никаких* шансов, а на бытовом компьютере тем более!

6.3. Некоторые обобщения совершенности

Число n называется **k-кратно совершенным**[39], если $\sigma(n) = kn$. Обычные совершенные числа получаются при $k = 2$. Кратно совершенные числа с $k \geq 3$ называются **полисовершенными**.

Задача. Если у числа n не более трех различных простых делителей, *как правило* из того, что n делит $\sigma(n)$ вытекает, что n совершенно. Найдите исключения.

Ответ. Имеются два таких числа, а именно 120 и 672, для которых $\sigma(n) = 3n$.

Для совершенного числа n выполняется равенство $\sigma(n) = 2n$. Число n называется **сверхсовершенным**, если $\sigma(\sigma(n)) = 2n$.

Задача. Найдите сверхсовершенные числа меньшие одного миллиона и сформулируйте гипотезу о том, как выглядят все сверхсовершенные числа.

Ответ. Таких чисел семь:

$$2 = 2^{2-1}, \quad 4 = 2^{3-1}, \quad 16 = 2^{5-1}, \quad 64 = 2^{7-1}, \quad 4096 = 2^{13-1}, \quad 65536 = 2^{17-1}, \quad 262144 = 2^{19-1}.$$

Все они являются степенями двойки, а список показателей уже встречался нам в связи с числами Мерсенна. Как заметил Сурьянарая [331], эта гипотеза верна: любое четное сверхсовершенное число имеет вид 2^{p-1}, для некоторого *простого* числа Мерсенна M_p.

Число n называется **избыточным**, если $s(n) > n$, и **недостаточным**, если $s(n) < n$.

Задача. Каких чисел среди чисел $< 10^6$ больше, избыточных или недостаточных?

Число n называется **полусовершенным**, если оно является суммой *каких-то* — не обязательно всех! — своих собственных делителей. Число называется **причудливым**, если оно избыточно, но не полусовершенно.

Задача. Найдите все причудливые числа, меньшие 500.

Ответ. Такое число ровно одно, а именно, 70.

[39] Про кратно совершенные числа я впервые услышал от Николая Григорьевича Чудакова году в 1968. Тогда в ЛОМИ, да и на мат-мех потоком шли письма любителей математики с новыми великими открытиями. Написаны они были от руки на клетчатых листочках бумаги, вырванных из школьных тетрадок. Процентов на 90 это были доказательства теоремы Ферма с одной и той же стандартной ошибкой. Но встречались и более занимательные вещи, опровержение канторовского диагонального процесса, доказательство четной гипотезы Гольдбаха, основанное на равенстве $2 + 3 = 5$, доказательство формулы $(-1) \cdot (-1) = -1$ и т.д. Теперь, конечно, весь подобный делириум сразу выплескивается в социальные сети, минуя отдел науки Василеостровского райкома КПСС (собственно, социальные сети и играют теперь такую же роль). Так вот, Чудаков упомянул про письмо, автор которого нашел общее решение уравнения $\sigma(n) = kn$, для любого k, и уверял, что это знание гарантирует бессмертие в буквальном физическом смысле — “Some pirates achieved immortality by great deeds of cruelty or derring-do ... But the captain had long ago decided that he would, on the whole, prefer to achieve immortality by not dying.” Николай Григорьевич улыбнулся и добавил: “Неудивительно, ведь уже тот, кто найдет все решения уравнения $\sigma(n) = 2n$, станет бессмертным”. Гораздо больше про роль Николая Григорьевича в возникновении этой статьи, а также про то, как избежать Танатоса и черную Керу, рассказано в [5].

Вот еще несколько подобных условий, которые ФАКТИЧЕСКИ РАССМАТРИВАЛИСЬ и которые могут послужить субстратом для такого же рода задач.

• Число n называется **квазисовершенным**, если оно совпадает с суммой своих *нетривиальных* делителей — всех, кроме 1 и n, т.е. $n = s(n) - 1$. Никаких квазисовершенных чисел пока не обнаружено, но они интенсивно изучались, и удовлетворяют большому количеству ограничений, в частности, $n > 10^{35}$.

• Число n называется **просто совершенным**, если у n и $s(n)$ одинаковые множества различных простых делителей. Ясно, что любое совершенное число просто совершенно, но есть и другие примеры, скажем, 120, 270 и 672.

• Делитель d числа n называется **унитарным**, если d и n/d взаимно просты. Число равное сумме своих собственных *унитарных* делителей называется **унитарно совершенным**

• Делитель d числа n называется **би-унитарным**, если наибольший общий *унитарный* делитель d и n/d равен 1. Число равное сумме своих собственных *би-унитарных* делителей называется **би-унитарно совершенным**.

Задача. Докажите, что единственными би-унитарно совершенными числами являются 6, 60 и 90.

В общем, you've got the idea! Фантазия числовиков-затейников столь же неисчерпаема, как электрон. Попрактиковавшись на [13, 16, 55, 58–61, 66, 67, 70, 71, 75, 76, 82, 90, 94, 120, 121, 154–158, 165, 173, 180, 187, 219, 232, 255, 259, 261, 265, 267, 285, 293, 297, 311, 312, 315, 325, 329–332, 354, 372, 373] я теперь и сам могу придумать несколько сот такого рода задач за вечер.

7. ДРУЖЕСТВЕННЫЕ ЧИСЛА

В связи с совершенными числами невозможно не упомянуть и о другой пифагорейской задаче — задаче о дружественных числах.

7.1. Пары дружественных чисел

Числа m и n называются **дружественными**[40], если сумма собственных делителей числа m равна n, а сумма собственных делителей числа n равна m. Иными словами, одновременно выполняются равенства $s(m) = n$ и $s(n) = m$ или, что то же самое,

$$\sigma(m) = \sigma(n) = m + n.$$

Известный болтун и фантазер Ямвлих из Халкиса приписывает лично товарищу Пифагору с острова Самос открытие первой пары дружественных чисел[41]

$$220 = 2^2 \cdot 5 \cdot 11, \qquad 284 = 2^2 \cdot 71.$$

Впрочем, Леонард Диксон отмечает [101] что уже в относящейся к более ранней дате части Библии в знак примирения Иаков подарил Исаву, брату своему, *ровно* 220 овец и 220 коз[42], а Поль Таннери считал, что магические свойства пары 220, 284 были известны

[40] По-английски `amicable pair`. Термин `friendly pair` тоже существует, но означает нечто совершенно другое, равенство $\sigma(m)/m = \sigma(n)/n$.

[41] Эта точка зрения получила широкое распространение в литературе: "It might be argued that elementary number theory began with Pythagoras who noted two-and-a-half millennia ago that 220 and 284 form an amicable pair", [262].

[42] "Двести коз, двадцать козлов, двести овец, двадцать овнов", Книга Бытия, XXXII, 14.

уже в древнем Египте.

В IX веке сирийский математик абу-Хасан Сабит ибн-Корра ибн Марван аль-Харрани доказал следующий результат. **Теорема Сабита ибн-Корры**: если все три числа $p = 3\cdot 2^{n-1}-1$, $q = 3\cdot 2^n - 1$ и $r = 3^2 2^{2n-1}-1$ нечетные простые, то числа $2^n pq$ и $2^n r$ — дружественные[43] [2, 171], это так называемая **первая форма Эйлера**, [85].

Задача. Найдите три пары дружественных чисел.

Указание. Как всегда, когда речь идет о небольшом переборе вначале по-простому: `Select`, `PrimeQ` и поверх `Map`. Обратите внимание, что $n \geq 2$, иначе $p = 2$.

Ответ. Пифагорейская пара получается, если взять в теореме Сабита ибн-Корры $n = 2$. С помощью этой теоремы в XIII веке марокканский ученый, ибн аль-Банна, открыл следующую пару дружественных чисел,

$$17296 = 2^4\cdot 23\cdot 47, \qquad 18416 = 2^4\cdot 1151,$$

отвечающую случаю $n = 4$. Теорема Сабита ибн-Корры была независимо переоткрыта в 1636 году Пьером Ферма и в 1638 Рене Декартом. При этом Ферма переоткрыл пару, отвечающую случаю $n = 4$, а Декарт переоткрыл следующую пару,

$$9363584 = 2^7\cdot 191\cdot 383, \qquad 9437056 = 2^7\cdot 73727,$$

отвечающую случаю $n = 7$, обнаруженную в XVI веке иранским ученым Мухаммадом Бакиром Йазди. Сейчас мы можем найти все эти пары за доли секунды.

Задача. Найдите все дружественные числа $\leq 10^6$.

Ответ. В данном случае, конечно, лучше не выбирать их из списка, а организовать цикл, вычисляющий все получающиеся 40 пар за секунды:

220	284	1184	1210	2620	2924	5020	5564
6232	6368	10744	10856	12285	14595	17296	18416
63020	76084	66928	66992	67095	71145	69615	87633
79750	88730	100485	124155	122265	139815	122368	123152
141664	153176	142310	168730	171856	176336	176272	180848
185368	203432	196724	202444	280540	365084	308620	389924
319550	430402	356408	399592	437456	455344	469028	486178
503056	514736	522405	525915	600392	669688	609928	686072
624184	691256	635624	712216	643336	652664	667964	783556
726104	796696	802725	863835	879712	901424	898216	980984

Кроме того, имеется две пары дружественных чисел, *одно* из которых меньше миллиона:

947835 1125765 998104 1043096

В качестве исторического курьеза отметим, что вторую по величине пару 1184 и 1210 открыл только Никколо Паганини[44] в 1866 году [249] — четыре следующих построил еще Эйлер в 1747–1750 годах!

[43] Вот, что пишет по этому поводу Херман те Риле: “De meeste bekende bevriende getallenparen zijn gevonden met behulp van variaties van de Regel van Thabit ibn Kurrah”, [300].

[44] Другой Паганини, полный тезка.

Всего Эйлер обнаружил *пятьдесят девять* новых пар дружественных чисел [113], как четных, так и *нечетных*, из которых мы укажем лишь несколько самых маленьких: две *четные* пары

$$6232 = 2^3 \cdot 19 \cdot 41 \qquad 6368 = 2^5 \cdot 199 \qquad 10744 = 2^3 \cdot 17 \cdot 79 \qquad 10856 = 2^3 \cdot 23 \cdot 59$$

и две *нечетные* пары

$$69615 = 3^2 \cdot 7 \cdot 13 \cdot 5 \cdot 17 \qquad 87633 = 3^2 \cdot 7 \cdot 13 \cdot 107$$

$$11498355 = 3^4 \cdot 5 \cdot 11 \cdot 29 \cdot 89 \qquad 12024045 = 3^4 \cdot 5 \cdot 11 \cdot 2699.$$

Всего к 1946 году было известно 390 пар дружественных чисел, из которых 233 открыл Эдвард Эскотт [112][45]. После этого построение дружественных пар стало набирать обороты. К 1971–1972 годам было открыто уже 1108 таких пар, из которых 389 открыл Элвин Ли, и все их авторы известны *поименно*. Все они перечислены в обзоре Ли и Джозефа Мадачи [205–207], которые насчитывают таковых 27 человек[46],[47].

Однако в это время произошли два события — появились работы Вальтера Боро [2], и начали всерьез использовать компьютеры, и это породило *лавину* новых пар. За последние 50 лет было открыто примерно в миллион раз больше новых дружественных пар, чем за всю предшествующую историю. Огромную роль в этом сыграли работы Яна Педерсена, Хенрика те Риле и Мариано Гарсии, за которыми стоят уже миллионы новых пар[48].

Но в последние годы рекордсменами стали Роберт Гербич, который открыл больше 173 миллионов новых дружественных пар и Сергей Черных, который открыл их больше миллиарда, см. описание истории всего проекта и текущей ситуации на его сайте `https://sech.me/ap/`. В настоящее время запущен еще один проект распределенных вычислений Amicable pairs, см. `https://boinc.ru/tag/amicable-numbers/` и добровольцы открыли еще примерно 5 миллионов новых пар.

Тем не менее, вопрос о *бесконечности* множества таких пар открыт так же широко, как во время Пифагора.

Проблема. Бесконечно ли количество дружественных пар?

Обратите внимание, что все известные пары либо четные, либо нечетные. Следующий вопрос по-прежнему открыт.

Проблема. Существуют ли четно-нечетные дружественные пары?

[45] Впрочем, Ли утверждает, что у Эскотта были ошибки и фактически тот открыл всего 219 пар.

[46] Тут, правда, нужно аккуратно сверять, как они учитывают повторы, иранских и арабских авторов, и т.д. Но это, конечно, серьезная собственно историческая работа.

[47] Чтобы проиллюстрировать, какого рода бреднями наполнен интернет, процитирую широко обсуждавшуюся на шахматных сайтах байку о Федоре Ивановиче Дуз-Хотимирском: “. . . исписывал целые пачки бумаги цифрами, открывая «родственные числа», . . . А гении математические заседали в академиях, и одному из них, академику по фамилии Виноградов, дядя Федя послал обнаруженные им в бесконечности «родственные числа». Как я поняла, первые четырнадцать этих чисел нашел в свое время Декарт, а дядя Федя довел их количество до шестисот. Академик, разумеется, был человеком умным и опубликовал Дузово открытие под своим великим именем. Дуз жутко на него разозлился, но судиться и доказывать авторство не стал. Во-первых, потому, что наверняка проиграл бы. А во-вторых, потому, что не желал апеллировать к государству, коего в принципе не признавал.” [9]. Матерый человечище, шестьсот пар дружественных чисел от руки в школьной тетрадке, это шутка посильнее, чем “Микромегас” Гете.

[48] “Millionen stehen hinter mir”.

7.2. Некоторые обобщения дружественности

Леонард Диксон предложил следующее обобщение понятия дружественных чисел — совершенно другое обобщение, предложенное Каталаном, обсуждается в следующем параграфе. А именно, он говорит, что $n_1, \ldots, n_m$ образуют m-ку дружественных чисел, если

$$\sigma(n_1) = \ldots = \sigma(n_m) = n_1 + \ldots + n_m.$$

Существуют ли дружественные m-ки при $m \geq 3$?

Задача. Постройте четыре первых дружественных тройки.

Ответ. Вот самая маленькая[49] из них:

$$1980 = 2^2 \cdot 3^2 \cdot 5 \cdot 11, \qquad 2016 = 2^5 \cdot 3^2 \cdot 7, \qquad 2556 = 2^2 \cdot 3^2 \cdot 71,$$

с суммой 6552. Вот следующая

$$9180 = 2^2 \cdot 3^3 \cdot 5 \cdot 17, \qquad 9504 = 2^5 \cdot 3^3 \cdot 11, \qquad 11556 = 2^2 \cdot 3^3 \cdot 107,$$

с суммой 30240. Еще две совсем маленькие тройки с суммами 70680, 87360 без труда строятся за секунды.

Задача. Постройте две дружественных тройки с одинаковой суммой.

Ответ. Две таких тройки встречаются довольно рано. А именно тройка

$$37380 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 89, \quad 41412 = 2^2 \cdot 3 \cdot 7 \cdot 17 \cdot 29, \quad 42168 = 2^3 \cdot 3 \cdot 7 \cdot 251$$

и тройка

$$38940 = 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 59, \quad 40608 = 2^5 \cdot 3^3 \cdot 47, \quad 41412 = 2^2 \cdot 3 \cdot 7 \cdot 17 \cdot 29$$

обе имеют сумму 120960.

В заключение параграфа приведем неполную и достаточно случайную подборку статей про дружественные пары и различные их обобщения, которые мы использовали для составления задач в разные годы и где можно найти дальнейшие ссылки: [1, 21, 22, 33–37, 39, 41, 42, 47, 69, 73, 74, 85–87, 104, 107, 122–126, 130, 144–147, 149, 161, 181, 182, 185, 186, 198, 203, 204, 220, 226, 251, 252, 256, 257, 259, 268, 269, 271, 292, 295, 296, 298, 299, 301, 333, 353].

8. ОБЩИТЕЛЬНЫЕ ЧИСЛА И ГИПОТЕЗА КАТАЛАНА—ДИКСОНА

В действительности, как задача о совершенных числах, так и задача о дружественных числах являются частными случаями вопроса о траекториях функции $s : n \mapsto \sigma(n) - n$. Число n совершенно, если оно является неподвижной точкой этой функции, $s(n) = n$, и является одним из дружественных чисел, если $s^2(n) = n$. Естественно возникает вопрос, имеет ли эта функция более длинные циклы? Элементы таких циклов называются **общительными числами**. Иными словами, число m общительное, если существует такое $k \geq 1$, что $s^k(n) = n$.

- Начинающаяся с числа n последовательность

$$n,\ s(n),\ s^2(n),\ s^3(n), \ldots$$

[49] Мы не рассматриваем тройки с повторяющимися элементами.

называется **аликвотной последовательностью**.

• **Общительное число** n это такое число, для которого аликвотная последовательность возвращается в n, иными словами, является **аликвотным циклом**.

В пакете `NumberTheory‘NumberTheoryFunctions‘` реализованы функции `AliquotSequence` и `AliquotCycle`, возвращающие аликвотную последовательность и ее период, хотя, конечно, эти функции за несколько секунд можно напись от руки.

Задача. Существуют ли общительные числа, не являющиеся совершенными или дружественными?

Ответ. Существуют, хотя найти их непросто, так как дополнительным параметром здесь служит длина аликвотного цикла, а коротких циклов (кроме циклов длины 4) среди маленьких чисел весьма мало! Следующий примитивный код

```
Timing[Block[{i=1},While[
            Implies[Nest[divsum,i,5]==i,divsum[i]==i],i++];i]]
```

позволяет за секунду найти цикл длины 5:

$$12496,\ 14288,\ 15472,\ 14536,\ 14264.$$

Этот цикл нашел Пуле в 1918 году.

За пару минут прямым перебором можно обнаружить и цикл длины 4:

$$1264460,\ 1547860,\ 1727636,\ 1305184.$$

Известно много десятков циклов длины 4. Вот наименьшие элементы в остальных циклах до 10^7:

$$2115324,\quad 2784580,\quad 4938136,\quad 7169104,$$

Кроме того, имеется еще пять циклов в интервале от 10^7 до 10^8, начинающеися с

$$18048976,\quad 18656380,\quad 28158165,\quad 46722700,\quad 81128632,$$

и четыре цикла в интервале от 10^8 до 10^9, начинающиеся с

$$174277820,\quad 209524210,\quad 330003580,\quad 498215416.$$

Мы не будем приводить остальные известные 4-циклы.

Есть еще несколько коротких циклов, состоящих из совсем небольших чисел. Вот два 6-цикла:

$$21548919483,\ 23625285957,\ 24825443643,\ 26762383557,\ 25958284443,\ 23816997477,$$
$$90632826380,\ 101889891700,\ 127527369100,\ 159713440756,\ 129092518924,\ 106246338676;$$

два 8-цикла:

$$1095447416,\ 1259477224,\ 1156962296,\ 1330251784,$$
$$1221976136,\ 1127671864,\ 1245926216,\ 1213138984,$$
$$1276254780,\ 2299401444,\ 3071310364,\ 2303482780,$$
$$2629903076,\ 2209210588,\ 2223459332,\ 1697298124;$$

и, наконец, 9-цикл

805984760, 1268997640, 1803863720, 2308845400, 3059220620,
3367978564, 2525983930, 2301481286, 1611969514.

Самый длинный известный цикл это открытый Пуле цикл длины 28:

14316, 19116, 31704, 47616, 83328, 177792, 295488, 629072, 589786, 294896
358336, 418904, 366556, 274924, 275444, 243760, 376736, 381028, 285778
152990, 122410, 97946, 48976, 45946, 22976, 22744, 19916, 17716

В 1888 году Эжен Каталан [57] высказал предположение, что каждое аликвотная последовательность достигает либо 0, либо совершенного числа, на что Перро [253] тут же возразил, что это неверно для последовательности, начинающейся с 220. Гипотеза Каталана был исправлена Леонардом Диксоном в 1913 году. Диксон [99] истолковал ее как отсутствие у функции s бесконечных траекторий.

Гипотеза Каталана—Диксона. Каждая траектория функции s за конечное число шагов доходит либо до 1, либо до общительного числа.

Задача. Найдите число, которое само не является общительным, но начинающаяся с которого аликвотная последовательность доходит до общительного числа, не являющегося ни совершенным, ни дружественными.

Ответ. В качестве совсем простых примеров можно взять 9464, 12032 или 15476, сумма собственных делителей которых равна 12496, или же $s(16312) = 14288$, $s(29066) = 14536$. Легко строятся и более длинные траектории. Например, $s(18922) = 9464$.

Впрочем, многие считают, что эта гипотеза может быть неверна. Никто, насколько я знаю, не выражал сомнения в том, что все траектории начинающиеся в *нечетных* числах обрываются, либо зацикливаются.

Гипотеза Гая—Селфриджа. Почти все траектории функции s начинающиеся в *четных* числах бесконечны.

Самым убедительным *опровержением* гипотезы Каталана—Диксона было бы построение строго возрастающей траектории, т.е. нахождение такого n, что $s^k(n) > s^{k-1}(n)$ для всех k. Это вряд ли получится, но Хенрик Ленстра доказал следующий удивительный результат. Для любого k существует такое n, что $n < s(n) < \ldots < s^k(n)$. Доказательство этого факта конструктивно и приведено в работе Эрдеша [109].

Это значит, что как и для теоремы Гудстайна и других подобных результатов, никакое чисто финитное *доказательство* гипотезы Каталана—Диксона невозможно, мы должны научиться делать предсказания о поведении функции s не раскладывая значения $s^k(n)$ на множители — что сегодня представляет основную трудность при *экспериментальном* исследовании функции s.

Подобными экспериментами занималось много специалистов начиная с Лемера и Годвина, см., например, [30–32, 38, 62, 72, 78, 96, 118, 136, 141–143, 196, 221–223, 233–236, 250, 254, 263, 264, 272, 294]. Тем не менее, для многих даже относительно небольших n вопрос о поведении последовательности $s^k(n)$ открыт. Дело в том, что ее промежуточные члены могут достигать огромных значений, для которых разложение на множители становится совершенно небанальным делом, а никаких других способов вычислять $s^k(n)$ мы сегодня не знаем.

Так, еще Лемер обнаружил, что уже для $n = 138$ последовательность итераций s заканчивается только на 117-м шаге, $s^{117}(138) = 1$. В дальнейшем Гай и Гай [136] обнаружили, что для $n = 840$ такая последовательность заканчивается только на 747 шаге, достигая в промежутке значений порядка 10^{48}. Митчел Дикерман побил этот рекорд, проверив, что последовательность значений s, начинающаяся в $n = 1248$ заканчивается на 1075 шаге, достигая в промежутке значений порядка 10^{57}. Бенито и Варона [25] построили последовательность начинающуюся в 4170, которая сошлась к 1 после 869 итераций, достигнув на 289-м шаге значения порядка 10^{83} Это произошло в процессе проверки аликвотных последовательностей для чисел меньших 10000 с использованием `PARI-GP1` и `UBASIC` и потребовало работу примерно 20 компьютеров на протяжении двух лет, “during nights and weekends”.

Сегодня систематические исследования поведения аликвотных последовательностей проводятся в значительно больших интервалах значений n, но следить за ними можно только по специализированным сайтам, так как порождаемые компьютерным поиском объемы данных слишком велики для традиционной бумажной публикации. Среди таких сайтов можно упомянуть, например,

`https://www.unirioja.es/cu/jvarona/aliquot.html`

`http://www.aliquot.de/`

`https://www.rieselprime.de/Others/Aliquot000.htm`

9. OÙ SOMMES-NOUS?

Жан Дьедонне [102] разделял все математические задачи на:

• **неприступные** — вот такие, как задачи о бесконечности количества простых чисел Мерсенна или Ферма;

• **стерильные** — такие как проблема четырех красок — решение которых ничего не дало математике; и

• **плодотворные** — такие как задача о представлении числа суммами квадратов, решение которой привело к развитию нескольких фундаментальных математических теорий.

Мне представляется, однако, что эти характеристики относятся не к самим задачам, а к их решениям. Проблема четырех красок стерильна не потому, что она сама не относится к математике, а потому что ее *решение* не является продуктивным математическим решением. Но ведь, скажем, и доказательство гипотезы Римана методами комплексного анализа тоже было бы почти бесполезно для математики.

Теория чисел с компьютером, это то же самое, что теория чисел без компьютера, только с компьютером. Теорема Ленстры говорит, что существует натуральное число n, для которого последовательность $s^k(n)$ является строго возрастающей на протяжении $10 \uparrow\uparrow 3$ шагов, на протяжении $10 \uparrow\uparrow\uparrow 3$ шагов, на протяжении $10 \uparrow\uparrow\uparrow\uparrow 3$ шагов, и так далее.

По своему мироощущению и эстетике я совсем не интуиционист или конструктивист. Но тут мне тоже было бы интересно знать, *что означает* найти и просуммировать делители числа $n > 10 \uparrow\uparrow\uparrow\uparrow 3$? Меня пока не интересует вопрос, КАК ЭТО СДЕЛАТЬ? Для начала хотелось бы просто понять, ЧТО ЭТО ОЗНАЧАЕТ? Как там насчет “He also sometimes throws the dice where they cannot be seen”?

Тот факт, что все упомянутые здесь задачи о разложении целых чисел на множители и суммах их делителей продолжают казаться столь же неприступными, как и несколько

тысячелетий назад, означает лишь, что мы все еще не понимаем чего-то чрезвычайно важного.

Огромная благодарность Володе Халину, вместе с которым мы начинали все это дело лет 15–20 назад и Саше Юркову, который вдохнул в это новую жизнь. Отдельная благодарность Сергею Позднякову, который убедил меня написать этот цикл статей. Мне были очень полезны обсуждения с Галиной Ивановной Синкевич, повлиявшие на содержание последних параграфов. Я признателен Леше Степанову и Илье Шкредову, которые чрезвычайно внимательно прочли первый вариант этой статьи и предложили большое количество исправлений и уточнений.

References

1. *Артюхов М. М.* К проблемам теории дружественных чисел. Acta Arith. **27** (1975), 281–291.
2. *Боро В.* Дружественные числа, двухтысячелетняя история одной арифметической задачи. В книге “Живые числа”, М., Мир, 1985, с.11–41.
3. *Вавилов Н. А.* Компьютеры как новая реальность математики: I. Personal account. Компьютерные инструменты в Образовании, 2020, 1–20.
4. *Вавилов Н. А.* Компьютеры как новая реальность математики: II. Проблема Варинга. Компьютерные инструменты в Образовании, 2020, 1–47.
5. *Вавилов Н. А.* Компьютеры как новая реальность математики: IV. Проблема Гольдбаха, 2021, 1–43.
6. *Вавилов Н. А., Халин В. Г.* Задачи по курсу Математика и Компьютер. Вып. 1. Арифметика и теория чисел. ОЦЭиМ, СПб, 2005, 180с.
7. *Вавилов Н. А., Халин В. Г.* Дополнительные задачи по курсу Математика и Компьютер. ОЦЭиМ, СПб, 2007, 172с.
8. *Вавилов Н. А., Халин В. Г., Юрков А. В.* `Mathematica` для нематематика, 2020, 484с.
9. *Венгерова Э. В.* Мемуарески, Текст, 2016, 352с.
10. *Ейтс С.* Репьюниты и десятичные периоды. М. Мир, 1992, 256с.
11. *Градштейн И. С.* О нечетных совершенных числах, Матем. сб., **32** (1925), no. 3, 476–510.
12. *Эдвардс Г.* Последняя теорема Ферма: генетическое введение в алгебраическую теорию чисел, Мир, М., 1980, 484р.
13. *Abbott H. L., Aull C. E., Brown E., Suryanarayana D.* Quasiperfect numbers, Acta Arith. **22** (1973), 439–447.
14. *Alanen J., Ore O., Stemple J.* Systematic computations on amicable numbers, Math. Comput., **21** (1967), 242–245.
15. *Archibald R. C.* Mersenne’s numbers, Scripta Math., **3** (1935), 112–119.
16. *Artuhov M. M.* On the problem of h-fold perfect numbers. Acta. Arith. **23** (1972), 249–255.
17. *Bach E., Shallit J.* Algorithmic number theory. Vol. 1. Efficient algorithms. Foundations of Computing Series. MIT Press, Cambridge, MA, 1996. xvi+512
18. *Bang T.* Store primtal. Nordisk Mat. Tidskr. **2** (1954), 157–168, 191.
19. *Barker C. B.* Proof that the Mersenne number M_{167} is composite, Bull. Amer. Math. Soc. **51** (1945), 389.
20. *Bateman P. T., Selfridge J. L., Wagstaff S. S. Jr.* The new Mersenne conjecture. Amer. Math. Monthly **96** (1989), no. 2, 125–128.
21. *Battiato S., Borho, W.* Are there odd amicable numbers not divisible by three? Math. Comput., **50** (1988), 633–637.
22. *Battiato S., Borho, W.* Breeding amicable numbers in abundance II, Math. Comput. **70**, (2001), 1329–1333.
23. *Beck W. E., Najar R. M.* Reduced and augmented amicable pairs to 10^8, Fibonacci Quart. **31** (1993), 295–298.
24. *Beiler A. H.* Recreations in the theory of numbers — the queen of mathematics entertains. 2nd ed. New York: Dover Publications, Inc. (1966). xvi+349p.

25. *Benito M., Varona J. L.* Advances in aliquot sequences. Math. Comput. **68** (1999), no. 225, 389–393.
26. *Benito M., Creyaufmїler W., Varona J. L., Zimmermann P.* Aliquot sequence 3630 ends after reaching 100 digits. Experiment. Math. **11** (2002), no. 2, 201–206.
27. *Bernhard H. A.* On the least possible odd perfect number. Amer. Math. Monthly **56** (1949), 628–629.
28. *Bickmore C. E.* On the numerical factors of $a^n - 1$. Messenger of Math. (2) **25** (1895–1896), 1–44.
29. *Bickmore C. E.* On the numerical factors of $a^n - 1$. (Second notice). Messenger of Math. (2) **26** (1896–1897), 1–38.
30. *Blankenagel K., Borho W.* New amicable four-cycles II. Int. J. Math. Sci. Comput. **5** (2015), no. 1, 49–51.
31. *Blankenagel K., Borho W., vom Stein A.* New amicable four-cycles. Math. Comput. **72** (2003), no. 244, 2071–2076.
32. *Borho W.* Über die Fixpunkte der k-fach iterierten Teilersummenfunktion. Mitt. Math. Gesellsch. Hamburg **9** (1969), no. 5, 34–48.
33. *Borho W.* Bemerkung zu einer Arbeit von H.-J. Kanold. J. Reine Angew. Math. **243** (1970), 219–220.
34. *Borho W.* On Thabit ibn Kurrah's formula for amicable numbers. Math. Comput., **26** (1972), 571–578.
35. *Borho W.* Befreundete Zahlen mit gegebener Primteileranzahl, Math. Ann. **209** (1974), 183–193.
36. *Borho W.* Eine Schranke für befreundete Zahlen mit gegebener Teileranzahl, Math. Nachr. **63** (1974), 297–301.
37. *Borho W.* Some large primes and amicable numbers. Math. Comput. **36** (1981), no. 153, 303–304
38. *Borho W., Blankenagel K.* Befreundete Zyklen. Mitt. Math. Ges. Hamburg **35** (2015), 67–75.
39. *Borho W., Hoffmann H.* Breeding amicable numbers in abundance, Math. Comput. **46** (1986), 281–293
40. *Bosma W., Kane B.* The aliquot constant. Quart. J. Math. **63** (2012), no. 2, 309–323.
41. *Bratley P., Lunnon F., McKay J.* Amicable numbers and their distribution. Math. Comput., **24** (1970), 431–432.
42. *Bratley P., McKay J.* More amicable numbers. Math. Comput., **22** (1968), 677–678.
43. *Brauer A.* On the non-existence of odd perfect numbers of form $p^\alpha q_1^2 q_2^2 \cdots q_{t-1}^2 q_t^4$ Bull. Am. Math. Soc. **49** (1943), 712–718.
44. *Brauer A.* Note on the non-existence of odd perfect numbers of form $p^\alpha q_1^2 q_2^2 \cdots q_{t-1}^2 q_t^4$ Bull. Am. Math. Soc. **49** (1943), 937.
45. *Brent R. P., Cohen G. L.* A new lower bound for odd perfect numbers, Math. Comput. **53** (1989), 431–437, S7–S24.
46. *Brent R. P., Cohen G. L. te Riele H. J. J.* Improved techniques for lower bounds for odd perfect numbers. Math. Comput. 57 (1991), no. 196, 857–868.
47. *Brentjes S., Hogendijk J. P.* Notes on Thābit ibn Qurra and his rule for amicable numbers, Historia Math. **16** (1989), 373–378.
48. *Brillhart J.* Some miscellaneous factorizations, Math. Comput., **17** (1963), 447–450.
49. *Brillhart J.* On the factors of certain Mersenne numbers. II. Math. Comput. **18** (1964), 87–92.
50. *Brillhart J., Johnson G. D.* On the factors of certain Mersenne numbers, Math. Comput. **14** (1960), 365–369.
51. *Brillhart J., Lehmer D. H., Selfridge J. L.* New primality criteria and factorizations of $2^m \pm 1$, Math. Comput., v. 29, 1975, pp. 620-647.
52. *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.
53. *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.
54. *Bruce J. W.* A really trivial proof of the Lucas—Lehmer test. Amer. Math. Monthly **100** (1993), no. 4, 370–371.
55. *Carmichael R. D.* Note on multiply perfect numbers. Amer. Math. Soc. Bull. (2) **17** (1911), 518.
56. *Catalan E.* Propositions et questions diverses. Bull. Soc. Math. France **16** (1888), 128–129.
57. *Cataldi P. A.* Trattato dè numeri perfetti, Bologna, Giovanni Rossi, 1603, 41p., полный текст на `https://gutenberg.beic.it` по ссылке на `https://it.wikipedia.org/wiki/Pietro_Antonio_Cataldi`

58. *Cattaneo P.* Sui numeri quasiperfetti, Boll. Un. Mat. Ital. **6** (1951), 59–62.
59. *Chen Shi-Chao, Luo, Hao* Bounds for odd k-perfect numbers. Bull. Aust. Math. Soc. **84** (2011), no. 3, 475–480.
60. *Chen Shi-Chao, Luo, Hao* Odd multiperfect numbers. Bull. Aust. Math. Soc. **88** (2013), no. 1, 56–63.
61. *Chen Yong-Gao, Tang Cui-E* Improved upper bounds for odd multiperfect numbers. Bull. Aust. Math. Soc. **89** (2014), no. 3, 353–359.
62. *Chishiki Y., Goto T., Ohno Y.* On the largest prime divisor of an odd harmonic number. Math. Comput. **76** (2007), no. 259, 1577–1587.
63. *Chum K., Guy R. K., Jacobson M. J. Jr., Mosunov A. S.* Numerical and statistical analysis of aliquot sequences. Exp. Math. **29** (2020), no. 4, 414–425.
64. *Cohen G. L.* On odd perfect numbers. II. Multiperfect numbers and quasiperfect numbers, J. Austral. Math. Soc. Ser. A **29** (1980), 369–384.
65. *Cohen G. L.* Even perfect numbers, Math. Gaz. **65** (1981), 28–30.
66. *Cohen G. L.* The nonexistence of quasiperfect numbers of certain forms, Fibonacci Quart. **20** (1982), 81–84.
67. *Cohen G. L.* On primitive abundant numbers, J. Aust. Math. Soc. Ser. A **34** (1983) 123–137.
68. *Cohen G. L.* On the largest component of an odd perfect number, J. Aus. Math. Soc. A. **42** (1987) 280–286.
69. *Cohen G. L., Gretton S. F., Hagis P. Jr*. Multiamicable numbers. Math. Comput. **64** (1995), no. 212, 1743–1753.
70. *Cohen G. L., Hagis P. Jr* Results concerning odd multiperfect numbers. Bull. Malaysian Math. Soc. (2) **8** (1985), no. 1, 23–26.
71. *Cohen G. L., Hendy M. D.* On odd multiperfect numbers, Math. Chron. **10** (1981) 57–61.
72. *Cohen G. L., te Riele H. J. J.* Iterating the sum-of-divisors function. Experiment. Math. **5** (1996), no. 2, 91–100. errata: **6** (1997), no. 2, 177.
73. *Cohen G. L., te Riele H. J. J.* On ϕ-amicable pairs. Math. Comput. **67** (1998), no. 221, 399–411.
74. *Cohen G. L., Sorli R. M.* On the number of distinct prime factors of an odd perfect number. Combinatorial algorithms. J. Discrete Algorithms **1** (2003), no. 1, 21–35.
75. *Cohen G. L., Sorli R. M.* Odd harmonic numbers exceed 10^{24}. Math. Comput. **79** (2010), no. 272, 2451–2460.
76. *Cohen G. L., Sorli R. M.* On odd perfect numbers and even 3-perfect numbers. Integers **12** (2012), no. 6, 1213–1230.
77. *Cohen G. L., Williams R. J.* Extensions of some results concerning odd perfect numbers, Fibonacci Quarterly **23** (1985) 70–76.
78. *Cohen H.* On amicable and sociable numbers, Math. Comput., **24**, 1970, 423–429.
79. *Cohen H.* A course in computational algebraic number theory. Graduate Texts in Mathematics, **138**. Springer-Verlag, Berlin, 1993. xii+534 pp.
80. *Cohen P., Cordwell K., Epstein A., Kwan Chung-Hang, Lott A., Miller S. J.* On near-perfect numbers. Acta Arith. **194** (2020), no. 4, 341–366
81. *Cole F. N.* On the factoring of large numbers, Bull. Amer. Math. Soc., **10** (1903), 134–137,
82. *Colquitt W. N., Welsh L., Jr.* A new Mersenne prime. Math. Comput. **56** (1991), no. 194, 867–870.
83. *Conway J. H., Guy R. K.* The book of numbers. Copernicus, New York, 1996. x+310 pp.
84. *Cook R. J.* Bounds for odd perfect numbers, Number theory, Ottawa, ON, 1996; CRM Proc. Lecture Notes **19**, Amer. Math. Soc., Providence, RI, 1999, 67–71.
85. *Costello P.* Amicable pairs of Euler's first form. J. Rec. Math. **10** (1977–1978), 183–189.
86. *Costello P.* Amicable pairs of the form $(i, 1)$, Math. Comput. **56** (1991), 859–865.
87. *Costello P., Edmonds R. A. C.* Gaussian amicable pairs. Missouri J. Math. Sci. **30** (2018), no. 2, 107–116.
88. *Crandall R., Penk M. A.* A search for large twin prime pairs, Math. Comput., v. 33, 1979, pp. 383-388.
89. *Crandall R., Pommerance C.* Prime numbers. A computational perspective. 2nd edition. Springer, New York, 2005. xvi+597 pp.
90. *Cross J. T.* A note on almost perfect numbers, Math. Mag. **47** (1974), 230–231
91. *Cunningham A.* On Mersenne's numbers. Proc. London Math. Soc. (2) **2** (1911), 10.
92. *Cunningham A.* On Mersenne's numbers. Proc. 5. Intern. Math. Congr. 1, 384–386; Brit. Ass. Rep.

Dundee 82 (1913), 406–407.
93. *Cunningham A.* On Lucas's process applied to composite Mersenne's numbers. Lond. M. S. Proc. (2) **32** (1919), 17.
94. *Dai Li-Xia, Pan Hao, Tang Cui-E* Note on odd multiperfect numbers. Bull. Aust. Math. Soc. **87** (2013), no. 3, 448–451.
95. *Dandapat G. G., Hunsucker J. L., Pomerance C.* Some new results on odd perfect numbers, Pacific J. Math. **57** (1975), 359–364.
96. *Devitt J. S., Guy R. K., Selfridge J. L.* Third report on aliquot sequences. Proceedings of the Sixth Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1976), 177–204, Congress. Numer., XVIII, Utilitas Math., Winnipeg, Man., 1977.
97. *Devlin K.* Mathematics. The new golden age. 2nd edition. Columbia Univ. Press, New York, 1999. xii+320 pp.
98. *Dickson L. E.* Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors, Amer. J. Math. **35** (1913), 413–422.
99. *Dickson L. E.* Theorems and tables on the sum of the divisors of a number, Quart. J. Math., **44** (1913), 264–296.
100. *Dickson L. E.* Amicable number triples. Amer. Math. Monthly, **20** (1913), 84–91.
101. *Dickson L. E.* History of the theory of numbers, vol. I. Chelsea, 1952.
102. *Dieudonné J.* Pour l'honneur de l'esprit humain. Les mathématiques aujourd'hui. Histoire et Philosophie des Sciences. Librairie Hachette, Paris, 1987. 303 pp
103. *Drake S.* The rule behind 'Mersenne's numbers', Physis-Riv. Internaz. Storia Sci., **13** (1971), 421–424.
104. *Dubner H.* New amicable pair record. Oct. 14, 1997. `https://listserv.nodak.edu/scripts/wa.exe?A2=ind9710&L=NMBRTHRY&F=&S=&P=695.`
105. *Ehrman J. R.* The number of prime divisors of certain Mersenne numbers, Math. Comput., **21**, 1967, 700–704.
106. *Engberg Z., Pollack P.* The reciprocal sum of divisors of Mersenne numbers. Acta Arith. **197** (2021), no. 4, 421–440
107. *Erdős P.* On amicable numbers. Publ. Math. Debrecen **4** (1955–1956), 108–111.
108. *Erdős P.* On perfect and multiply perfect numbers, Ann. Mat. Pura Appl. (4) **42** (1956), 253–258.
109. *Erdős P.* On the sum $\sum_{d|2^n-1} d^{-1}$. Israel J. Math. **9** (1971), 43–48.
110. *Erdős P.* On asymptotic properties of aliquot sequences. Math. Comput. **30** (1976), 641–645.
111. *Erdős P., Kiss P., Pomerance C.* On prime divisors of Mersenne numbers, Acta Arith. **57** (1991), 267–281.
112. *Escott E. B.* Amicable numbers, Scripta Math., **12** (1946), 61–72.
113. *Euler L.* De numeris amicabilibus, Opuscula varii argumenti (1750), 23–107
114. *Eum Ick Sun* A congruence relation of the Catalan—Mersenne numbers. Indian J. Pure Appl. Math. **49** (2018), no. 3, 521–526.
115. *Fauquembergue E.* Nombres de Mersenne, Sphinx-Œdipe, **9** (1914) 103–105; **15** (1920) 17–18.
116. *Fauquembergue E.* Plus grand nombre premier connu (question 176, de G. de Rocquigny). Interméd. des math. **24** (1917), 33.
117. *Ferrier A.* Les Nombres Premiers. Principaux résultats obtenus depuis Euclide. Table donnant, jusqu'à 100.000, les nombres premiers et les nombres composés n'ayant pas de diviseur inférieur à 17, avec, pour chacun d'eux, son plus petit diviseur. Librairie Vuibert, Paris, 1947. vi+111 pp.
118. *Flammenkamp A.* New sociable numbers, Math. Comput. **56** (1991), 871–873.
119. *Fletcher S., Nielsen P. P., Ochem P.* Sieve methods for odd perfect numbers. Math. Comput. **81** (2012), no. 279, 1753–1776.
120. *Franqui B., García M.* Some new multiply perfect numbers. Amer. Math. Monthly **60** (1953), 459–462.
121. *Franqui B., García M.* 57 new multiply perfect numbers. Scripta Math. **20** (1954), 169–171.
122. *García M.* New amicable pairs, Scripta Math. **23** (1957), 167–171.
123. *García M.* New amicable pairs of Euler's first form with greatest common factor a prime times a power of 2. Nieuw Arch. Wisk. (4) **17** (1999), no. 1, 25–27.
124. *García M.* A million new amicable pairs. J. Integer Seq. **4** (2001), no. 2, Article 01.2.6, 1–3.
125. *García V.* The first known type $(7, 1)$ amicable pair. Math. Comput. **72** (2003), no. 242, 939–940.

126. *García M., Pedersen J. M., te Riele H. J. J.* Amicable pairs, a survey, 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, 179–196.
127. *Gardner M.* Perfect, Amicable, Sociable. Ch. 12 in Mathematical Magic Show: More Puzzles, Games, Diversions, Illusions and Other Mathematical Sleight-of-Mind from Scientific American. New York: Vintage, 160–171, 1978.
128. *Gillies D. B.* Three new Mersenne primes and a statistical theory, Mathematics of Comput., **18** (1964), no. 85, 93–97.
129. *Gimbel S., Jaroma J. H.* Sylvester: ushering in the modern era of research on odd perfect numbers. Integers 3 (2003), A16, 26 pp.
130. *Gioia A. A., Vaidya A. M.* Amicable numbers with opposite parity. Amer. Math. Monthly **74** (1967), 969–973.
131. *Golubev V. A.* Nombres de Mersenne et caractères du nombre 2. Mathesis **67** (1958), 257–262.
132. *Good I. J.* Conjectures concerning the Mersenne numbers. Math. Comput. **9** (1955), 120–121.
133. *Goto T., Ohno Y.* Odd perfect numbers have a prime factor exceeding 10^8. Math. Comput. 77 (2008), no. 263, 1859–1868.
134. *Granville A.* Number theory revealed: a masterclass. American Mathematical Society, Providence, RI, 2019. xxviii+587p.
135. *Grün O.* Über ungerade vollkommene Zahlen, Math. Zeit. **55** (1952), 353–354.
136. *Guy A. W. P., Guy R. K.* A record aliquot sequence. Mathematics of Computation 1943–1993: a half-century of computational mathematics (Vancouver, BC, 1993), 557–559, Proc. Sympos. Appl. Math., 48, Amer. Math. Soc., Providence, RI, 1994.
137. *Guy R. K.* The strong law of small numbers. Amer. Math. Monthly, **95** (1988), no. 8, 697–712.
138. *Guy R. K.* Graphs and the strong law of small numbers. Proc. 6 Intern. Conf Theory Appl. Graphs, Kalamazoo, MI, 1988.
139. *Guy R. K.* The second strong law of small numbers. Math. Magazine, **63** (1990), no. 1, 3–20.
140. *Guy R. K.* Unsolved problems in number theory. 3rd edition. Problem Books in Mathematics. Springer-Verlag, New York, 2004. xviii+437 pp.
141. *Guy R. K., Lehmer D. H., Selfridge J. L., Wunderlich, M. C.* Second report on aliquot sequences. Proceedings of the Third Manitoba Conference on Numerical Mathematics (Winnipeg, Man., 1973), pp. 357–368. Utilitas Math., Winnipeg, Man., 1974.
142. *Guy R. K., Selfridge J. L.* Interim report on aliquot series. Proceedings of the Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1971), pp. 557–580. Dept. Comput. Sci., Univ. Manitoba, Winnipeg, Man., 1971.
143. *Guy R. K., Selfridge J. L.* What drives an aliquot sequence? Math. Comput. **29** (1975), 101–107.
144. *Hagis P. Jr.* On relatively prime odd amicable numbers, Math. Comput. **23** (1969), 539–543.
145. *Hagis P. Jr.* Lower bounds for relatively prime amicable numbers of opposite parity, Math. Comput. **24** (1970), 963–968.
146. *Hagis P. Jr.* Unitary amicable numbers. Math. Comput. **25** (1971), 915–918.
147. *Hagis P. Jr.* Relatively prime amicable numbers with twenty-one prime divisors, Math. Mag. **45** (1972), 21–26.
148. *Hagis P. Jr.* A lower bound for the set of odd perfect numbers. Math. Comput., **35** (1973), 1027–1031.
149. *Hagis P. Jr.* On the number of prime factors of a pair of relatively prime amicable numbers, Math. Mag. **48** (1975), 263–266.
150. *Hagis P. Jr.* On the largest prime divisor of an odd perfect number. Math. Comput., **29** (1975), 922–924.
151. *Hagis P. Jr.* Outline of a proof that every odd perfect number has at least eight prime factors. — Math. Comput., **35** 1980, 1027–1031.
152. *Hagis P. Jr.* On the second largest prime divisor of an odd perfect number, in: Analytic Number Theory, in: Lecture Notes in Math, **899**, Springer-Verlag, Berlin, 1981, pp. 254–263.
153. *Hagis P. Jr.* Sketch of a proof that an odd perfect number relatively prime to 3 has at least eleven prime factors, Math. Comput. **40** (1983) 399–404.
154. *Hagis P. Jr.* Lower bounds for unitary multiperfect numbers. Fibonacci Quart. **22** (1984), no. 2, 140–

143.
155. *Hagis P. Jr.* The third largest prime factor of an odd multiperfect number exceeds 100. Bull. Malaysian Math. Soc. (2) **9** (1986), no. 2, 43–49.
156. *Hagis P. Jr.* A systematic search for unitary hyperperfect numbers. Fibonacci Quart. **25** (1987), no. 1, 6–10.
157. *Hagis P. Jr.* Odd nonunitary perfect numbers. Fibonacci Quart. **28** (1990), no. 1, 11–15.
158. *Hagis P. Jr.* A new proof that every odd triperfect number has at least twelve prime factors. A tribute to Emil Grosswald: number theory and related analysis, 445–450, Contemp. Math., 143, Amer. Math. Soc., Providence, RI, 1993.
159. *Hagis P. Jr., Cohen G. L.* Some results concerning quasiperfect numbers, J. Austral. Math. Soc. Ser. A **33** (1982), 275–286.
160. *Hagis P. Jr., Cohen G. L.* Every odd perfect number has a prime factor which exceeds 10^6. Math. Comput. **67** (1998), no. 223, 1323–1330.
161. *Hagis P. Jr., Lord G.* Quasi-amicable numbers. Math. Comput. **31** (1977), no. 138, 608–611.
162. *Hagis P. Jr., McDaniel W. L.* A new result concerning the structure of odd perfect numbers. Proc. Amer. Math. Soc. **32** (1972), 13–15.
163. *Hagis P. Jr., McDaniel W. L.* On the largest prime divisor of an odd perfect number. Math. Comput. **27** (1973), 955–957.
164. *Hagis P. Jr., McDaniel W. L.* On the largest prime divisor of an odd perfect number. II, Math. Comput. **29** (1975), 922–924.
165. *Harborth H.* Eine Bemerkung zu den vollkommenen Zahlen, Elem. Math. **31** (1976), 115–117.
166. *Hare K. G.* More on the total number of prime factors of an odd perfect number, Math. Comput. **74** (2005), 1003–1008.
167. *Haworth G.* Mersenne numbers. Reading 1990, 81p.
168. *Heath-Brown D. R.* Odd perfect numbers, Math. Proc. Cambridge Philos. Soc. **115** (1994), 191–196.
169. *Heyworth M. R.* A conjecture on Mersenne's conjecture, New Zealand Math. Mag., **19** (1982), 147–151.
170. *Heyworth M. R.* Continued fractions in a search for odd perfect numbers. N.Z. Math. Mag. **19** (1982), 63–69.
171. *Hogendijk J. P.* Thābit ibn Qurra and the pair of amicable numbers 17296; 18416, Historia Mathematica, **12** (1985), 269–273.
172. *Holdener J. A.* A theorem of Touchard and the form of odd perfect numbers. American Math. Monthly, **109** (2002), 661–663.
173. *Hornfeck B., Wirsing E.* Über die Häufigkeit vollkommener Zahlen. Math. Ann. **133** (1957), 431–438.
174. *Hurwitz A.* New Mersenne primes, Math. Comput. **16** (1962), 249–251
175. *Iannucci D. E.* The second largest prime divisor of an odd perfect number exceeds ten thousand, Math. Comput. **68** (1999), 1749–1760.
176. *Iannucci D. E.* The third largest prime divisor of an odd perfect number exceeds one hundred, Math. Comput. **69** (2000), 867–879.
177. *Iannucci, D. E., Sorli R. M.* On the total number of prime factors of an odd perfect number. Math. Comput. **72** (2003), no. 244, 2077–2084.
178. *Imchenetski V., Bouniakowsky V.* Sur un nouveau nombre premier, annoncé par le père PERVOUCHINE. Extrait d'un rapport à l'Académie (Lu le 27 Janvier 1887), Bull. Acad. Impériale Sci., **31**, SPb, 1887, 532–533, `https://archive.org/stream/mobot31753003685184#page/n3 /mode/1up/search/Den`
179. *Jenkins P. M.* Odd perfect numbers have a prime factor exceeding 10^7, Math. Comput. **72** (2003), 1549–1554.
180. *Jerrard R. P., Temperley N.* Almost perfect numbers, Math. Mag. **46** (1973), 84–87.
181. *Jobling P.* Large Amicable Pairs. Jun. 6, 2004. `https://listserv.nodak.edu/scripts/wa.exe?A2=ind0306&L=nmbrthry&P=R97&D=0`.
182. *Jobling P.* A New Largest Known Amicable Pair." Mar. 10, 2005. `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0503&L=nmbrthry&F=&S=&P=552`.
183. *Kanold H.-J.* Untersuchungen über ungerade vollkommene Zahlen, J. Reine Angew. Math **183** (1941) 98–109.

184. *Kanold H.-J.* Folgerungen aus dem vorkommen einer Gauss'schen Primzahl in der Primfactorenzerlegung einer ungeraden vollkommenen Zahl, J. reine angew. Math. **186** (1949) 25–29.
185. *Kanold H.-J.* Über befreundete Zahlen. I, Math. Nachr. **9** (1953), 243–248.
186. *Kanold H.-J.* Über befreundete Zahlen. II, Math. Nachr., **10** (1953), 99–111.
187. *Kanold H.-J.* Über mehrfach vollkommene Zahlen II, J. reine angew. Math. **197** (1957) 82–96.
188. *Kanold H.-J.* Über "quasi-vollkommene Zahlen", Abh. Braunschweig Wiss. Ges. **40** (1988), 17–20.
189. *Kaplansky I.* Lucas' tests for Mersenne numbers. Amer. Math. Monthly **52** (1945), 188–190.
190. *Karst E.* New factors of Mersenne numbers, Math. Comput., **15** (1961), 51.
191. *Karst E.* Faktorenzerlegung Mersennescher Zahlen mittels programmgesteuerter Rechengeräte, Numer. Math., **3** (1961), 79–86.
192. *Karst E.* Search limits on divisors of Mersenne Numbers. Nordisk Tidskr. Informationsbehandling (BIT) **2** (1962), 224–227.
193. *Karst E.* A remarkable quartic yielding certain divisors of Mersenne numbers. Nordisk Tidskr. Informationsbehandling (BIT) **3** (1963), 122–123.
194. *Kishore M.* On odd perfect, quasiperfect, and odd almost perfect numbers, Math. Comput. **36** (1981), 583–586.
195. *Kishore M.* Odd perfect numbers not divisible by 3. II, Math. Comput. **40** (1983), 405–411.
196. *Kobayashi M., Pollack P., Pomerance C.* On the distribution of sociable numbers. J. Number Theory **129** (2009), no. 8, 1990–2009.
197. *Konyagin S., Acquaah P.* On prime factors of odd perfect numbers. Intern. J. Number Theory **8** (2012). no. 6. 1537–1540.
198. *Kozek M., Luca F., Pollack P., Pomerance C.* Harmonious pairs. Int. J. Number Theory 11 (2015), no. 5, 1633–1651.
199. *Kraitchik M.* Factorisation de $2^n \pm 1$, Sphinx, Bruxelles, **8** (1938), 148–150 .
200. *Kraitchik M.* On the factorization $2^n \pm 1$, Scripta Mathematica **18** (1952), 39–52.
201. *Kravitz S.* Divisors of Mersenne numbers $10,000 < p < 15,000$, Math. Comput., **15** (1961) p. 292–293.
202. *Kühnel U.* Verscharfung der notwendigen Bedingungen für die Existenz von ungeraden vollkommenen Zahlen, Math. Z. **52** (1949), 202–211.
203. *Lee E. J.* Amicable numbers and the bilinear diophantine equation. Math. Comput. **22** (1968), 181–187.
204. *Lee E. J.* On divisibility by nine of the sums of even amicable pairs. Math. Comput. **23** (1969), 545–548.
205. *Lee E. J., Madachy J. S.* The history and discovery of amicable numbers. I. J. Recreational Math. **5** (1972), no. 2, 77–93. Errata: **6** (1973), no. 2, 164. Errata: **6** (1973), no. 3, 229.
206. *Lee E. J., Madachy J. S.* The history and discovery of amicable numbers. II. J. Recreational Math. **5** (1972), no. 3, 153–173.
207. *Lee E. J., Madachy J. S.* The history and discovery of amicable numbers. III. J. Recreational Math. **5** (1972), no. 4, 231–249.
208. *Lehmer D. H.* Note on the Mersenne number $2^{139} - 1$, Bull. Amer. Math. Soc. **32** (1926), 522.
209. *Lehmer D. H.* Note on the largest Mersenne number. Bull. Amer. Math. Soc. **33** (1927), 271 .
210. *Lehmer D. H.* An extended theory of Lucas' functions, Ann. Math. **31** (1930), 419–448.
211. *Lehmer D. H.* Note on Mersenne numbers. Bull. Amer. Math. Soc. **38** (1932), 383–384.
212. *Lehmer D. H.* Some new factorizations of $2^n \pm 1$. Bull. Amer. Math. Soc. **39** (1933), 105–108.
213. *Lehmer D. H.* Hunting big game in the theory of numbers, Scripta Math., 1933, pp. 229–235.
214. *Lehmer D. H.* On Lucas' test for the primality of Mersenne numbers. J. London Math. Soc. **10** (1935), 162–165.
215. *Lehmer D. H.* On the factors of $2^n \pm 1$. Bull. Amer. Math. Soc. **53** (1947), 164–167.
216. *Lehmer D. H.* Recent discoveries of large primes, Mathematical Tables and Other Aids to Computation **6** (1952), 61.
217. *Lehmer D. H.* Two new Mersenne primes, Mathematical Tables and Other Aids to Computation **7** (1953), 72.
218. *Lehmer D. H.* Computer technology applied to the theory of numbers, Studies in Number Theory, vol. 6, W. J. LeVeque (Ed.), Math. Assoc. Amer.; distributed by Prentice-Hall, Englewood Cliffs, N. J., 1969, 117–151.

219. *Lehmer D. N.* Multiply perfect numbers. Ann. of Math. (2) **2** (1900/01), no. 1–4, 103–104.
220. *Luca F., Phaovibul M. T.* Amicable pairs with few distinct prime factors. Int. J. Number Theory **12** (2016), no. 7, 1725–1732.
221. *Luca F., Pomerance C.* The range of the sum-of-proper-divisors function. Acta Arithm. **168** (2015), 187–199.
222. *Luca F., te Riele.* ϕ and σ: from Euler to Erdős. Nieuw Arch. Wiskd. (5) **12** (2011), no. 1, 31–36.
223. *Luca F., te Riele.* Aliquot cycles of repdigits. Integers **12** (2012), no. 1, 129–140.
224. *Lucas E.* Sur la recherche des grands nombres premiers, Association Française pour l'Avancement des Sciences, Comptes Rendus, **5** (1876), 61–68.
225. *Macdivitt A. R. G.* The most recently discovered prime number. Math. Gaz. **63** (1979), no. 426, 268–270.
226. *Mason Th. E.* On amicable numbers and their generalizations, Amer. Math. Monthly, **28** (1921), 195–200.
227. *McCarthy P. J.* Odd perfect numbers, Scripta Mathematica **23** (1957), 43–47.
228. *McDaniel W. L.* On odd multiply perfect numbers, Boll. Un. Mat. Ital. **2** (1970), 185–190.
229. *McDaniel W. L., Hagis P. Jr* Some results concerning the non-existence of odd perfect numbers of the form $p^{\alpha}M^{2\beta}$. Fibonacci Quart. **13** (1975), 25–28.
230. *Mercenne M.* Cogitata physico mathematica, 1644, 726p. `https://gallica.bnf.fr/ark:/12148/bpt6k81531h.r=mersenne.langFR`
231. *Mercenne M.* Novarum observationum physico mathématicarum, 1647, 275p. `https://gallica.bnf.fr/ark:/12148/bpt6k815336.r=mersenne.langFR`
232. *Minoli D.* Issues in nonlinear hyperperfect numbers. Math. Comput. **34** (1980), no. 150, 639–645.
233. *Moews D., Moews P. C.* A search for aliquot cycles below 10^{10}, Math. Comput. **5**7 (1991), 849–855
234. *Moews D., Moews P. C.* A search for aliquot cycles and amicable pairs. Math. Comput. **61** (1993), 935–938.
235. *Moews D., Moews P. C.* A list of amicable pairs below 2.01×10^{11}. Rev. Jan. 8, 1993b. `https://xraysgi.ims.uconn.edu:8080/amicable.txt`.
236. *Moews D., Moews P. C.* A list of the first 5001 amicable pairs. Rev. Jan. 7, 1996. `https://xraysgi.ims.uconn.edu:8080/amicable2.txt`.
237. *Moreira C. G., Saldanha N. C.* Primos de Mersenne (e outros primos muito grandes). 22o Colóquio Brasileiro de Matemática. Instituto de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, 1999. 81p.
238. *Murata L., Pomerance C.* On the largest prime factor of a Mersenne number. Number theory, 209–218, CRM Proc. Lecture Notes, 36, Amer. Math. Soc., Providence, RI, 2004.
239. *Narkiewicz W.* Classical problems in number theory. Monografie Matematyczne **62**, PWN, Warszawa, 1986. 363p.
240. *Nguyen Hanh My, Pomerance C/* The reciprocal sum of the amicable numbers. Math. Comput. **88** (2019), no. 317, 1503–1526.
241. *Nielsen P. P.* An upper bound for odd perfect numbers, Integers **3** (2003), A14, 1–9.
242. *Nielsen P. P.* Odd perfect numbers have at least nine distinct prime factors, Math. Comput. **76** (2007), 2109–2126.
243. *Nielsen P. P.* Odd perfect numbers, Diophantine equations, and upper bounds. Math. Comput. **84** (2015), no. 295, 2549–2567.
244. *Noll L. C., Nickel L.* The 25th and 26th Mersenne primes. Math. Comput. **35** (1980), no. 152, 1387–1390.
245. *Ochem P., Rao M.* Odd perfect numbers are greater than 10^{1500}, Math. Comput. **81** (2012), 1869–1877.
246. *Ochem P., Rao M.* On the number of prime factors of an odd perfect number". Math. Comput. **83** (2014), no. 289, 2435–2439.
247. *Ondrejka R.* More on large primes. J. Recreational Math. **11** (1978/79), no. 2, 112–113
248. *Ondrejka R.* More very large twin primes. J. Recreational Math. **15** (1982/83), no. 1, 7.
249. *Paganini B. N. I.* Atti della R. Accad. Sc. Torino **2** (1866–1867), 362.
250. *Parks J.* Amicable pairs and aliquot cycles on average. Int. J. Number Theory **11** (2015), no. 6, 1751–1790
251. *Pedersen J. M.* Known amicable pairs, online at `http://amicable.homepage.dk/knwnc2.htm`.

252. *Pedersen J. M.* Various amicable pair lists and statistics, `http://www.vejlehs.dk/staff/jmp/aliquot/apstat.htm`.
253. *Perrott J.* Sur une proposition empirique énoncée au Bulletin, Bull. Soc. Math. France **17** (1889) 155–156.
254. *Pollack P.* A remark on sociable numbers of odd order. J. Number Theory **130** (2010), no. 8, 1732–1736.
255. *Pollack P.* On Dickson's theorem concerning odd perfect numbers. Amer. Math. Monthly **118** (2011), no. 2, 161–164.
256. *Pollack P.* Powerful amicable numbers. Colloq. Math. **122** (2011), no. 1, 103–123.
257. *Pollack P.* Quasi-amicable numbers are rare, J. Integer Seq. **14** (2011), art. 11.5.2, 13 pp
258. *Pollack P.* The greatest common divisor of a number and its sum of divisors, Michigan Math. J. **60** (2011), 199–214.
259. *Pollack P.* Finiteness theorems for perfect numbers and their kin, Amer. Math. Monthly **119** (2012), 670–681; errata in **120** (2013), 482–483.
260. *Pollack P.* On relatively prime amicable pairs. Mosc. J. Comb. Number Theory **5** (2015), no. 1–2, 36–51.
261. *Pollack P., Pomerance C.* Prime-perfect numbers. Integers **12** (2012), no. 6, 1417–1437.
262. *Pollack P., Pomerance C.* Erdős and the rise of statistical thinking in elementary number theory. Erdős centennial, 515–533, Bolyai Soc. Math. Stud., 25, János Bolyai Math. Soc., Budapest, 2013.
263. *Pollack P., Pomerance C.* Some problems of Erdős on the sum-of-divisors function. Trans. Am. Math. Soc. Ser. B **3** (2016), 1–26.
264. *Pollack P., Pomerance C., Thompson L.* Divisor-sum fibers. Mathematika **64** (2018), no. 2, 330–342.
265. *Pollack P., Shevelev V.* On perfect and near-perfect numbers. J. Number Theory **132** (2012), no. 12, 3037–3046.
266. *Pomerance C.* Odd perfect numbers are divisible by at least seven distinct primes, Acta Arith. **25** (1974) 265–300.
267. *Pomerance C.* Multiply perfect numbers, Mersenne primes, and effective computability, Math. Ann. **226** (1977), 195–206.
268. *Pomerance C.* On the distribution of amicable numbers. J. reine angew. Math. **293/294** (1977), 217–222.
269. *Pomerance C.* On the distribution of amicable numbers, II. J. reine angew. Math. **325** (1981), 182–188.
270. *Pomerance C.* On primitive divisors of Mersenne numbers. Acta Arith. **46** (1986), no. 4, 355–367.
271. *Pomerance C.* On amicable numbers. in: Analytic number theory, 321–327, Springer, Cham, 2015.
272. *Pomerance C.* The first function and its iterates. Connections in discrete mathematics, 125–138, Cambridge Univ. Press, Cambridge, 2018.
273. *Pomerance C.* The aliquot constant, after Bosma and Kane. Q. J. Math. **69** (2018), no. 3, 915–930.
274. *Pomey L.* Sur les nombres de Fermat et de Mersenne. Ann. Fac. Sci. Toulouse Sci. Math. Sci. Phys. (3) **16** (1924), 135–138.
275. *Poulet P.* Sur les nombres multiparfaits. Association Française Grenoble 1925, 88.
276. *Poulet P.* La chasse aux nombres. I: Parfaits, amiables et extensions. Bruxelles: Stevens. (1929), 72p.
277. *Poulet P.* Forty-three new couples of amicable numbers, Scripta Math., **14** (1948), 77.
278. *Powers R. E.* The tenth perfect number. Amer. Math. Monthly **18** (1911), no. 11, 195–197.
279. *Powers R. E.* The tenth perfect number. Amer. Math. Soc. Bull. (2) **18** (1912),
280. *Powers R. E.* On Mersenne's Numbers, Proc. London Math. Soc. **13** (1914), 39.
281. *Powers R. E.* A Mersenne prime. Bull. Amer. Math. Soc.. (2) **20** (1914), 531.
282. *Powers R. E.* Certain composite Mersenne's numbers. Proc. London Math. Soc. (2) **15** (1917), 22
283. *Powers R. E.* Note on a Mersenne number. Bull. Amer. Math. Soc. **40** (1934), 883.
284. *Reid C.* From zero to infinity. What makes numbers interesting. 4th edition. MAA Spectrum. Mathematical Association of America, Washington, DC, 1992. xvi+ 186p.
285. *Reidlinger H.* Über ungerade mehrfach vollkommene Zahlen, Österreichische Akad. Wiss. Math. Natur. **192** (1983), 237–266.
286. *Ribenboim P.* The book of prime number records. 2nd edition. Springer-Verlag, New York, 1989. xxiv+479 pp

287. *Ribenboim P.* The new book of prime number records. Springer-Verlag, New York, 1996. xxiv+541p.
288. *Ribenboim P.* My numbers, my friends. Popular lectures on number theory. Springer-Verlag, New York, 2000. xii+375p.
289. *Ribenboim P.* The little book of bigger primes. 2nd edition. Springer-Verlag, New York, 2004. xxiv+356p.
290. *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.
291. *Rieger G. J.* Bemerkung zu einem Ergebnis von Erdős über befreundete Zahlen, J. reine angew. Math. **261** (1973) 157–163.
292. *te Riele H. J. J.* Four large amicable pairs, Math. Comput., **28** (1974), 309–312.
293. *te Riele H. J. J.* Hyperperfect numbers with three different prime factors. Math. Comput. **36** (1981), no. 153, 297–298.
294. *te Riele H. J. J.* Perfect numbers and aliquot sequences, Computational methods in number theory, Part I, Math. Centre Tracts, **154**, Math. Centrum, Amsterdam, 1982, 141–157.
295. *te Riele H. J. J.* New very large amicable pairs, Number Theory Noordwijkerhout 1983 (H. Jager, ed.), Springer-Verlag, 1984, pp. 210–215.
296. *te Riele H. J. J.* On generating new amicable pairs from given amicable pairs, Math. Comput. **42** (1984), 219–223.
297. *te Riele H. J. J.* Rules for constructing hyperperfect numbers. Fibonacci Quart. **22** (1984), no. 1, 50–60.
298. *te Riele H. J. J.* Computation of all the amicable pairs below 10^{10}. Math. Comput. **47** (1986), 361–368, S9–S40.
299. *te Riele H. J. J.* A new method for finding amicable pairs. Mathematics of Computation 1943–1993: a half-century of computational mathematics (Vancouver, BC, 1993), 577–581, Proc. Sympos. Appl. Math., 48, Amer. Math. Soc., Providence, RI, 1994.
300. *te Riele H. J. J.* Grootschalig rekenen in de getaltheorie Nieuw Arch. Wiskd. (5) **14** (2013), no. 4, 236–243.
301. *te Riele H. J. J., Borho W., Battiato S., Hoffmann H., Lee E. J.* Table of amicable pairs between 10^{10} and 10^{52} (1986), Technical Report NM-N8603, Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098 SJ Amsterdam, the Netherlands
302. *Riesel H.* Några stora primtal. Elementa **39** (1956), 258–260.
303. *Riesel H.* A new Mersenne prime, Math. Tables Aids Comput. **12** (1958), 60.
304. *Riesel H.* Mersenne numbers, Math. Tables Aids Comput. **12** (1958), 207–213.
305. *Riesel H.* All factors $q < 10^8$ in all Mersenne numbers $2^p - 1$, p prime $< 10^4$. Math. Comput. **16** (1962), 478–482.
306. *Roberts T.* On the form of an odd perfect number, Australian Math. **35** (2008), no. 4, 244.
307. *Robinson R. M.* Mersenne and Fermat numbers. Proc. Amer. Math. Soc.**5** (1954), 842–846.
308. *Robinson R. M.* Some factorizations of numbers of the form $2^n \pm 1$, Math. Tables Aids Comput. **11** (1957) 265–268,
309. *Rosen M. I.* A Proof of the Lucas—Lehmer Test, Amer. Math. Monthly, **95** (1988), 855–856.
310. *Rouse Ball W. W.* Mersenne's numbers. Mess. (2) **21** (1891), 34–40.
311. *Sándor J., Crstici B.* Handbook of number theory. II. Kluwer Academic Publishers, Dordrecht, 2004. ii+637 pp
312. *Sándor J., Mitrinović D. S., Crstici B.* Handbook of number theory. I. Second printing of the 1996 original. Springer, Dordrecht, 2006. xxvi+622
313. *du Sautoy M.* The music of the primes. Searching to solve the greatest mystery in mathematics. Harper Collins Publishers, New York, 2003. x+335p.
314. *Scheffler D., Ondrejka R.* The numerical evaluation of the eighteenth perfect number. Math. Comput. **14** (1960), 199–200.
315. *Schinzel A., Sierpiński W.* Sur certaines hypothèses concernant les nombres premiers, Acta Arith. **4** (1958), 185–208; erratum **5** (1958), 259.
316. *Selfridge J. L., Hurwitz A.* Fermat numbers and Mersenne numbers. Math. Comput. **18** (1964), 146–148.

317. *Shanks D., Kravitz S.* On the distribution of Mersenne divisors, Math. Comput., **21** (1967), 97–101.
318. *Sierpiński W.* Les nombres de Mersenne et de Fermat. Matematiche (Catania) **10** (1955), 80–91.
319. *Sierpiński W.* O liczbach złodżonych postaci $(2^p + 1)/3$, gdzie p jest liczbą pierwszą, Prace Mat. 7 (1962). 169–172.
320. *Sierpiński W.* Elementary theory of numbers. 2nd edition. Edited and with a preface by Andrzej Schinzel. North-Holland Mathematical Library, 31. North-Holland Publishing Co., Amsterdam; PWN—Polish Scientific Publishers, Warszawa, 1988. xii+515 pp.
321. *Sitaramaiah V., Subbarao M. V.* On unitary multiperfect numbers. Nieuw Arch. Wisk. (4) **16** (1998), no. 1–2, 57–61.
322. *Skula L.* Prime power divisors of Mersenne numbers and Wieferich primes of higher order. Integers 19 (2019), Paper No. A19, 4 pp.
323. *Slowinski D.* Searching for the 27th Mersenne prime. J. Recreational Math. **11** (1978/79), no. 4, 258–267.
324. *Steuerwald R.* Verscharfung einen notwendigen Bedeutung für die Existenz einen ungeraden volkommenen Zahl, Bayer. Akad. Wiss. Math. Natur. (1937), no. 2, 69–72.
325. *Steuerwald R.* Ein Satz über natürliche Zahlen mit $\sigma(N) = 3N$. Arch. Math. **5** (1954), 449–451.
326. *Stewart I.* Professor Stewart's incredible numbers. Basic Books, New York, 2015. ix+341 pp.
327. *Stewart I.* Do dice play God? The mathematics of uncertainty. Basic Books, New York, 2019. 292 pp.
328. *Subbarao M. V.* Odd perfect numbers: some new issues. Period. Math. Hungar. **38** (1999), no. 1–2, 103–109.
329. *Subbarao M. V., Cook T. J., Newberry R. S., Weber J. M.* On unitary perfect numbers. Delta (Waukesha) **3** (1972/73), no. 1, 22–26.
330. *Subbarao M. V., Warren L. J.* Unitary perfect numbers. Canad. Math. Bull. **9** (1966), 147–153.
331. *Suryanarayana D.* Super perfect numbers, Elemente Math., **24** (1969), 16–17.
332. *Suryanarayana D.* Quasiperfect numbers. II, Bull. Calcutta Math. Soc. **69** (1977), 421–426.
333. *Suzuki Y.* On amicable tuples. Illinois J. Math. **62** (2018), no. 1–4, 225–252.
334. *Sylvester J. J.* Sur l'impossibilité de l'existence d'un nombre parfait impair qui ne contient pas au moins 5 diviseurs premiers distincts, Comptes Rendus Acad. Sci. Paris, **106** (1888), 522–526.
335. *Touchard J.* On prime numbers and perfect numbers. Scripta Math. **19** (1953), 35–39.
336. *Troupe L.* On the number of prime factors of values of the sum-of-proper-divisors function. J. Number Theory **150C** (2015), 120–135.
337. *Tuckerman B.* The 24th Mersenne prime. Proc. Nat. Acad. Sci. U.S.A. **68** (1971), 2319–2320.
338. *Tuckerman B.* A search procedure and lower bound for odd perfect numbers. Math. Comput., **27** (1973), 943–949. Corrigenda: **28** (1974), 887.
339. *Tuckerman B.* Corrigendum: "Three new Mersenne primes and a statistical theory" (Math. Comput. **18** (1964), 93–97) by D. B. Gillies. Math. Comput. **31** (1977), no. 140, 1051.
340. *Uhler H. S.* First proof that the Mersenne number M_{157} is composite, Proc. Nat. Acad. Sci. U.S.A. **30** (1944), 314–316.
341. *Uhler H. S.* Note on the Mersenne numbers M_{157} and M_{167}, Bull. Amer. Math. Soc. **52** (1946), 178;
342. *Uhler H. S.* A new result concerning a Mersenne number, Mathematical Tables and Other Aids to Computation **2** (1946), 94.
343. *Uhler H. S.* On Mersenne's number M_{199} and Lucas's sequences, Bull. Amer. Math. Soc. **53** (1947), 163–164;
344. *Uhler H. S.* On Mersenne's number M_{227} and cognate data, Bull. Amer. Math. Soc. **54** (1948), 379;
345. *Uhler H. S.* On all of Mersenne's numbers particularly M_{193}, Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 102–103;
346. *Uhler H. S.* A brief history of the investigations on Mersenne's numbers and the latest immense primes, Scripta Mathematica **18** (1952), 122–131;
347. *Uhler H. S.* On the 16th and 17th perfect numbers, Scripta Mathematica, **19** (1953), 128–131.
348. *Uhler H. S.* Full values of the first seventeen perfect numbers. Scripta Math. 20, 240 (1954).
349. *Viêt Chu Hùng* What's Special about the Perfect Number 6? Amer. Math. Monthly **128** (2020), no. 1, 87.
350. *Wagstaff S. S. Jr.* Divisors of Mersenne numbers, Math. Comput., **40** (1983) 385–397

351. *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.
352. *Wagstaff S. S. Jr.* The joy of factoring. Student Mathematical Library, 68. Amer. Math. Soc., Providence, RI, 2013. xiv+293p.
353. *Walker A.* New Large Amicable Pairs. May 12, 2004.https://listserv.nodak.edu/scripts/wa.exe?A2=ind0405&L=nmbrthry&F=&S=&P=1043.
354. *Wall C. R.* Bi-unitary perfect numbers. Proc. Amer. Math. Soc. 33 (1972), 39–42.
355. *Warren L. J., Bray H. G.* On the square-freeness of Fermat and Mersenne numbers. Pacific J. Math. **22** (1967), 563–564.
356. *Watkins J.* Number theory. A historical approach. Princeton University Press, Princeton, NJ, 2014. xvi+576p.
357. *Webber G. C.* Non-existence of odd perfect numbers of the form $3^{2\beta}p^{\alpha}s_1^{2\beta_1}s_2^{2\beta_2}s_3^{2\beta_3}$, Duke Math. J. **18** (1951) 741–749.
358. *Western A. E.* On Lucas' and Pepin's tests for the primeness of Mersenne's numbers. J. London Math. Soc. **7** (1932), 130–137. Corrigenda:J. London Math. Soc. 7 (1932), no. 4, 272.
359. *Williams H. C.* Édouard Lucas and Primality Testing. Wiley, 1998.
360. *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.
361. *Wirsing E.* Bemerkung zu der Arbeit über vollkommene Zahlen. Math. Ann. **137** (1959), 316–318.
362. *Woodall H. J.*. Note on a Mersenne number. Bull. Amer. Math. Soc. (2) **17** (1911), 540.
363. *Woodall H. J.* Mersenne's numbers. Manchester Mem. and Proc. **56** (1912), no. 1, 1–5.
364. *Woltman G.* GIMPS: Mathematics and Research Strategy, http://mersenne.org/math.htm.
365. *Woltman G.* On the discovery of the 38th known Mersenne prime. Fibonacci Quart. **37** (1999), 367–370.
366. *Woltman G., Kurowski S.* On the discovery of the 45th and 46th known Mersenne primes. Fibonacci Quart. **46/47** (2008/09), no. 3, 194–197.
367. *Yamada T.* On the divisibility of odd perfect numbers, quasiperfect numbers and amicable numbers by a high power of a prime. Integers **20** (2020), Paper no. A91, 1–17.
368. *Yamagami A.* On the numbers of prime factors of square free amicable pairs. Acta Arith. **177** (2017), no. 2, 153–167.
369. *Yates S.* Titanic primes. J. Recreational Math. **16** (1983/84), no. 4, 250–262.
370. *Yates S.* Sinkers of the titanics. J. Recreational Math. **17** (1984/85), no. 4, 268–274.
371. *Yates S.* Tracking titanics, in The Lighter Side of Mathematics, Proc. Strens Mem. Conf., Calgary 1986, Math. Assoc, of America, Washington DC, Spectrum series, 1993, 349–356.
372. *Yuan Pingzhi* An upper bound for the number of odd multiperfect numbers. Bull. Aust. Math. Soc. **89** (2014), no. 1, 1–4.
373. *Yuan Pingzhi, Zhang Zhongfeng* Addition to 'An upper bound for the number of odd multiperfect numbers'. Bull. Aust. Math. Soc. **89** (2014), no. 1, 5–7.
374. *Zelinsky J.* Upper bounds on the second largest prime factor of an odd perfect number. International Journal of Number Theory. **15** (2019), no. 6, 1183–1189.

ГРНТИ 00000

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

Computer tools in education, 2020
№ -: 2–47
http://ipo.spb.ru/journal
doi:10.1000/182

Computers as novel mathematical reality. III. Mersenne numbers and divisor sums

N. A. Vavilov
SPbU

Abstract

Nowhere in mathematics is the progress resulting from the advent of computers is as apparent, as in the additive number theory. In this part, we describe the role of computers in the investigation of the oldest function studied in mathematics, the divisor sum. The disciples of Pythagoras started to systematically explore its behaviour more that 2500 years ago. A description of the trajectories of this function — perfect numbers, amicable numbers, sociable numbers, and the like — constitute the contents of several problems stated over 2500 years ago, which still seem completely inaccessible. A theorem due to Euclid and Euler reduces classification of *even* perfect numbers to Mersenne primes. After 1914 not a single new Mersenne prime was ever produced manually, since 1952 all of them have been discovered by computers. Using computers, now we construct hundreds or thousands times more new amicable pairs *daily*, than what was constructed by humans over several millenia. At the end of the paper, we discuss yet another problem posed by Catalan and Dickson.

Keywords: *Mersenne primes, divisor sums, суммы делителей, perfect numbers, amicable numbers, sociable numbers, aliquot sequences, Catalan—Mersenne conjecture, Catalan—Dickson conjecture, Guy—Selfridge conjecture*

Citation: N. A. Vavilov. Computers as novel mathematical reality.
III. Mersenne numbers and divisor sums. Computer tools in education, 2020. № -. P. 2–47
: DOI: http://dx.doi.org/10.1000/182.

Acknowledgements: *here we may thank everybody who helped authors with this paper, and name grants that supported the research and the paper.*

Received October 7, 2020, The final version: December 28, 2020

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**