Обманчивая простота

В. М. Журавлёв, П. И. Самовол

Говорят, истина лежит между двумя противоположными мнениями. Неверно! Между ними лежит проблема.

Иоганн Вольфганг Гёте

Стоящие с семнадцатого века вопросы построения больших простых чисел, проверки на простоту и разложения чисел на сомножители ставят теперь новые и конкретные проблемы. Насколько могут быть быстрыми алгоритмы нахождения ответов на эти вопросы? Проблема проверки на простоту уже решена. Две другие проблемы ещё не получили своего теоретического решения. Тем не менее, первая из них кажется более простой, чем другая.

Ю. И. Манин, А. А. Панчишкин. Введение в современную теорию чисел

§ 1. Красивые не простые степени

В 1986 году была издана книга [13], авторы которой Б. А. Кордемский и А. А. Ахадов в предисловии отмечают: «Некоторые из предлагаемых авторами задач близки по форме и содержанию задачам школьных учебников. Другие — по трудности на ступеньку выше, оставаясь всё же в границах доступности для учащихся VIII–X классов и всех, окончивших школу. Но те и другие задачи нацелены на проникновение разумом в удивительный мир чисел, на раскопку его богатств, на возбуждение математической любознательности и собственной инициативы». Книга была красочно иллюстрирована и рассчитана на учащихся.

Обратим внимание на одну из задач.

Задача 1 (Красивые не простые степени, [13, с. 82, 86.]).
1) Докажите, что $7777^{2222} + 2222^{7777}$ делится на 9.
2) Докажите, что $2222^{2222} + 4444^{4444} + 8888^{8888}$ делится на 3.
3) Докажите, что сумма $2^{2145} + 3^{2145}$ делится на 241, на 341 и на 11.

Первому пункту задачи даже посвящена иллюстрация книги (рис. 1).

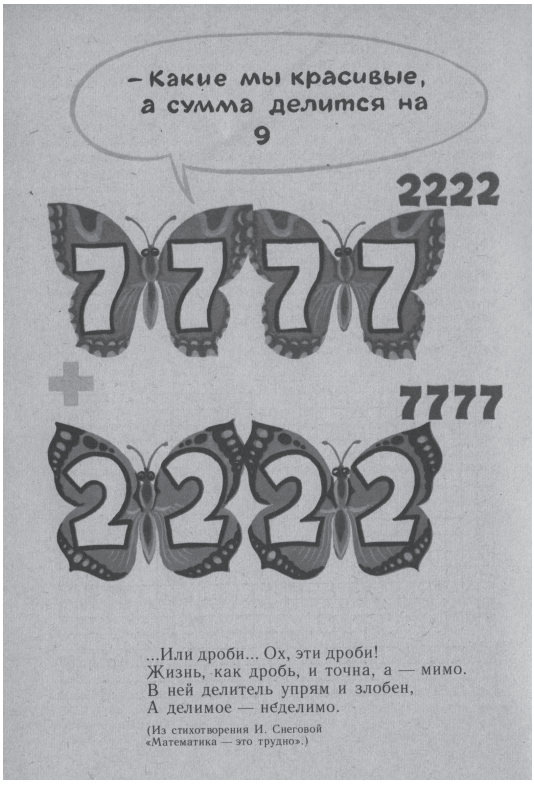


Рис. 1. Иллюстрация из книги [13]

Поскольку числа 2222 и 7777 делятся на 1111, понятно, что сумма $7777^{2222} + 2222^{7777}$ делится на 1111. Идея в том, чтобы показать ученику, что так сконструированные числа могут иметь другие делители. Заинтересовать учащегося поиском закономерностей, не лежащих на поверхности.

Напомним формулы сокращённого умножения, изучаемые в школе:

$$A^n - B^n = (A-B)(A^{n-1} + A^{n-2}B + \ldots + AB^{n-2} + B^{n-1}) \quad \text{для} \quad n \in \mathbb{N},$$
$$A^{2k+1} + B^{2k+1} = (A+B)(A^{2k} - A^{2k-1}B + \ldots - AB^{2k-1} + B^{2k}) \quad \text{для} \quad k \in \mathbb{N}.$$

Если учащийся знает эти формулы, то, применив приём «прибавить—отнять», он решит задачу в пару строчек. Действительно, прибавим и отнимем единицу, получим

$$7777^{2222} + 2222^{7777} = (7777^{2222} - 1^{2222}) + (2222^{7777} + 1^{7777}).$$

Первая скобка делится на 7776 и, следовательно, на 9, а вторая скобка делится на 2223, т. е. тоже делится на 9. Значит, сумма делится на 9.

Похожие задачи мы можем найти в разных источниках (см., например, [9, 16, 23]).

Задача 2.

1) [23, с. 20, задача 63]. Докажите, что $2222^{5555} + 5555^{2222}$ делится на 7.

2) [9, с. 140, задача 11.56]. Докажите, что число $222^{555} + 555^{222}$ составное.

3) [16, с. 85, задача 4г]. Число $30^{239} + 239^{30}$ составное.

Пункт 2 можно усложнить: докажите, что сумма из п. 2 делится на 7.

В книгах, рассчитанных на педагогов, мы видим более строгие формулировки похожих задач.

Задача 3 [21, с. 8, задача 3]. Докажите равенства:

а) $19^{71} + 71^{19} = 360m + 90$;

б) $19^{77} + 77^{19} = 456n + 96$.

Задача 4 [16, с. 85, задача 4в]. Если p и q — различные простые числа, то $p^q + q^p \equiv p + q \pmod{pq}$.

В книге [23], ставшей классикой литературы для математических кружков, отметим ещё одну задачу.

Задача 5 [23, с. 21, задача 70]. При каких натуральных n сумма $5^n + n^5$ делится на 13? Каково наименьшее n, удовлетворяющее этому условию?

В § 3 мы вернёмся к этой задаче.

В приведённых примерах рассматриваются суммы вида $a^n + n^a$, где $a, n \in \mathbb{N}$. В зависимости от пары a, n такая сумма может быть как составным, так и простым числом.

Исключим из рассмотрения простейшие случаи, когда $a = 1$ или $n = 1$. Очевидно, что если числа a и n имеют общий делитель d, то сумма будет делиться на d и, следовательно, будет составным числом. Такие примеры мы видели выше.

Чтобы задача выглядела более содержательной, числа a и n будем считать взаимно простыми, т. е. НОД$(a, n) = 1$. Минимальный пример,

когда сумма является простым числом, мы получим для пары $a = 2$ и $n = 3$, тогда $2^3 + 3^2 = 17$ — простое число. (В силу симметрии, пара $a = 3$, $n = 2$ даёт то же простое число 17.)

Нас будут интересовать два вопроса.

1) Есть ли другие примеры таких пар $2 \leqslant a$ и $2 \leqslant n$, что сумма $a^n + n^a$ является простым числом?

2) Если сумма $a^n + n^a$ является составным числом, где a и n — взаимно простые числа, то какие делители она имеет?

§ 2. Олимпиадные задачи и теорема Софи Жермен

Наши изыскания начнём со случая $a = 4$. Пусть читатели нас не осуждают за перепрыгивание случаев $a = 2$ и $a = 3$, мы вернёмся к ним чуть позже.

Для начала докажем одну теорему, носящую имя Софи Жермен (Marie-Sophie Germain). Софи Жермен переписывалась со многими математиками своего времени, в том числе с Гауссом, Даламбером, Лагранжем, Фурье. Она становится первой женщиной, получившей право участия в заседаниях Парижской Академии наук. Подробности биографии Софи Жермен можно прочесть в [10].

Теорема 1 (Софи Жермен, [9, с. 139, задача 11.51а]). *Число* n^4+4 — *составное при всех натуральных* $n \neq 1$.

Доказательство. Применим упоминавшийся нами искусственный приём: добавим и вычтем $4n^2$. Имеем

$$n^4 + 4 = n^4 + 4n^2 + 4 - 4n^2 = (n^2 + 2)^2 - (2n)^2 = (n^2 + 2n + 2)(n^2 - 2n + 2).$$

Так как $n > 1$, получаем, что

$$n^2 - 2n + 2 = (n - 1)^2 + 1 > 1.$$

Число $n^4 + 4$ представимо в виде произведения двух множителей, не равных ему самому и единице, следовательно, это число составное. Что и требовалось доказать. □

Изящество и простота доказательства не могут не вызвать восхищения. Эта идея в завуалированном виде возникает в олимпиадных задачах.

Задача 6 (олимпиада Чехословакии, 1973, [12, с. 12, задача 1.9]). Докажите, что существует бесконечно много значений $n \in \mathbb{N}$, для которых любое число вида $m^4 + n$ $(m \in \mathbb{N})$ является составным.

Задача 7 (XV Всероссийская олимпиада, 1989, [25], [9, с. 142, задача 11.92]). Докажите, что число $4^{545} + 545^4$ является составным.

Задача 7 является частным случаем задачи, предлагавшейся на венгерской математической олимпиаде 1977 года.

Задача 8 (олимпиада Венгрии, 1977, [12, с. 15, задача 2.17]). Докажите, что для любого простого числа $p > 5$ уравнение $x^4 + 4^x = p$ в целых числах не имеет решений.

В формулировке задачи область допустимых значений переменной x — целые числа. Однако понятно, что её расширение с натуральных чисел до целых ничего нового нам не даёт.

Действительно, если $x < 0$, то $x^4 + 4^x$ — не целое. При $x = 0$ имеем $x^4 + 4^x = 1$. А, как известно, единица не является ни составным, ни простым числом.

Решение задачи 8. Учитывая вышесказанное, нам осталось рассмотреть случай, когда x — натуральное число. При $x = 1$ имеем $x^4 + 4^x = 5$, но по условию $p > 5$. Итак, остаётся $x \in \mathbb{N}$, $x \geqslant 2$. Докажем, что в этом случае $x^4 + 4^x$ является составным числом.

Если $x = 2k$, где $k \in \mathbb{N}$, то $x^4 + 4^x = 2^4k^4 + 4^{2k}$ делится на 16, следовательно, не является простым.

Если $x = 2k + 1$, где $k \in \mathbb{N}$, то применим формулы сокращённого умножения для разложения на множители. Имеем

$$\begin{aligned} x^4 + 4^x = x^4 + 4^{2k+1} &= x^4 + (2^{2k+1})^2 = \\ &= x^4 + 2 \cdot 2^{2k+1}x^2 + (2^{2k+1})^2 - 2 \cdot 2^{2k+1}x^2 = \\ &= (x^2 + 2^{2k+1})^2 - (2^{k+1}x)^2 = \\ &= (x^2 + 2^{2k+1} + 2^{k+1}x)(x^2 + 2^{2k+1} - 2^{k+1}x) = \\ &= ((x + 2^k)^2 + 2^{2k})((x - 2^k)^2 + 2^{2k}). \end{aligned}$$

Поскольку каждый из сомножителей больше 1, исходное выражение является составным числом. Что и требовалось доказать. □

Хотя решение задач занимает пару абзацев, они предлагались на соревнованиях достаточно высокого уровня.

Упражнение 1 [9, с. 139, задача 11.51б]. Число $n^4 + 4m^4$ — составное при всех натуральных n и m, одновременно не равных 1.

Итак, случай $a = 4$ полностью разобран. Сумма $4^n + n^4$ является составным числом для любого натурального $n \geqslant 2$.

Вернёмся теперь к решению задачи 5.

§ 3. Случай $5^n + n^5$

В книге [23] решение задачи 5 занимает несколько страниц. Идея решения состоит в вычислении остатков каждого из слагаемых при делении на 13. Для удобства эти остатки вносятся в таблицу. После этого становится видна некоторая периодическая закономерность.

Посмотрим на это решение, опуская детали.

Решение задачи 5. Рассмотрим последовательность $\{n^5\}$, $n = 0, 1, 2, \ldots$ Сопоставим этой последовательности другую последовательность $\{r'_n\}$, где r'_n — остаток от деления n^5 на 13. Таким образом, последовательности 0, 1, 32, 243, 1024, 3125, … мы сопоставили последовательность 0, 1, 6, 9, 10, 5, … Последовательность $\{r'_n\}$ периодична с периодом 13.

Аналогично рассмотрим последовательность $\{5^n\}$, $n = 0, 1, 2, \ldots$, и сопоставим ей последовательность $\{r''_n\}$, где r''_n — остаток от деления 5^n на 13. Теперь последовательности 1, 5, 25, 125, 625, 3125, … мы сопоставили последовательность 1, 5, 12, 8, 1, 5, … Как видим, члены последовательности начали повторяться начиная с пятого. Значит, последовательность $\{r''_n\}$ периодична с периодом 4. Действительно, остаток от деления 5^n на 13 совпадает с остатком от деления $5^{(4k+n)} = 5^n \cdot (5^4)^k$ на 13 для любого целого $k \geqslant 0$, поскольку 5^4 даёт остаток 1 при делении на 13.

Таким образом, последовательность $\{r_n\}$, являющаяся последовательностью остатков от деления суммы $5^n + n^5$ на 13, периодична с периодом $52 = 4 \cdot 13$.

Внесём полученные данные в таблицу 1.

Продолжив нашу таблицу, убедимся, что остаток от деления $5^n + n^5$ на 13 равен нулю только в случаях $n = 52k + 12$, $n = 52k + 14$, $n = 52k + 21$, $n = 52k + 31$, где $k \in \mathbb{Z}$, $k \geqslant 0$.

Наименьшее n, при котором сумма $5^n + n^5$ делится на 13, равно 12. Это также видно из таблицы 1. □

Таблица 1

n	0	1	2	3	4	5	6	7	8	9	10	11	12
n^5	0	1	32	243	1024	3125	7776	16 807	32 768	9^5	10^5	11^5	12^5
r'_n	0	1	6	−4	−3	5	2	−2	−5	3	4	−6	−1
5^n	1	5	25	125	625	3125	15 625	78 125	390 625	5^9	5^{10}	5^{11}	5^{12}
r''_n	1	5	−1	−5	1	5	−1	−5	1	5	−1	−5	1
r_n	1	6	5	4	−2	−3	1	6	−4	−5	3	2	0

Мы специально разобрали это решение, чтобы отметить возникающие закономерности. В дальнейшем мы укажем ряд теорем, упрощающих такие рассуждения.

Сделаем выводы из решения задачи. Во-первых, в последовательности $\{5^n + n^5\}$ бесконечно много чисел, делящихся на 13 (четыре семейства).

Во-вторых, нам ничто не мешало взять другое простое число p и провести аналогичные рассуждения. Мы получили бы другую периодическую последовательность остатков и для каких-то значений n сумма $5^n + n^5$ делилась бы на p.

Упражнение 2. При каких натуральных n сумма $5^n + n^5$ делится на а) 3; б) 7; в) 11? Каково наименьшее n, удовлетворяющее этому условию?

Упражнение 3. Докажите, что для любого простого p существует бесконечно много натуральных n таких, что сумма $5^n + n^5$ делится на p.

Итак, в последовательности $\{5^n + n^5\}$ бесконечно много составных чисел. Но встречаются ли в этой последовательности простые числа?

Если n нечётное, то сумма $5^n + n^5$ делится на 2. Если 5 и n не взаимно простые, то $5^n + n^5$ делится на 5. Поэтому если в последовательности $\{5^n + n^5\}$ есть простые числа, то число n должно иметь вид $n = 2(5k + r)$, где $r = 1, 2, 3, 4$, а k — целое неотрицательное число.

Таблица 2

n	$5^n + n^5$
2	$57 = 3 \cdot 19$
4	$1649 = 17 \cdot 97$
6	$23\,401 = 7 \cdot 3343$
8	$423\,393 = 3 \cdot 141\,131$
12	$244\,389\,457 = 13 \cdot 19 \cdot 463 \cdot 2137$
14	$6\,104\,053\,449 = 3^2 \cdot 13 \cdot 19 \cdot 2\,745\,863$
16	$152\,588\,939\,201 = 17^2 \cdot 4513 \cdot 116\,993$
18	$3\,814\,699\,155\,193 = 19 \cdot 3121 \cdot 64\,329\,907$
22	$2\,384\,185\,796\,169\,257 = 23 \cdot 4999 \cdot 20\,736\,197\,641$
24	59 604 644 783 353 249 (простое)
26	$1\,490\,116\,119\,396\,647\,001 = 3 \cdot 7 \cdot 17 \cdot 31 \cdot 1283 \cdot 104\,945\,433\,641$
28	$37\,252\,902\,984\,636\,350\,993 = 29 \cdot 1303 \cdot 985\,865\,588\,287\,939$

Используя онлайн-калькулятор [27], удаётся провести вычисления вплоть до $n \leqslant 90$. Часть вычислений мы внесли в таблицу 2.

Значения $n = 12$ и $n = 14$ дают составные числа, которые делятся на 13, что согласуется с решением задачи 5.

Пара $a = 5$, $n = 24$ даёт 17-значное простое число

$$5^{24} + 24^5 = 59\,604\,644\,783\,353\,249.$$

Отметим, что определить простоту 17-значного числа в начале XX века было не просто, а во времена Ферма и Эйлера практически невозможно. Напомним, что Ферма думал, что число

$$F_5 = 2^{2^5} + 1 = 4\,294\,967\,297$$

— простое[1)]. Эйлер опроверг это утверждение в 1732 году, найдя разложение на простые сомножители

$$2^{2^5} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417.$$

Но развитие вычислительных машин и методов позволяет сейчас это сделать в течение нескольких минут.

Существуют ли в последовательности $\{5^n + n^5\}$ простые числа при $n > 90$?

Приоткроем карты: нам известно ещё одно простое число в этой последовательности — это $5^{1036} + 1036^5$. В этом числе 725 десятичных знаков.

Подождём с комментариями, а сейчас самое время рассмотреть другие значения a.

§ 4. Случай $2^n + n^2$

Следующую задачу можно найти в задачнике «Кванта» [11] и в более поздних изданиях, например в книге [1].

Задача 9 (С. Майзус, [11, М663]). Найдите все простые числа p, для которых число $2^p + p^2$ тоже простое.

Отметим, что в условии задачи 8 число x было целым (как мы выяснили, даже натуральным), а в условии задачи 9 появляется ограничение простотой показателя. Зачем же автор задачи ввёл такое ограничение?

При $p = 2$ получаем составное число 8. При $p = 3$ — простое число 17. Остаётся рассмотреть случай $p > 3$. Докажем более сильное утверждение, из которого будет следовать ответ к задаче 9.

[1)] Числа вида $F_n = 2^{2^n} + 1$, где $n \geqslant 0$, называются числами Ферма.

Задача 10. Если натуральное число $n > 3$ не делится на 3, то число $2^n + n^2$ — составное.

Решение. Если n — чётное число, то сумма $2^n + n^2$ делится на 4 и, следовательно, является составным числом.

Пусть теперь n — нечётное число и НОД$(3, n) = 1$. Применим приём, который мы использовали при решении задачи 1:

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

Слагаемое $2^n + 1 = (2 + 1)(2^{n-1} - 2^{n-2} + \ldots + 1)$ делится на 3. Поскольку n не делится на 3, получаем, что $n^2 - 1 = (n+1)(n-1)$ делится на 3. Поскольку оба слагаемых делятся на 3, их сумма делится на 3. Значит, число $2^n + n^2$ — составное. □

Упражнение 4. При каких натуральных n сумма $2^n + n^2$ делится на а) 5; б) 11?

Упражнение 5. а) Докажите, что сумма $2^n + n^2$ не делится на 7 ни для какого натурального n.

б) Докажите, что существует бесконечно много простых чисел p таких, что сумма $2^n + n^2$ не делится на p ни для какого натурального n.

(*Указание*. Примените теорему Дирихле о простых числах в арифметических прогрессиях.)

Сравните с условием упражнения 3.

Резюмируем сказанное. Если число p простое, то число $2^p + p^2$ простое только при $p = 3$. Если n — чётное число или НОД$(3, n) = 1$, то сумма $2^n + n^2$ является составным числом.

Для удобства введём обозначение $\delta_n = 2^n + n^2$. Итак, если мы хотим в последовательности $\{\delta_n\} = \{2^n + n^2\}$ найти ещё простые числа, то мы должны рассмотреть случай $n = 3(2k + 1) = 6k + 3$, где $k \in \mathbb{N}$.

Уже при $k = 1$ мы находим, что $\delta_9 = 2^9 + 9^2 = 593$ — простое число.

Используя онлайн-калькулятор, удаётся провести вычисления для $1 \leqslant k \leqslant 42$. Частичные результаты вычислений для $1 \leqslant k \leqslant 24$ приведены в таблице 3. Мы находим простые числа при $k = 2$, $k = 3$, $k = 5$, т. е. при $n = 15$, $n = 21$, $n = 33$ соответственно.

Полученные результаты удобно занести в таблицу 3.

Существуют ли среди чисел вида $2^n + n^2$ простые при $n > 255$?

Чтобы ответить на этот вопрос, нам пришлось отказаться от онлайн-калькулятора.

Студент 2 курса университета Тель-Авива Джонатан Хашпер (Jonathan Khashper) написал небольшую программу и провёл вычисления на домашнем компьютере. Он нашёл три следующих простых числа.

Таблица 3

k	n	$2^n + n^2 = 2^{3(2k+1)} + (3(2k+1))^2$
1	9	593 (простое)
2	15	32 993 (простое)
3	21	2 097 593 (простое)
4	27	$134\,218\,457 = 73 \cdot 521 \cdot 3529$
5	33	8 589 935 681 (простое)
6	39	$549\,755\,815\,409 = 17 \cdot 43 \cdot 752\,059\,939$
7	45	$35\,184\,372\,090\,857 = 11 \cdot 17 \cdot 5689 \cdot 33\,072\,899$
8	51	$2\,251\,799\,813\,687\,849 = 83 \cdot 1979 \cdot 79\,691 \cdot 172\,027$
9	57	$144\,115\,188\,075\,859\,121 = 11 \cdot 137 \cdot 179 \cdot 221\,587 \cdot 2\,411\,011$
10	63	$9\,223\,372\,036\,854\,779\,777 = 17 \cdot 41 \cdot 13\,232\,958\,445\,989\,641$
11	69	$590\,295\,810\,358\,705\,656\,473 = 857 \cdot 688\,793\,244\,292\,538\,689$
12	75	$37\,778\,931\,862\,957\,161\,715\,193 = 71\,329 \cdot 11\,594\,347 \cdot 45\,681\,172\,811$
13	81	$2\,417\,851\,639\,229\,258\,349\,418\,913 = 59 \cdot 67 \cdot 307 \cdot 604\,681\,729 \cdot 3\,294\,864\,907$
14	87	$154\,742\,504\,910\,672\,534\,362\,398\,097 = 19 \cdot 151\,163 \cdot 53\,877\,882\,575\,230\,758\,001$
15	93	$9\,903\,520\,314\,283\,042\,199\,193\,002\,441 = 11 \cdot 3067 \cdot 293\,550\,710\,326\,438\,100\,577\,793$
16	99	$633\,825\,300\,114\,114\,700\,748\,351\,612\,489 = 17 \cdot 1049 \cdot 35\,542\,269\,955\,370\,083\,594\,928\,033$
17	105	$40\,564\,819\,207\,303\,340\,847\,894\,502\,583\,057 = 4\,561\,633 \cdot 8\,892\,609\,117\,678\,546\,443\,322\,929$
18	111	$2\,596\,148\,429\,267\,413\,814\,265\,248\,164\,622\,369 = 2\,940\,725\,100\,673 \cdot 882\,825\,949\,516\,080\,897\,953$
19	117	$166\,153\,499\,473\,114\,484\,112\,975\,882\,535\,056\,761 = 193 \cdot 860\,898\,961\,000\,593\,181\,932\,517\,526\,088\,377$
20	123	$10\,633\,823\,966\,279\,326\,983\,230\,456\,482\,242\,771\,737 = 1867 \cdot 5\,695\,674\,325\,805\,745\,572\,164\,143\,804\,093\,611$

При $n = 2007$ это $\delta_{2007} = 2^{2007} + 2007^2$ из 605 цифр! Не станем приводить здесь десятичную запись этого числа.

При $n = 2127$ это простое число $\delta_{2127} = 2^{2127} + 2127^2$ из 642 цифр!

При $n = 3759$ это простое число $\delta_{3759} = 2^{3759} + 3759^2$ из 1133 цифр!

В этом месте мы должны перевести дыхание.

Посмотрим на сайте [28] последовательность под номером A061119, т. е. последовательность простых чисел, представимых в виде $2^n + n^2$. Мы видим, что 19 июля 2017 года Харви Дэйл (Harvey P. Dale) нашёл вышеуказанное 605-значное число. Таким образом, 10 апреля 2021 года мог бы быть поставлен новый рекорд: найдены простые числа вида $2^n + n^2$ из 642 и 1133 цифр! К сожалению, в другой последовательности под номером A064539 мы находим оба показателя 2127 и 3759, а также показатели 29 355, 34 653, 57 285, 99 069. Эти результаты были получены Хьюго Пфертнером 14 ноября 2019 года с использованием программы тестирования на простоту Primeform GW (PFGW).

Мы не можем утверждать, конечное или бесконечное количество простых чисел имеется в последовательности $\{\delta_n\} = \{2^n + n^2\}$. Однако отыскание таких многозначных чисел говорит в пользу того, что в этой последовательности будут ещё встречаться простые числа[2)]. Почему мы это предполагаем? Самое время обратиться к истории.

§ 5. Простые числа Мерсенна

Немного отойдём от нашей «красивой» последовательности $\{2^n+n^2\}$ и посмотрим на другую очень известную последовательность $\{2^n - 1\}$.

Упражнение 6. Если число n составное, то число $2^n - 1$ также составное.

Следовательно, если число $2^n - 1$ простое, то n также простое. Исходя из этого, в последовательности $\{2^n - 1\}$ рассматривается подпоследовательность $\{M_p\} = \{2^p - 1\}$ с простым показателем p. Числа $M_p = 2^p - 1$ называются числами Мерсенна в честь монаха Марена Мерсенна (Marin Mersenne). Он был членом монашеского ордена минимов и сыграл выдающуюся роль как организатор науки своего времени. Он вёл переписку с П. Ферма, Р. Декартом, Б. Паскалем, Х. Гюйгенсом, Дж. Валлисом и другими выдающимися учёными.

Не для каждого простого p число $M_p = 2^p - 1$ будет простым. Например при $p = 11$ получаем $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ — составное число.

[2)] Это неизвестно и для более простых выражений, например, $n^2 + 1$ (4-я задача Э. Ландау `https://en.wikipedia.org/wiki/Landau%27s_problems`).

Последовательность простых чисел Мерсенна начинается так (см. [28, A000 668]):

3, 7, 31, 127, 8191, 131 071, 524 287,

2 147 483 647, 2 305 843 009 213 693951, …

Показатели p простых чисел Мерсенна образуют последовательность (см. [28, A000043])

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, …

Не обязательно проверять все простые нечётные p, поскольку некоторые числа Мерсенна специального вида всегда являются составными, что вытекает, например, из следующей доказанной Эйлером теоремы:

Теорема 2 (Эйлер). *Пусть числа* $p = 4n + 3$ *и* $q = 2p + 1 = 8n + 7$ — *простые*[3)]. *Тогда* $M_p \equiv 0 \pmod{q}$.

Существует эффективный алгоритм проверки чисел Мерсенна на простоту — *критерий Люка* (тест Люка — Лемера). Поэтому простые числа Мерсенна вызывают особый интерес и давно удерживают лидерство как самые большие известные простые числа [29].

Критерий состоит в следующем.

Теорема 3 (критерий Люка или тест Люка — Лемера, [9, с. 96]). *Пусть* p — *простое нечётное. Число Мерсенна* $M_p = 2^p - 1$ *простое тогда и только тогда, когда оно делит нацело* $(p-1)$*-й член рекуррентной последовательности* (*см.* [28, A003010])

$$S_k = S_{k-1}^2 - 2, \quad S_1 = 4.$$

Начальные члены этой последовательности: $4, 14, 194, 37\,634, \ldots$

Этот критерий простоты был предложен французским математиком Люка в 1878 году. Чуть ранее (без использования компьютера!) Люка доказал простоту числа $M_{127} = 2^{127} - 1$ (см. [20]). В частности, Люка показал, что алгоритм позволяет проверять простоту M_p для простых $p \equiv 1 \pmod 4$. В 1930 году в своей докторской диссертации американский математик Лемер полностью доказал справедливость критерия для всех простых нечётных p.

В 1952 году Робинсон при поддержке Лемера провёл вычисления на компьютере SWAC с использованием теста Люка — Лемера, результатом которого стало открытие простых чисел M_{521} и M_{607}. Позднее в том же году были открыты M_{1279}, M_{2203} и M_{2281}.

[3)] Если числа p и $2p + 1$ одновременно являются простыми, то меньшее из них называется простым числом Софи Жермен.

Для проверки простоты M_p последовательность чисел $S_1, S_2, \ldots, S_{p-1}$ вычисляется по модулю числа M_p (т. е. вычисляются не сами числа S_k, длина которых растёт экспоненциально, а остатки от деления S_k на M_p, длина которых ограничена p битами). Последнее число в этой последовательности $S_{p-1} \pmod{M_p}$ называется вычетом Люка — Лемера. Таким образом, число Мерсенна M_p является простым тогда и только тогда, когда число p — нечётное простое и вычет Люка — Лемера равен нулю.

Лёгкость реализации теста и рост вычислительных мощностей компьютеров позволили фактически любому человеку заниматься поиском простых чисел Мерсенна. Так, в 1978 году два американских старшеклассника Лора Никель и Курт Нолл[4)] за 3 года работы доказали простоту числа M_{21701}, используя суперкомпьютер CDC Cyber 176 в Калифорнийском университете.

До настоящего времени остаётся открытым вопрос о существовании бесконечного количества простых чисел Мерсенна. Этому вопросу уже более 400 лет. Но, несмотря на это, с упорством и с верой, заложенной ещё монахом Мерсенном, большие простые числа ищутся среди простых чисел Мерсенна.

Самым большим известным простым числом является число Мерсенна, проверенное с помощью теста Люка — Лемера,

$$M_{82589933} = 2^{82589933} - 1.$$

Это число было найдено 7 декабря 2018 года Патриком Ларошем в рамках проекта добровольных вычислений GIMPS. Десятичная запись числа $M_{82589933}$ содержит 24 862 048 цифр.

Всего в настоящее время известно 51 простое число Мерсенна, при этом порядковые номера достоверно установлены только у первых 47 чисел. Неизвестно, существуют ли другие простые числа Мерсенна, меньшие известного рекордного. В таблице 4 приведены простые числа Мерсенна, известные в настоящее время.

Завершим наш исторический экскурс и снова посмотрим на последовательность $\{2^n + n^2\}$.

В настоящее время мы не располагаем доказательством, однако склонны считать, что верна следующая гипотеза.

Гипотеза 1. *В последовательности* $\{\delta_n\} = \{2^n + n^2\}$ *встречается бесконечно много простых чисел.*

Косвенным подтверждением нашей гипотезы является нахождение простого числа $2^{3759} + 3759^2$ из 1133 цифр!

[4)] Лемер преподавал им теорию чисел.

Таблица 4

Открытие простых чисел Мерсенна

№	p — показатель	Знаков в M_p	Год	Первооткрыватель
1	2	1	—	—
2	3	1	—	—
3	5	2	—	—
4	7	3	—	—
5	13	4	1456	неизвестен
6	17	6	1588	Катальди (Cataldi)
7	19	6	1588	Катальди
8	31	10	1772	Эйлер
9	61	19	1883	Первушин
10	89	27	1911	Пауэрс (Powers)
11	107	33	1914	Пауэрс
12	127	39	1876	Люка (Lucas)
13	521	157	1952	Робинсон (Robinson)
14	607	183	1952	Робинсон
15	1279	386	1952	Робинсон
16	2203	664	1952	Робинсон
17	2281	687	1952	Робинсон
18	3217	969	1957	Ризель (Riesel)
19	4253	1281	1961	Гурвиц (Hurwitz)
20	4423	1332	1961	Гурвиц
21	9689	2917	1963	Гиллис (Gillies)
22	9941	2993	1963	Гиллис
23	11213	3376	1963	Гиллис
24	19937	6002	1971	Такерман (Tuckerman)
25	21701	6533	1978	Нолл (Noll), Никель (Nickel)
26	23209	6987	1979	Нолл
27	44497	13395	1979	Нельсон (Nelson), Словинский (Slowinski)
28	86243	25962	1982	Словинский
29	110503	33265	1988	Колквит (Colquitt), Уэлш (Welsh)
30	132049	39751	1983	Словинский
31	216091	65050	1985	Словинский
32	756839	227832	1992	Словинский, Гейдж (Gage) и др.
33	859433	258716	1994	Словинский, Гейдж
34	1 257 787	378 632	1996	Словинский, Гейдж

Окончание таблицы 4

№	p — показатель	Знаков в M_p	Год	Первооткрыватель
35	1 398 269	420 921	1996	Арменгауд (Armengaud), Вольтман (Woltman), и др.
36	2 976 221	895 932	1997	Спенс (Spence), Вольтман, и др. (GIMPS)
37	3 021 377	909 526	1998	Кларксон (Clarkson), Вольтман, Куровский (Kurowski) и др.
38	6 972 593	2 098 960	1999	Хаджратвала (Hajratwala), Вольтман, Куровский и др.
39	13 466 917	4 053 946	2001	Кемерон (Cameron), Вольтман, Куровский и др.
40	20 996 011	6 320 430	2003	Шефер (Shafer), Вольтман, Куровский и др.
41	24 036 583	7 235 733	2004	Финдли (Findley), Вольтман, Куровский и др.
42	25 964 951	7 816 230	2005	Новак (Nowak), Вольтман, Куровский и др.
43	30 402 457	9 152 052	2005	Купер (Cooper), Бун (Boone), Вольтман, Куровский и др.
44	32 582 657	9 808 358	2006	Купер, Бун, Вольтман, Куровский и др.
45	37 156 667	11 185 272	2008	Елвенич (Elvenich), Вольтман, Куровский и др.
46	42 643 801	12 837 064	2009	Стриндмо (Strindmo), Вольтман, Куровский и др.
47	43 112 609	12 978 189	2008	Смит (Smith), Вольтман, Куровский и др.
48?	57 885 161	17 425 170	2013	Купер, Вольтман, Куровский и др.
49?	74 207 281	22 338 618	2016	Купер, Вольтман, Куровский, Блоссер (Blosser) и др.
50?	77 232 917	23 249 425	2017	Пак (Pace), Вольтман, Куровский, Блоссер и др.
51?	82 589 933	24 862 048	2018	Лярош (Laroche), Вольтман, Блоссер и др.

Существенным продвижением в нахождении простых чисел в последовательности $\{2^n + n^2\}$ было бы нахождение критерия, аналогичного критерию Люка, для последовательности простых чисел Мерсенна.

§ 6. Простые числа Каллена

Последовательность $\{n2^n + 1\}$ называется последовательностью Каллена[5)] (см. [28, A002064]). Предполагалось, что все числа в этой последовательности при $n > 1$ будут составными, пока Робинсон не показал, что при $n = 141$ мы получим простое число.

[5)] Названа в честь ирландского священника-иезуита Джеймса Каллена (James Cullen), который проверил, что для $1 < n \leqslant 100$ её члены являются составными числами.

В монографии Кристофера Хооли [22] анонсирован результат, опирающийся на «методы решета». Название эти методы получили от известного метода решета Эратосфена.

Приведём упомянутый результат без доказательства.

Теорема 4 (К. Хооли, [22]). *Пусть $k(x)$ есть количество положительных целых n, не превосходящих x, для которых $n2^n + 1$ является простым числом. Тогда при $x \to +\infty$*

$$k(x) = o(x). \tag{1}$$

Это означает, что если простые числа встречаются в последовательности Каллена, то встречаются они очень редко.

Процитируем ремарку Хооли: «Подобные методы применимы к другим последовательностям, таким, например, как $\{2^n + n^2\}$. Следовательно, можно заключить, что методы решета могут сделать скромный вклад в наши знания об очень редко распределённых последовательностях, хотя, по-видимому, они не приведут при этом к решению наиболее интересных проблем».

Подобную же ремарку со ссылкой на Хооли мы можем найти в [3, с. 255].

К сожалению, в своей монографии Хооли не привёл доказательство этого утверждения для последовательности $\{2^n + n^2\}$. Нам не удалось найти полного доказательства этого утверждения (которое использовало бы методы решета или иные методы) в других доступных нам источниках.

Поэтому сформулируем это утверждение в виде гипотезы.

Гипотеза 2 (К. Хооли). *Пусть $f(x)$ есть количество положительных целых n, не превосходящих x, для которых $2^n + n^2$ является простым числом. Тогда при $x \to +\infty$*

$$f(x) = o(x). \tag{2}$$

Итак, мы имеем ещё одно косвенное подтверждение гипотезы 1. С важным дополнением: простые числа в этой последовательности встречаются крайне редко.

§ 7. Случай $3^n + n^3$

Рассмотрим случай $a = 3$.

Если n нечётно, то сумма $3^n + n^3$ делится на 2. Если n делится на 3, то сумма $3^n + n^3$ делится на 3.

Таблица 5

n	$3^n + n^3$
2	17 (простое)
4	$145 = 5 \cdot 29$
8	$7073 = 11 \cdot 643$
10	$60\,049 = 11 \cdot 53 \cdot 103$
14	$4\,785\,713 = 677 \cdot 7069$
16	$43\,050\,817 = 17 \cdot 2\,532\,401$
20	$3\,486\,792\,401 = 83 \cdot 461 \cdot 91\,127$
22	$31\,381\,070\,257 = 23 \cdot 1\,364\,394\,359$
26	$2\,541\,865\,845\,905 = 5 \cdot 1709 \cdot 297\,468\,209$
28	$22\,876\,792\,476\,913 = 29 \cdot 10\,193 \cdot 77\,391\,829$
32	$1\,853\,020\,188\,884\,609 = 1049 \cdot 1\,766\,463\,478\,441$
34	$16\,677\,181\,699\,705\,873 = 23 \cdot 725\,094\,856\,508\,951$
38	$1\,350\,851\,717\,673\,046\,961 = 307 \cdot 10\,061 \cdot 437\,349\,017\,143$
40	$12\,157\,665\,459\,056\,992\,801 = 41 \cdot 8\,987\,921 \cdot 32\,991\,881\,641$
44	$984\,770\,902\,183\,611\,318\,065 = 5 \cdot 71 \cdot 1\,221\,907 \cdot 2\,270\,223\,954\,329$
46	$8\,862\,938\,119\,652\,501\,193\,265 = 5 \cdot 11 \cdot 47 \cdot 3\,428\,602\,754\,217\,602\,009$
50	$717\,897\,987\,691\,852\,588\,895\,249 = 41 \cdot 17\,509\,707\,016\,874\,453\,387\,689$
52	$6\,461\,081\,889\,226\,673\,299\,072\,849 = 53 \cdot 121\,907\,205\,457\,107\,043\,378\,733$
56	523 347 633 027 360 537 213 687 137 (простое)
58	$4\,710\,128\,697\,246\,244\,834\,921\,798\,801 = 59 \cdot 177\,949\,463 \cdot 295\,176\,373 \cdot 1\,519\,856\,161$

Поэтому в онлайн-калькуляторе проведём вычисления для чётных n, не делящихся на 3, т. е. вида $n = 2(3k \pm 1)$, где $k \in \mathbb{N}$. Данные внесём в таблицу 5.

Кроме уже упоминавшегося числа 17 мы находим ещё одну пару $a = 3$, $n = 56$.

Число $3^{56} + 56^3$ является простым!

К сожалению, вычисления Джонатана Хашпера на домашнем компьютере не дали новых простых чисел при $a = 3$.

§ 8. Числа Лейланда. Случай $7^n + n^7$

В случае $a = 7$ проведём аналогичные рассуждения.

Если n нечётное, то $7^n + n^7$ делится на 2. Если n делится на 7, то $7^n + n^7$ делится на 7. Поэтому вычисления проводим для чисел вида $n = 2(7k + r)$, где $r = 1, 2, 3, 4, 5, 6$.

Таблица 6

n	$7^n + n^7$
4	$18\,785 = 5 \cdot 13 \cdot 17^2$
6	$397\,585 = 5 \cdot 131 \cdot 607$
10	$292\,475\,249 = 11 \cdot 4397 \cdot 6047$
12	$13\,877\,119\,009 = 13 \cdot 1\,067\,470\,693$
16	$33\,233\,199\,005\,057 = 17 \cdot 1\,954\,894\,059\,121$
18	$1\,628\,414\,210\,130\,481 = 19 \cdot 85\,706\,011\,059\,499$
22	$3\,909\,821\,051\,077\,345\,937 = 13 \cdot 23 \cdot 47 \cdot 278\,219\,672\,032\,829$
24	$191\,581\,231\,385\,152\,885\,825 = 5^2 \cdot 341\,333 \cdot 22\,450\,947\,477\,701$
30	$22\,539\,340\,290\,692\,279\,957\,863\,249 = 31 \cdot 727\,075\,493\,248\,138\,063\,156\,879$
34	$54\,116\,956\,037\,952\,111\,721\,483\,010\,993 =$ $= 23^2 \cdot 31 \cdot 43 \cdot 13\,649 \cdot 5\,622\,723\,213\,426\,086\,701$
36	$2\,651\,730\,845\,859\,653\,471\,857\,387\,545\,697 =$ $= 37^2 \cdot 1\,936\,983\,817\,282\,434\,968\,486\,039\,113$
40	$6\,366\,805\,760\,909\,027\,985\,741\,598\,979\,224\,001 =$ $= 37 \cdot 41 \cdot 4\,196\,971\,496\,973\,650\,616\,836\,914\,290\,853$
46	$749\,048\,330\,965\,186\,233\,494\,494\,103\,130\,382\,150\,865 =$ $= 5 \cdot 11 \cdot 47 \cdot 107 \cdot 970\,090\,462\,791\,553 \cdot 2\,791\,600\,584\,558\,224\,939$
48	$36\,703\,368\,217\,294\,125\,441\,230\,211\,032\,620\,728\,531\,073 =$ $= 643 \cdot 3631 \cdot 15\,720\,584\,845\,159\,650\,136\,109\,872\,534\,726\,981$
52	$88\,124\,787\,089\,723\,195\,184\,393\,736\,687\,913\,846\,185\,013\,729 =$ $= 53 \cdot 110\,703\,724\,474\,073 \cdot 15\,019\,655\,750\,344\,554\,442\,695\,759\,941$
54	$4\,318\,114\,567\,396\,436\,564\,035\,293\,097\,707\,729\,426\,477\,458\,833$ (простое)
58	$10\,367\,793\,076\,318\,844\,190\,248\,738\,727\,596\,255\,140\,420\,933\,654\,001 =$ $= 59 \cdot 1\,310\,148\,050\,957 \cdot 44\,316\,771\,096\,751 \cdot 3\,026\,535\,857\,960\,488\,271\,777$

Если $n \equiv 2 \pmod 3$, то $7^n + n^7 \equiv 1^n + 2^7 \equiv 0 \pmod 3$. Значит, в этом случае сумма делится на 3 и является составным числом. Например, $7^2 + 2^7 = 177 = 3 \cdot 59$. Опять используем онлайн-калькулятор и внесём данные в таблицу 6.

Нам везёт (!), мы находим пару $a = 7$, $n = 54$.

Число $7^{54} + 54^7$, состоящее из 46 знаков, является простым!

Вычисления Джонатана Хашпера на домашнем компьютере позволили найти ещё одно простое число при $n = 3076$. А именно, $7^{3076} + 3076^7$ — простое число, состоящее из 2600 десятичных знаков.

Снова заглянем на сайт [28]. Последовательность под номером A094133 состоит из простых чисел, представимых в виде $a^n + n^a$. Члены этой последовательности называются простыми числами Лейланда (Leyland).

Поиски всё больших чисел Лейланда ведутся на суперкомпьютерах, и вряд ли домашний компьютер сможет составить им конкуренцию.

Мы собрали достаточно примеров, поэтому самое время вернуться к теории. В дальнейшем мы предполагаем, что наш читатель знаком с теорией сравнений. Основы теории сравнений можно найти в [7].

§ 9. Малая теорема Ферма как критерий простоты

Норвежский математик О. Оре в своей книге [18] в параграфе о простых числах Мерсенна пишет: «В течение нескольких столетий шла погоня за простыми числами. Многие математики боролись за честь стать открывателем самого большого из известных простых чисел. <…> Теперь эта погоня утихла, она идёт только в одном направлении, оказавшемся удачным».

Однако он ошибся, погоня за простыми числами не утихла и идёт по разным направлениям. Более того, для современной криптографии необходимы очень большие простые числа и их нужно много. Фактически нужно «массовое производство» больших простых чисел. В своё время сборник «Математическое просвещение» опубликовал ряд статей, связанных с криптографией, см. [6, 17, 24].

Сейчас разработано много алгоритмов и методов определения простоты больших чисел. Но простейшим критерием для определения простоты (хотя правильнее было бы сказать непростоты) служит следующая известная

Теорема 5 (малая теорема Ферма, [15, гл. 1, § 1.1, с. 23]). *Пусть a и n — произвольные взаимно простые числа. Тогда если n — простое число, то справедливо сравнение*

$$a^{n-1} \equiv 1 \pmod{n}, \tag{3}$$

т. е. $a^{n-1} - 1$ делится на n.

Итак, если у нас есть число n и мы найдём взаимно простое с ним число a, для которого условие (3) не будет выполнено, то мы можем утверждать, что число n составное.

К сожалению, выполнение условия (3) даже для всех взаимно простых с n чисел a не гарантирует его простоту.

Определение. Число n называется *псевдопростым по основанию a*, если выполнено сравнение (3).

В качестве примера рассмотрим составное число $91 = 7 \cdot 13$ и взаимно простое с ним число 3. Тогда выполнено сравнение

$$3^{90} \equiv (3^6)^{15} \equiv 729^{15} \equiv 1^{15} \equiv 1 \pmod{91}.$$

Это означает, что число 91 является псевдопростым по основанию 3.

Если же мы возьмём другое основание, например 2, то получим

$$2^{90} \equiv (2^{10})^9 \equiv 1024^9 \equiv 23^9 \equiv 12\,167^3 \equiv 64^3 \equiv 64 \pmod{91}.$$

Поскольку по основанию 2 условие (3) не выполнено, мы можем утверждать, что число 91 составное.

Собственно говоря, так действуют современные алгоритмы: берётся несколько оснований и проводится тест. Если хотя бы в одном случае сравнение не выполнено, то проверяемое число является составным.

Однако если сравнение выполнено для всех выбранных нами оснований, то мы не можем утверждать, что проверяемое нами число является простым.

Определение. *Числами Кармайкла* (Carmichael) называются составные числа, которые являются псевдопростыми для всех a, взаимно простых с n.

Такие числа есть: например, $561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, и их бесконечно много.

Теорема 6 (Корселт, [14, § 11.3, с. 272]). *Нечётное натуральное число n является числом Кармайкла, если и только если для каждого его простого делителя p выполнены следующие два условия*:

(1) p^2 *не делит* n;

(2) $p-1$ *делит* $n-1$.

Обобщением малой теоремы Ферма является следующая

Теорема 7 (Эйлер, [16, с. 85]). *Если n взаимно просто с*

$$m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},$$

где $p_1, \ldots, p_k$ — простые числа и

$$\varphi(m) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdot \ldots \cdot (p_k - 1)p_k^{\alpha_k - 1},$$

то

$$n^{\phi(m)} \equiv 1 \pmod{m}, \tag{4}$$

т. е. $n^{\phi(m)} - 1$ делится на m.

Здесь $\varphi(m)$ — *функция Эйлера*, равная количеству чисел от 1 до m, взаимно простых с m.

Доказательства малой теоремы Ферма и теоремы Эйлера можно найти в разных источниках, в том числе и адаптированных для школьников [8], [7]. Доказательство теоремы Корселта можно найти в [14].

Используя всё вышесказанное, получаем целый ряд примеров, когда сумма $a^n + n^a$ — составное число.

Первый пример. Пусть $p \geqslant 3$ — простое число. Поскольку p нечётно, для любого n имеем

$$(n-1)^p \equiv (-1)^p \equiv -1 \pmod{n}.$$

Если n простое и $(n, p) = 1$, из малой теоремы Ферма получаем $p^{n-1} \equiv 1 \pmod{n}$.

Следовательно, если числа $p \geqslant 3$ и n простые, $p \neq n$, то

$$(n-1)^p + p^{n-1} \equiv -1 + 1 \equiv 0 \pmod{n}.$$

Например, если взять $n = 11$ и простое число $p \neq 11$, то числа $3^{10} + 10^3$, $5^{10} + 10^5$, $7^{10} + 10^7$, …, $p^{10} + 10^p$ делятся на 11.

Как мы отметили, число $5^{10} + 10^5$ делится на 11, но этот пример не столь интересен, поскольку сразу видно, что это число составное и делится на 5^5. Поэтому в содержательных примерах числа p и $n-1$ должны быть взаимно просты.

Второй пример. Пусть n — число Кармайкла, $n = p_1 p_2 \dots p_k$. Пусть a — нечётное число, взаимно простое с n. Тогда $a^{n-1} \equiv 1 \pmod{n}$, следовательно,

$$a^{n-1} + (n-1)^a \equiv 1 + (-1)^a \equiv 0 \pmod{n}.$$

В частности, числа $13^{560} + 560^{13}$, $19^{560} + 560^{19}$, …, $p^{560} + 560^p$ делятся на 561 при $p \neq 3, 11, 17$. Числа $5^{560} + 560^5$, $7^{560} + 560^7$ также делятся на 561, хотя этот случай не так интересен, поскольку первое делится на 5^5, а второе на 7^7.

Третий пример. Пусть n — псевдопростое число по основанию a. Пусть a — нечётное число, взаимно простое с n.

Рассуждая аналогично предыдущему, получаем

$$a^{n-1} + (n-1)^a \equiv 1 - 1 \equiv 0 \pmod{n}.$$

В частности, числа $11^{90} + 90^{11}$, …, $p^{90} + 90^p$ делятся на 91 при $p \neq 7, 13$. Числа $3^{90} + 90^3$, $5^{90} + 90^5$ также делятся на 91, к тому же первое делится на 3^6, а второе на 5^5.

Итак, мы достаточно хорошо продвинулись в определении того, какие из сумм $a^n + n^a$ могут быть составными числами. Однако методов для нахождения пар с простой суммой не нашли.

§ 10. Символ Лежандра. Квадратичный закон взаимности

Необходимое условие простоты, которое применял Гаусс, основано на свойстве цикличности мультипликативной группы $(\mathbb{Z}/n\mathbb{Z})^\times$ для простых чисел n. Для нечётного простого n извлечём квадратный корень

из левой и правой частей сравнения (3). Мы получим $a^{(n-1)/2} \equiv 1 \pmod{n}$ или $a^{(n-1)/2} \equiv -1 \pmod{n}$ в зависимости от того, является ли a квадратом по модулю n или нет. Эти два сравнения можно записать одной строчкой

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}, \tag{5}$$

где $\left(\frac{a}{n}\right)$ обозначает символ Лежандра.

Пусть a — целое число и p — простое число. *Символ Лежандра* $\left(\frac{a}{p}\right)$ определяется следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \text{ делится на } p; \\ 1, & \text{если } a \text{ является квадратичным вычетом,} \\ & \text{по модулю } p, \text{ т. е. существует такое } x \in \mathbb{Z}, \\ & \text{что } x^2 \equiv a \pmod{p}; \\ -1 & \text{в противном случае.} \end{cases} \tag{6}$$

Часто сравнение 5 называют *критерием Эйлера*.

Чтобы быстро вычислять символ Лежандра, нам понадобится

Теорема 8 (квадратичный закон взаимности, [15, гл. 1, § 1.1, с. 29–30]). *Пусть p и q — различные нечётные простые числа, тогда*:

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2} \cdot \left(\frac{p}{q}\right). \tag{7}$$

Нам также будут нужны два дополнения к квадратичному закону взаимности:

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}, \tag{8}$$

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}. \tag{9}$$

Если мы не знаем, простое число n или составное, то вместо символа Лежандра используется *символ Якоби* $\left(\frac{a}{p}\right)$, который определён для нечётного положительного числа n и любого целого числа a.

Доказательство квадратичного закона взаимности можно найти в [19] или [15].

Быстрое вычисление символа Лежандра является стандартным упражнением для студентов, изучающих курс теории чисел. В следующем параграфе мы проведём несколько таких вычислений.

§ 11. Тест Люка

Предыдущие тесты могли установить только разложимость того или иного числа. Следующий тест помогает определить его простоту.

Теорема 9 (тест Люка, [14, § 11.1, с. 265]). *Пусть n — нечётное натуральное число и b — натуральное число такое, что $2 \leqslant b \leqslant n-1$. Если для каждого простого делителя p числа $n-1$ справедливы следующие утверждения*: (1) $b^{n-1} \equiv 1 \pmod{n}$; (2) $b^{(n-1)/p} \not\equiv 1 \pmod{n}$, *то n — простое число*.

Заметим, что для успешного применения теста Люка нам нужно знать полное разложение числа $n-1$ на множители. Кроме того, нам должно повезти с выбором b, в противном случае тест может не дать ответ, даже если число простое.

Например, докажем, что число $m = 2^9 + 9^2 = 593$ — простое.

Найдём разложение числа $m-1=2^9+9^2-1=592$ на множители. Имеем $2^9 + 9^2 - 1 = 2^4 \cdot 37$. Для проверки выберем $b = 2$. Чтобы применить тест Люка, мы должны найти вычеты $2^{m-1} = 2^{2^9+9^2-1}$, $2^{(m-1)/2} = 2^{2^3 \cdot 37}$ и $2^{(m-1)/37} = 2^{2^4}$ по модулю $m = 593$.

Постараемся сократить наши вычисления. Сначала найдём вычет для $2^{(m-1)/37} = 2^{2^4}$. Имеем

$$2^{2^4} = 2^{16} = (2^8)^2 = 256^2 \equiv 306 \pmod{593}.$$

Теперь найдём вычет $2^{(m-1)/2^4} = 2^{37}$. Имеем

$$2^{37} = 2^{2^4 \cdot 2+5} = 2^5 \cdot (2^{2^4})^2 \equiv 32 \cdot 306^2 \equiv 516 \pmod{593}.$$

Отсюда

$$2^{(m-1)/2} = 2^{2^3 \cdot 37} = (2^{37})^8 \equiv (516^2)^4 \equiv (592^2)^2 \equiv 1 \pmod{593}.$$

Это означает, что кандидат $b = 2$ не подходит.

Придётся взять $b=3$ и искать вычеты $3^{m-1}=3^{2^9+9^2-1}$, $3^{(m-1)/2}=3^{2^3 \cdot 37}$ и $3^{(m-1)/37} = 3^{2^4}$ по модулю $m = 593$. Поступим аналогично предыдущему: сначала найдём вычет $3^{(m-1)/37} = 3^{2^4}$. Имеем

$$3^{2^4} = 3^{16} = (3^4)^4 = (81^2)^2 \equiv 38^2 \equiv 258 \pmod{593}.$$

Далее,

$$3^{37} = 3^{2^4 \cdot 2+5} = 3^5 \cdot (3^{2^4})^2 \equiv 243 \cdot 258^2 \equiv 384 \pmod{593}.$$

Отсюда

$$3^{(m-1)/2} = 3^{2^3 \cdot 37} = (3^{37})^8 \equiv (384^2)^4 \equiv (392^2)^2 \equiv 77^2 \equiv 592 \equiv -1 \pmod{593}.$$

Наконец,

$$3^{m-1} = 3^{2^9+9^2-1} \equiv (-1)^2 \equiv 1 \pmod{593}.$$

Итак, получаем

$$3^{m-1} \equiv 1 \pmod{m},$$
$$3^{(m-1)/2} \not\equiv 1 \pmod{m},$$
$$3^{(m-1)/37} \not\equiv 1 \pmod{m}.$$

Согласно тесту Люка число $m = 2^9 + 9^2 = 593$ — простое.

Можно проверить, что тест также сработает, если в качестве кандидата взять $b = 5$ или $b = 7$.

Упражнение 7. Докажите с помощью теста Люка, что число $2^{15} + 15^2 = 32993$ простое.

Тест Люка легко запрограммировать. Быстрое возведение в степень производится с помощью умножения и возведения в квадрат.

С помощью теста Люка можно обосновать следующий тест на простоту для чисел Ферма. Впервые его предложил Жан Франсуа Теофил Пепэн (Jean François Theophile Pepin).

Теорема 10 (тест Пепэна, [14, § 11.1, с. 266]). *Число Ферма F_k является простым при данном $k > 1$, если и только если*

$$5^{(F_k-1)/2} \equiv -1 \pmod{F_k}. \tag{10}$$

Доказательство. Докажем достаточность. Предположим, что сравнение (10) выполнено. Применим тест Люка. В качестве кандидата берём $b = 5$. Очевидно, что единственным простым делителем числа $F_k - 1 = 2^{2^k}$ является 2. Имеем

$$5^{(F_k-1)/2} \equiv -1 \not\equiv 1 \pmod{F_k}$$

и

$$5^{F_k-1} \equiv (-1)^2 \equiv 1 \pmod{F_k}.$$

Условия теста Люка выполнены, следовательно, F_k — простое число.

Докажем необходимость. Пусть F_k — простое число. Тогда по критерию Эйлера (5) имеем

$$5^{(F_k-1)/2} \equiv \left(\frac{5}{F_k}\right) \pmod{F_k}.$$

Найдём символ Лежандра $\left(\frac{5}{F_k}\right)$, для этого используем квадратичный закон взаимности. Имеем для $k \geqslant 2$:

$$\left(\frac{5}{F_k}\right) = (-1)^{(5-1)/2 \cdot (F_k-1)/2} \cdot \left(\frac{F_k}{5}\right) =$$
$$= \left(\frac{2^{2^k}+1}{5}\right) = \left(\frac{4^{2^{k-1}}+1}{5}\right) = \left(\frac{(-1)^{2^{k-1}}+1}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Итак, если F_k — простое число, то

$$5^{(F_k-1)/2} \equiv -1 \pmod{F_k}.$$

Что и требовалось доказать. □

При проверке на простоту числа $2^9 + 9^2 = 593$ с помощью теста Люка мы увидели, что при выборе кандидата $b = 2$ мы получаем неопределённый результат. Если читатель решал упражнение (7), то он мог также убедиться, что и при проверке числа $2^{15} + 15^2 = 32\,993$ кандидат $b = 2$ снова даст неопределённый результат. Это не случайно.

Предложение 1. *Если число $\delta_n = 2^n + n^2$ является простым, то*

$$\text{а)}\ 2^{(\delta_n-1)/2} \equiv 1 \pmod{\delta_n}; \tag{11}$$

$$\text{б)}\ 3^{(\delta_n-1)/2} \equiv -1 \pmod{\delta_n}. \tag{12}$$

Доказательство. Так как δ_n — простое, получаем, что $n = 6k + 3$, где $k \in \mathbb{Z}\ k \geqslant 0$.

а) Используем критерий Эйлера. Далее найдём символ Лежандра по формуле (8).

$$2^{(\delta_n-1)/2} \equiv \left(\frac{2}{\delta_n}\right) = (-1)^{((2^n+n^2)^2-1)/8} = 1 \pmod{\delta_n}.$$

б) Используем критерий Эйлера и квадратичный закон взаимности. Имеем

$$3^{(\delta_n-1)/2} \equiv \left(\frac{3}{\delta_n}\right) = (-1)^{(3-1)/2\,\cdot\,(2^n+n^2-1)/2} \cdot \left(\frac{\delta_n}{3}\right) =$$

$$= \left(\frac{2^n+n^2}{3}\right) = \left(\frac{(-1)^n}{3}\right) = \left(\frac{(-1)}{3}\right) = -1 \pmod{\delta_n}.$$

Что и требовалось доказать. □

Итак, мы показали, что при проверке простоты чисел $2^n + n^2$ тестом Люка кандидат $b = 2$ даёт неопределённый ответ.

§ 12. Критерий определения простоты $2^n + n^2$

На основании теста Люка с учётом предложения 1 можно предложить

Критерий определения простоты $2^n + n^2$ для нечётных $n > 3$.

Шаг 1. В качестве кандидатов выбираем небольшие простые b, например $b = 3, 5, 7$; достаточно взять $b \leqslant 100$.

Проверяем, выполняются ли сравнения

$$3^{2^n+n^2-1} \equiv 1 \pmod{2^n+n^2},$$
$$5^{2^n+n^2-1} \equiv 1 \pmod{2^n+n^2},$$
$$7^{2^n+n^2-1} \equiv 1 \pmod{2^n+n^2},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Если хотя бы одно из сравнений не выполнено, то число $2^n + n^2$ составное. (Это следует из малой теоремы Ферма.)

Шаг 2. Теперь мы должны разложить число 2^n+n^2-1 на множители. Это число при нечётных $n > 3$ делится на 8. Поэтому мы применим усечённый тест Люка — только для одного простого делителя, равного 2.

Проверим, выполняется ли сравнение

$$b^{(2^n+n^2-1)/4} \not\equiv \pm 1 \pmod{2^n+n^2}. \qquad (*)$$

Если сравнение не выполняется, то с большой вероятностью число $2^n + n^2$ — простое.

Вообще говоря, по критерию Люка мы должны были бы проверить сравнение

$$b^{(2^n+n^2-1)/2} \not\equiv 1 \pmod{2^n+n^2}. \qquad (**)$$

Но мы применили небольшую хитрость. Поскольку

$$b^{(2^n+n^2-1)/2} - 1 = (b^{(2^n+n^2-1)/4} - 1)(b^{(2^n+n^2-1)/4} + 1),$$

мы можем проверять сравнение $(*)$, у которого меньший показатель, вместо проверки сравнения $(**)$.

§ 13. Случай $a = p - 1$

Остался нерассмотренным случай суммы $a^n + n^a$ при условии, что числа a и $n + 1$ не являются взаимно простыми.

Пусть $p \geqslant 3$ — простое число. Рассмотрим пару $a = p - 1$ и $n = p$.

Можем ли мы что-то сказать о делителях числа $(p-1)^p + p^{p-1}$? Условие взаимной простоты чисел $p - 1$ и $p + 1$ не выполнено — оба числа чётны. Поэтому применить малую теорему Ферма так, как мы это делали раньше, не удаётся. Сумма $(p-1)^p + p^{p-1}$ не делится ни на $p-1$, ни на p.

Вообще говоря, нам следует рассматривать общий случай суммы $(lp-1)^p + p^{lp-1}$, где l — нечётное число, но остановимся на вышеуказанном частном случае.

Таблица 7

p	$(p-1)^p + p^{p-1}$
3	17 (простое)
5	$1649 = 17 \cdot 97$
7	$397585 = 5 \cdot 131 \cdot 607$
11	$125937424601 = 2531 \cdot 49757971$
13	$130291290501553 = 19 \cdot 6857436342187$
17	$34380909705501969 4337 = 573645313 \cdot 599340898049$
19	$812362695653248917890473 = 22156214713 \cdot 36665229425521$
23	$841925973678882643813296848 0177 = 103 \cdot 5419 \cdot 214765247 \cdot 70234990225477963$
29	$10166155490042397076886511571194164153939 69 = $ $= 11 \cdot 127 \cdot 200467 \cdot 690280837 \cdot 525886029388902397702216 3$
31	$67273524831853808373745368719051391856788624 01 = $ $= 137 \cdot 1608214821278413 \cdot 3053370855763752465383299222 1$
37	$41152188389775187691338562104937229569738102643876425739 37 = $ $= 6301 \cdot 26713 \cdot 48040093 \cdot 60035377 \cdot 84771469107423924796379485711078 09$
41	$51603075786128366985108989368203283551185095927223539010549116960 1 = $ $859 \cdot 24103 \cdot 108684413 \cdot 22932112290137934777954016132484434869492384775260 1$
43	$67088429435775785394473014655222228597785743578175424102581741354885 37 = $ $= 1300283 \times$ $\times 51595252291828613766751556895862076638536182952615256911442925 39$
47	(составное, делится на 5)
53	(составное, делится на 17)
59	(составное, делится на 1039)
61	?
67	(составное, делится на 5)

Призовём на помощь онлайн-калькулятор. Число $(p-1)^p + p^{p-1}$ удаётся разложить на множители для всех простых $p \leqslant 59$ (см. таблицу 7). Поскольку при $p \geqslant 47$ сумма $(p-1)^p + p^{p-1}$ содержит более 70 значащих цифр, в таблице мы указали только наименьший делитель.

В этом случае с помощью онлайн-калькулятора нам не удалось найти новые примеры простых чисел, за исключением 17.

Означает ли этот факт, что число $(p-1)^p + p^{p-1}$ при $p \geqslant 5$ всегда составное, нам неизвестно.

С другой стороны, в качестве упражнений мы предлагаем новые примеры, когда достоверно известно, что сумма является составным числом.

Упражнение 8. Если $p \equiv 7 \pmod{20}$, то $(p-1)^p + p^{p-1} \equiv 0 \pmod 5$. В частности, суммы $46^{47} + 47^{46}$ и $66^{67} + 67^{66}$ делятся на 5.

Таблица 8

r	$(r-1)^r + r^{r-1}$
2	3
3	17
4	$145 = 5 \cdot 29$
5	$1649 = 17 \cdot 97$
6	$23\,401 = 7 \cdot 3343$
7	$397\,585 = 5 \cdot 131 \cdot 607$
8	$7\,861\,953 = 3 \cdot 11 \cdot 19 \cdot 12\,539$
9	$177\,264\,449 = 7523 \cdot 23\,563$
10	$4\,486\,784\,401 = 11 \cdot 407\,889\,491$
11	$125\,937\,424\,601 = 2531 \cdot 49\,757\,971$
12	$3\,881\,436\,747\,409 = 13 \cdot 3631 \cdot 82\,228\,603$
13	$130\,291\,290\,501\,553 = 19 \cdot 6\,857\,436\,342\,187$
14	$4\,731\,091\,158\,953\,433 = 3 \cdot 23 \cdot 61 \cdot 71 \cdot 125\,497 \cdot 126\,151$
15	$184\,761\,021\,583\,202\,849 = 23 \cdot 1571 \cdot 5\,113\,359\,576\,653$
16	$7\,721\,329\,860\,319\,737\,601 = 17 \cdot 1601 \cdot 12\,401 \cdot 22\,876\,793\,153$
17	$343\,809\,097\,055\,019\,694\,337 = 573\,645\,313 \cdot 599\,340\,898\,049$
18	$16\,248\,996\,011\,806\,421\,522\,977 = 19 \cdot 5779 \cdot 147\,985\,865\,445\,728\,377$
19	$812\,362\,695\,653\,248\,917\,890\,473 = 22\,156\,214\,713 \cdot 36\,665\,229\,425\,521$
20	$42\,832\,853\,457\,545\,958\,193\,355\,601 = 3 \cdot 127 \cdot 552\,634\,829 \cdot 203\,429\,428\,717\,049$
21	$2\,375\,370\,429\,446\,951\,548\,637\,196\,401 = 58\,967 \cdot 40\,283\,046\,949\,089\,347\,408\,503$
22	$138\,213\,776\,357\,206\,521\,921\,578\,463\,913 = 13 \cdot 23 \cdot 316\,031 \cdot 1\,462\,683\,827\,323\,261\,743\,877$
23	$8\,419\,259\,736\,788\,826\,438\,132\,968\,480\,177 = 103 \cdot 5419 \cdot 214\,765\,247 \cdot 70\,234\,990\,225\,477\,963$
24	$535\,823\,088\,031\,930\,481\,975\,544\,151\,644\,865 = 5 \cdot 24\,821 \cdot 48\,763\,734\,563 \cdot 88\,539\,116\,795\,595\,251$
25	$35\,562\,372\,323\,207\,319\,916\,133\,576\,686\,141\,249 = 41\,719 \cdot 852\,426\,288\,338\,822\,117\,407\,741\,716\,871$
26	$2\,457\,219\,879\,258\,280\,669\,724\,058\,501\,120\,110\,001 = 3 \cdot 7 \cdot 31 \cdot 3019 \cdot 92\,269 \cdot 514\,847 \cdot 1\,072\,817\,117 \cdot 24\,532\,410\,559$
27	$176\,482\,312\,353\,646\,748\,226\,944\,999\,299\,114\,553\,465 = 5 \cdot 7 \cdot 17 \cdot 113 \cdot 3929 \cdot 211\,229 \cdot 3\,162\,788\,888\,980\,701\,288\,689\,959$

Упражнение 9. Если $p \equiv 2 \pmod{17}$ и $p \equiv 5 \pmod 8$, то $(p-1)^p + p^{p-1} \equiv 0 \pmod{17}$. В частности, сумма $52^{53} + 53^{52}$ делится на 17.

Разложение на множители чисел $(r-1)^r + r^{r-1}$ для $r \leqslant 27$ представлено в таблице 8.

§ 14. Криптосистема с открытым ключом Диффи — Хэллмана

Разложение на простые множители и малая теорема Ферма играют важнейшую роль в современной криптографии, а именно при построении криптосистем с открытым ключом.

В настоящее время криптосистемы с открытым ключом получили широкое распространение. По всей видимости, первым был опубликован протокол обмена ключами Диффи — Хэллмана [2]. Алгоритм (протокол) Диффи — Хэллмана активно использует малую теорему Ферма. Дадим краткое описание этого протокола передачи важной информации, например, коммерческой тайны.

Шаг 1. Софья и Макс вместе выбирают простое число p и целое число a, которое имеет порядок $p-1$ по модулю p, т. е. для которого выполнено следующее условие:

$$a^{p-1} \equiv 1 \pmod{p},$$

при этом $a^k \not\equiv 1 \pmod{p}$ для любого положительного числа $k < p-1$.

Шаг 2. Софья выбирает случайное число $n < p$. Макс выбирает случайное число $m < p$.

Шаг 3. Софья отправляет Максу число, равное остатку от деления a^n на p, т. е. число $a^n \pmod{p}$. Макс отправляет Софье число, равное остатку от деления a^m на p, т. е. число $a^m \pmod{p}$.

Шаг 4. Софья вычисляет секретный ключ: $s = a^{nm} = (a^m)^n \pmod{p}$. Аналогично Макс вычисляет секретный ключ: $s = a^{nm} = (a^n)^m \pmod{p}$.

Шаг 5. Софья использует ключ s для шифрования и отправляет зашифрованное сообщение Максу. Макс расшифровывает сообщение с помощью ключа s.

Третьи лица могут знать оба числа $a^n \pmod{p}$ и $a^m \pmod{p}$, но они не смогут использовать их для достаточно быстрого получения n, m или $a^{nm} \pmod{p}$.

Трудности расшифровки связаны с проблемой определения дискретного логарифма.

§ 15. Алгоритм RSA

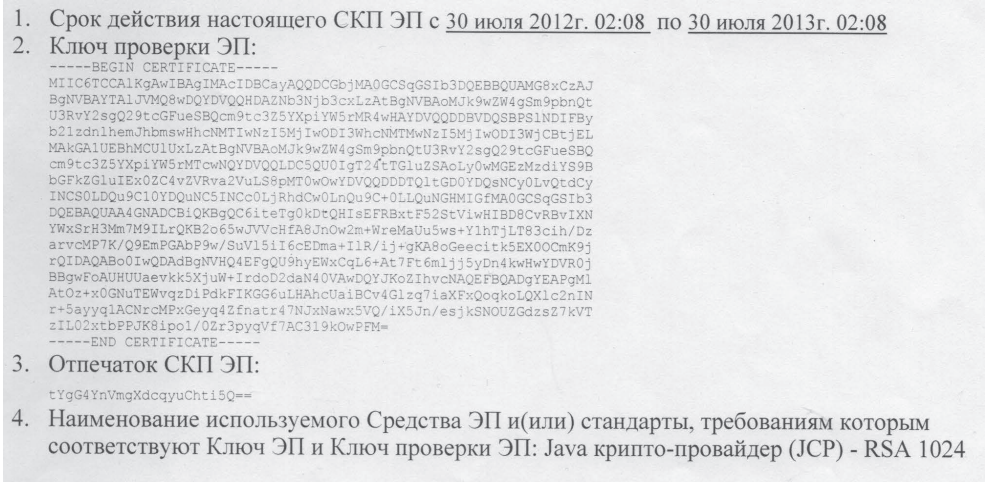
Алгоритм RSA является популярной «криптосистемой с открытым ключом», открытой Л. Адлеманом, Р. Ривестом и А. Шамиром [5].

Предположим, что существует некоторое количество пользователей U_1, U_2, U_3, … Время от времени некоторой паре пользователей необходимо обменяться сообщениями, которые должны оставаться

секретными для всех остальных пользователей. В классической криптосистеме эта пара должна сначала разделить между собой ключи и держать их в секрете. Система с открытым ключом обходит последнее ограничение: для секретного попарного общения достаточно использования лишь доступной всем информации.

Системы с открытым ключом названы так потому, что ключ, используемый при шифровании данных, не является секретным и может быть, например, опубликован в средствах массовой информации. Также несекретным является алгоритм шифрования. Защита данных обеспечивается тем, что для расшифрования необходим другой (секретный) ключ, причём он не может быть определён по открытому ключу зашифрования. Алгоритмы шифрования с открытым ключом называют поэтому несимметричными алгоритмами.

В настоящее время этот алгоритм широко используется в банковской сфере. Например, при открытии банковского счёта владельцу выдаётся сертификат ключа проверки электронной подписи (СКП ЭП). Фрагмент такого сертификата можно увидеть на рис. 2. В правом нижнем углу фрагмента можно увидеть название используемого алгоритма — RSA 1024.


1. Срок действия настоящего СКП ЭП с 30 июля 2012г. 02:08 по 30 июля 2013г. 02:08
2. Ключ проверки ЭП:

```
-----BEGIN CERTIFICATE-----
MIIC6TCCAlKgAwIBAgIMAcIDBCayAQQDCGbjMA0GCSqGSIb3DQEBBQUAMG8xCzAJ
BgNVBAYTAlJVMQ8wDQYDVQQHDAZNb3Njb3cxLzAtBgNVBAoMJk9wZW4gSm9pbnQt
U3RvY2sgQ29tcGFueSBQcm9tc3Z5YXpiYW5rMR4wHAYDVQQDDBVDQSBPSlNDIFBy
b21zdnlhemJhbmswHhcNMTIwNzI5MjIwODI3WhcNMTMwNzI5MjIwODI3WjCBtjEL
MAkGA1UEBhMCUlUxLzAtBgNVBAoMJk9wZW4gSm9pbnQtU3RvY2sgQ29tcGFueSBQ
cm9tc3Z5YXpiYW5rMTcwNQYDVQQLDC5QU0IgT24tTGluZSAoLy0wMGEzMzdiYS9B
bGFkZGluIEx0ZC4vZVRva2VuLS8pMT0wOwYDVQQDDDT0ltGD0YDQsNCy0LvQtdCy
INCS0LDQu9C10YDQuNC5INCc0LjRhdCw0LnQu9C+0LLQuNGHMIGfMA0GCSqGSIb3
DQEBAQUAA4GNADCBiQKBgQC6iteTg0kDtQHIsEFRBxtF52StViwHIBD8CvRBvIXN
YWxSrH3Mm7M9ILrQKB2o65wJVVcHfA8JnOw2m+WreMaUu5ws+Y1hTjLT83cih/Dz
arvcMP7K/Q9EmPGAbP9w/SuVl5iI6cEDma+Il1R/ij+gKA8oGeecitk5EXOOCmK9j
rQIDAQABo0IwQDAdBgNVHQ4EFgQU9hyEWxCqL6+At7Ft6mljj5yDn4kwHwYDVR0j
BBgwFoAUHUUaevkk5XjuW+IrdoD2daN40VAwDQYJKoZIhvcNAQEFBQADgYEAPgMl
AtOz+x0GNuTEWvqzDiPdkFIKGG6uLHAhcUaiBCv4Glzq7iaXFxQoqkoLQXlc2nIN
r+5ayyqlACNrcMPxGeyq4Zfnatr47NJxNawx5VQ/iX5Jn/esjkSNOUZGdzsZ7kVT
zIL02xtbPPJK8ipol/0Zr3pyqVf7AC319kOwPFM=
-----END CERTIFICATE-----
```

3. Отпечаток СКП ЭП:

```
tYgG4YnVmgXdcqyuChti5Q==
```

4. Наименование используемого Средства ЭП и(или) стандарты, требованиям которым соответствуют Ключ ЭП и Ключ проверки ЭП: Java крипто-провайдер (JCP) - RSA 1024

Рис. 2. Фрагмент Сертификата ключа проверки электронной подписи (СКП ЭП)

Согласно методу RSA для генерирования ключей необходимо выполнить следующие действия.

Шаг 1. Каждый пользователь U_i:

а) выбирает два больших простых числа p_i и q_i;

б) находит произведение этих чисел $n_i = p_i \cdot q_i$;

в) выбирает число d_i, взаимно простое с числом $\varphi(n_i)=(p_i-1)(q_i-1)$, где $\varphi(m)$ обозначает функцию Эйлера;

г) определяет число e_i, для которого выполняется условие $e_i d_i \equiv 1 \pmod{\phi(n_i)}$.

Числа d_i и e_i рассматриваются как остатки по модулю $n_i = p_i \cdot q_i$.

Шаг 2. Пары чисел (e_i, n_i) объявляются всем пользователям. Они называются открытым ключом.

Практически невозможно вычислить d_i, зная лишь (e_i, n_i). Так что числа d_i являются секретными данными.

Действительно, эффективный алгоритм нахождения d_i должен был бы также эффективно раскладывать на множители числа n_i, что по предположению является невыполнимо сложным.

Пусть нам известны числа d_i. Тогда $\varphi(n_i)$ делит $e_i d_i - 1$. Если бы мы знали сами числа $\varphi(n_i)$, то могли бы легко найти p_i и q_i, поскольку

$$p_i + q_i = n_i + 1 - \phi(n_i), \quad p_i - q_i = \sqrt{(p_i + q_i)^2 - 4n_i}.$$

Шаг 3. Зашифрованное сообщение представляется последовательностью битов. Предположим, что пользователю U_i необходимо передать это сообщение пользователю U_j. Сначала он разделяет последовательность битов на блоки длины $[\log_2 n_j]$. Затем он рассматривает каждый блок как некоторый остаток $m \pmod{n_j}$ и шифрует его как остаток $b = m^{e_j} \pmod{n_j}$. Таким образом, пара (n_j, e_j) служит шифрующим ключом j-го пользователя (напомним, что она известна всем пользователям).

Шаг 4. Получив зашифрованное сообщение, пользователь U_j дешифрует каждый блок $b \pmod{n_j}$, вычисляя остаток $b = m^{e_j} \pmod{n_j}$ (напомним, что ему известен дешифрующий ключ d_j). Результат легко проверить при помощи малой теоремы Ферма.

Детали этой схемы могут меняться. Например, аналогично можно построить процедуру аутентификации пользователя («электронная подпись») и т. п.

Пример. Рассмотрим алгоритм RSA, основанный на небольших числах p_i и q_i.

Предположим, что у нас есть два пользователя U_1, U_2 и шифрованию подлежит сообщение на русском языке. Буквы сообщения можно представить числами от 0 до 32.

Первый пользователь выбирает $p_1=3$, $q_1=11$ и находит $n_1=3\cdot11=33$.

Второй пользователь выбирает $p_2=5$, $q_2=7$ и находит $n_2=5\cdot7=35$.

Согласно описанному алгоритму:

в) первый пользователь в качестве числа d_1, взаимно простого с числом $(p_1-1)(q_1-1)=20$, выбирает число 3; второй пользователь в качестве числа d_2, взаимно простого с числом $(p_2-1)(q_2-1)=24$, выбирает число 5.

г) соотношению $e_1d_1=3e_1\equiv 1 \pmod{20}$ удовлетворяют числа $7, 27, 47, \ldots$, выберем $e_1=7$; соотношению $e_2d_2=5e_2\equiv 1 \pmod{24}$ удовлетворяют числа $5, 29, 53, \ldots$, выберем $e_2=5$.

Итак, открытыми ключами для шифрования являются пары чисел $e_1=7$, $n_1=33$ и $e_2=5$, $n_2=35$. Закрытыми (секретными) ключами — числа $d_1=3$ и $d_2=5$.

Зашифруем слово КВАНТ. Буквам К, В, А, Н и Т сопоставим числа 11, 03, 01, 14 и 19. Для простоты мы нумеруем буквы по порядку, считая Е и Ё одной буквой. Используя открытый ключ, получим криптограмму (Шаг 3), состоящую из чисел:

$C_1=11^5=161\,051 \pmod{35}\equiv 16 \pmod{35}$;
$C_2=3^5=243 \pmod{35}\equiv 33 \pmod{35}$;
$C_3=1^5=1 \pmod{35}\equiv 1 \pmod{35}$;
$C_4=14^5=537\,824 \pmod{35}\equiv 14 \pmod{35}$;
$C_5=19^5=2\,476\,099 \pmod{35}\equiv 24 \pmod{35}$.

Для расшифрования криптограммы $\{16, 33, 01, 14, 24\}$ второй пользователь использует формулу (Шаг 4) и секретный ключ $e_2=5$:

$M_1=16^5=1\,048\,576 \pmod{35}\equiv 11 \pmod{35}$;
$M_2=33^5=39\,135\,393 \pmod{35}\equiv 3 \pmod{35}$;
$M_3=1^5=1 \pmod{35}\equiv 1 \pmod{35}$;
$M_4=14^5=537\,824 \pmod{35}\equiv 14 \pmod{35}$;
$M_5=24^5=7\,962\,624 \pmod{35}\equiv 19 \pmod{35}$.

Как видим, в результате расшифрования получилось исходное сообщение КВАНТ.

Отметим, что на практике применяются настолько большие числа p_i и q_i, что, зная лишь e_i и n_i (открытый ключ), невозможно найти d_i за приемлемое время. Сейчас не только неизвестен достаточно эффективный (полиномиальный) алгоритм разложения большого числа на простые множители, но остаётся открытым и сам вопрос о существовании таких алгоритмов (а следовательно, о возможности взлома систем с открытым ключом в будущем).

Однако нельзя исключить открытие в дальнейшем эффективных алгоритмов определения делителей целых чисел (факторизации), вследствие чего метод шифрования с открытым ключом станет абсолютно

бесполезным. Пока этого не произошло, метод RSA имеет важные преимущества перед другими криптосистемами, такие как очень высокая криптостойкость и простота аппаратной и программной реализации.

§ 16. Краткие комментарии к вычислениям. Тест Бейли — Померанца — Селфриджа — Уогстаффа (BPSW)

Мы упоминали, что для разложения чисел на множители мы использовали онлайн-калькулятор [27].

Программа, написанная студентом Джонатаном Хашпером, подтвердила простоту чисел, найденных онлайн-калькулятором, и, как мы уже упоминали, нашла ещё пять простых чисел:

$$2^{2007}+2007^2,\quad 2^{2127}+2127^2,\quad 2^{3759}+3759^2,\quad 5^{1036}+1036^5,\quad 7^{3076}+3076^7 \tag{!}$$

Для своей программы Дж. Хашпер использовал тест на простоту Бейли — Померанца — Селфриджа — Уогстаффа. Это алгоритм вероятностной проверки на простоту. Он назван по фамилиям своих создателей — Роберта Бэйли, Карла Померанца, Джона Селфриджа, Сэмюэля Вагстаффа. Более подробно об этом тесте можно прочитать в [4, 26].

Погнавшись за обманчивой простотой школьной задачи, мы шаг за шагом дошли до серьёзных теорем, тестов на простоту и алгоритмов шифрования. С помощью компьютера мы нашли интересные простые числа и придумали аналог теста Люка для них. Появилась гипотеза о бесконечности количества простых чисел вида 2^n+n^2. Мы получили больше вопросов, чем ответов. Но мы надеемся, что часть вопросов будет решена уже в обозримом будущем.

§ 17. Ответы, указания, решения

Решение задач

1. 2) Квадрат числа, не кратного трём, даёт остаток 1 при делении на 3. Следовательно, каждое слагаемое даёт остаток 1, а их сумма делится на 3.

3) Выражение $2^{2145}+3^{2145}=(2^{15})^{143}+(3^{15})^{143}$ делится на $2^{15}+3^{15}$. Далее,

$$2^{15}+3^{15}=(2^5+3^5)(2^{10}-2^5\cdot 3^5+3^{10})=275\cdot 52\,297=25\cdot 11\cdot 7\cdot 31\cdot 241.$$

Отсюда следует делимость на 11, 241 и $341=11\cdot 31$.

2. 1) Имеем

$$2222^{5555} + 5555^{2222} = \\ = (2222^{5555} + 4^{5555}) + (5555^{2222} - 4^{2222}) - (4^{5555} - 4^{2222}).$$

Выражение в первой скобке делится на $2222 + 4 = 2226 = 7 \cdot 318$, следовательно, делится на 7. Выражение во второй скобке делится на $5555 - 4 = 5551 = 7 \cdot 793$, следовательно, делится на 7.

Преобразуем третье выражение:

$$4^{5555} - 4^{2222} = 4^{2222}(64^{1111} - 1).$$

Теперь видно, что третье выражение делится на $64 - 1 = 63$, следовательно, делится на 7.

Поскольку каждое из выражений делится на 7, их сумма также делится на 7.

2) Имеем

$$222^{555} + 555^{222} = 111^{555} \cdot 2^{555} + 111^{222} \cdot 5^{222} = \\ = 111^{222}(111^{333} \cdot 2^{555} + 5^{222}) = \\ = 111^{222}((111^3 \cdot 2^5)^{111} + 25^{111}),$$

поэтому сумма делится на 111^{222} и на $111^3 \cdot 2^5 + 25 = 43\,764\,217 = \\ = 7 \cdot 6\,252\,031$.

3) Имеем

$$30^{239} \equiv (-1)^{239} \equiv -1 \pmod{31}.$$

Поскольку НОД$(239, 31) = 1$ и 31 — простое число, применив малую теорему Ферма, получим $239^{30} \equiv 1 \pmod{31}$. Следовательно,

$$30^{239} + 239^{30} \equiv -1 + 1 \equiv 0 \pmod{31},$$

т. е. сумма делится на 31 и является составным числом.

Замечание. Можно, конечно, представить сумму в виде

$$30^{239} + 239^{30} = (30^{239} + 1^{239}) + (239^{30} - 1^{30}).$$

Понятно, что выражение в первой скобке делится на 31. Разложим выражение во второй скобке на множители:

$$239^{30} - 1^{30} = (239^{15} + 1)(239^{15} - 1).$$

Увидеть без малой теоремы Ферма, что первый сомножитель делится на 31, достаточно трудно, поскольку ни $239 + 1 = 240$, ни $239^3 + 1$, ни $239^5 + 1$ на 31 не делятся.

3. а) Докажем, что выражение $19^{71} + 71^{19} - 90$ делится на 360. Имеем

$$19^{71} + 71^{19} - 90 = 19^{71} - 19 + 71^{19} - 71 = \\ = 19(19^{70} - 1) + 71(71^{18} - 1) = 19(361^{35} - 1) + 71(5041^{9} - 1).$$

Применяя формулы сокращённого умножения, видим, что первое слагаемое делится на $360 = 361 - 1$. Второе слагаемое делится на $5041 - 1 = 5040 = 360 \cdot 14$ и также делится на 360. Значит, сумма делится на 360. Тогда $19^{71} + 71^{19} - 90 = 360m$ для некоторого натурального m. Отсюда следует утверждение задачи.

б) Поступим аналогично. Докажем, что выражение $19^{77} + 77^{19} - 96$ делится на 456. Имеем

$$19^{77} + 77^{19} - 96 = 19^{77} - 19 + 77^{19} - 77 = 19(19^{76} - 1) + 77(77^{18} - 1).$$

Рассмотрим первое слагаемое. Поскольку $456 = 19 \cdot 24$, достаточно доказать, что множитель $19^{76} - 1$ делится на 24. Имеем $19^{76} - 1 = \\ = (19^2)^{38} - 1$. Этот множитель делится на $19^2 - 1 = 360 = 24 \cdot 15$, т. е. делится на 24. Следовательно, первое слагаемое делится на 456.

Рассмотрим второй множитель второго слагаемого

$$77^{18} - 1 = (77^2)^9 - 1.$$

Он делится на $77^2 - 1 = (77 - 1)(77 + 1) = 76 \cdot 78 = 456 \cdot 13$, т. е. делится на 456. Следовательно, сумма делится на 456.

Тогда $19^{77} + 77^{19} - 96 = 456n$ для некоторого натурального n. Отсюда следует утверждение задачи.

4. Поскольку p и q — различные простые числа (и, следовательно, взаимно просты), применима малая теорема Ферма. Имеем

$$p^q + q^p \equiv pp^{q-1} \equiv p \pmod{q},$$
$$p^q + q^p \equiv qq^{p-1} \equiv q \pmod{p}.$$

Остаётся применить китайскую теорему об остатках.

6. Для любого $k \in \mathbb{N}$ число $m^4 + 4k^4$ будет составным. См. решение упражнения 1.

Решения упражнений

1. Имеем

$$n^4 + 4m^4 = n^4 + 4n^2m^2 + 4m^4 - 4n^2m^2 = \\ = (n^2 + 2m^2)^2 - (2nm)^2 = (n^2 + 2nm + 2m^2)(n^2 - 2nm + 2m^2).$$

2. а) Последовательность $\{r'_n\}$, где r'_n — остаток от деления n^5 на 3, периодична с периодом 3. Её начальные члены равны $0, 1, 2, 0, 1, 2, \ldots$

Последовательность $\{r_n''\}$, где r_n'' — остаток от деления 5^n на 3, периодична с периодом 2. Её начальные члены равны $1, 2, 1, 2, \ldots$ Тогда последовательность $\{r_n\}$, где r_n — остаток от деления $5^n + n^5$ на 3, периодична с периодом 6. Её начальные члены равны $1, 0, 0, 2, 2, 1, 1, \ldots$

Следовательно, остаток от деления $5^n + n^5$ на 3 равен нулю только в случаях $n = 6k+1$, $n = 6k+2$, где $k \in \mathbb{Z}$, $k \geqslant 0$. Наименьшим будет $n = 1$.

б) Последовательность $\{r_n'\}$, где r_n' — остаток от деления n^5 на 7, периодична с периодом 7. Её начальные члены равны $0, 1, 4, 5, 2, 3, 6, \ldots$ Последовательность $\{r_n''\}$, где r_n'' — остаток от деления 5^n на 7, периодична с периодом 6. Её начальные члены равны $1, 5, 4, 6, 2, 3, \ldots$ Тогда последовательность $\{r_n\}$, где r_n — остаток от деления $5^n + n^5$ на 7, периодична с периодом 42. Её начальные члены равны $1, 6, 1, 4, 4, 6, 0, \ldots$

Следовательно, остаток от деления $5^n + n^5$ на 7 равен нулю только в случаях $n = 42k+6$, $n = 42k+10$, $n = 42k+15$, $n = 42k+23$, $n = 42k+25$, $n = 42k + 26$, где $k \in \mathbb{Z}$, $k \geqslant 0$. Наименьшим будет $n = 6$.

в) Последовательность $\{r_n'\}$, где r_n' — остаток от деления n^5 на 11, периодична с периодом 11. Её начальные члены равны $0, 1, 10, 1, 1, 1, \ldots$ Последовательность $\{r_n''\}$, где r_n'' — остаток от деления 5^n на 11, периодична с периодом 5. Её начальные члены равны $1, 5, 3, 4, 9, \ldots$ Тогда последовательность $\{r_n\}$, где r_n — остаток от деления $5^n + n^5$ на 11, периодична с периодом 55. Её начальные члены равны $1, 6, 2, 5, 10, 2, 4, \ldots$

Следовательно, остаток от деления $5^n + n^5$ на 11 равен нулю только в случаях $n = 55k+10$, $n = 55k+30$, $n = 55k+35$, $n = 55k+40$, $n = 55k+50$, где $k \in \mathbb{Z}$, $k \geqslant 0$.

Наименьшим будет $n = 10$.

3. При $p = 2$ подойдёт любое нечётное n. В этом случае $5^n + n^5$ делится на 2.

При $p = 5$ подойдёт любое n, делящееся на 5. В этом случае $5^n + n^5$ делится на 5.

Рассмотрим нечётное простое $p \neq 5$. Поскольку 5 и p взаимно просты, можно применить малую теорему Ферма, получив для $n = p - 1$:

$$5^{p-1} + (p-1)^5 \equiv 1 + (-1)^5 \equiv 0 \pmod{p}.$$

Учтём периодичность последовательности и возьмём теперь

$$n = (p-1)pk + p - 1 = (p-1)(pk+1).$$

Имеем НОД$(n, p) = 1$, откуда

$$5^{(p-1)(pk+1)} + ((p-1)pk + p - 1)^5 \equiv$$
$$\equiv (5^{(p-1)})^{(pk+1)} + (-1)^5 \equiv 1 - 1 \equiv 0 \pmod{p}.$$

Что и требовалось доказать!

4. а) Последовательность $\{r'_n\}$, где r'_n — остаток от деления n^2 на 5, периодична с периодом 5. Её начальные члены равны $0, 1, 4, 4, 1, \ldots$ Последовательность $\{r''_n\}$, где r''_n — остаток от деления 2^n на 5, периодична с периодом 4. Её начальные члены равны $1, 2, 4, 3, \ldots$ Тогда последовательность $\{r_n\}$, где r_n — остаток от деления $2^n + n^2$ на 5, периодична с периодом 20. Её начальные члены равны $1, 3, 3, 2, 2, 2, 0, \ldots$

Следовательно, остаток от деления $2^n + n^2$ на 5 равен нулю только в случаях $n = 20k+6$, $n = 20k+8$, $n = 20k+12$, $n = 20k+14$, где $k \in \mathbb{Z}$, $k \geqslant 0$.

б) Последовательность $\{r'_n\}$, где r'_n — остаток от деления n^2 на 11, периодична с периодом 11. Её начальные члены равны 0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1, … Последовательность $\{r''_n\}$, где r''_n — остаток от деления 2^n на 11, периодична с периодом 10. Её начальные члены равны 1, 2, 4, 8, 5, 10, 9, 7, 3, 6, … Тогда последовательность $\{r_n\}$, где r_n — остаток от деления $2^n + n^2$ на 11, периодична с периодом 110. Её начальные члены равны 1, 3, 8, 6, 10, 2, 1, …

Следовательно, остаток от деления $2^n + n^2$ на 11 равен нулю только в случаях $n = 110k + t$, где $t \in \{29, 41, 45, 57, 59, 65, 83, 91, 93, 97\}$ и $k \in \mathbb{Z}$, $k \geqslant 0$.

5. а) Остатками от деления n^2 на 7 являются числа $\{0, 1, 2, 4\}$. Остатками от деления 2^n на 7 являются числа $\{1, 2, 4\}$. Тогда возможные остатки от деления $2^n + n^2$ на 7 будут $\{1, 2, 3, 4, 5, 6\}$. Следовательно, $2^n + n^2$ не делится на 7 ни для какого натурального n.

б) Рассмотрим простые числа вида $p = 8k - 1$, где $k \in \mathbb{Z}$, $k \geqslant 0$. Таких чисел бесконечно много в силу теоремы Дирихле о простых числах в арифметических прогрессиях. Для таких простых чисел сумма $2^n + n^2$ не делится на p ни для какого натурального n.

6. Пусть $n = pq$ — составное число, где $p \geqslant 2$, $q \geqslant 2$. Тогда $2^n - 1 = 2^{pq} - 1 = (2^q)^p - 1^p$ делится на $2^q - 1$.

7. Докажем с помощью теста Люка, что число

$$m = 2^{15} + 15^2 = 32\,993$$

— простое.

Найдём разложение числа $m - 1 = 2^{15} + 15^2 - 1$ на простые множители. Имеем $2^{15} + 15^2 - 1 = 2^5 \cdot 1031$.

В качестве кандидата возьмём $b = 3$. Нам нужно найти вычеты

$$3^{m-1} = 3^{2^{15}+15^2-1}, \quad 3^{(m-1)/2} = 3^{2^4 \cdot 1031}, \quad 3^{(m-1)/1031} = 3^{2^5}$$

по модулю $m = 32\,993$.

Начнём с вычета $3^{(m-1)/1031} = 3^{2^5}$. Имеем

$$3^{2^5} = 3^{32} = (3^4)^8 = (81^2)^4 \equiv (6561^2)^2 \equiv 23\,849^2 \equiv 8474 \pmod{32\,993}.$$

Далее,

$$3^{1031} = 3^{2^{10}+7} = 3^7 \cdot (3^{32})^{32} \equiv 3^7 \cdot (8474^2)^{16} \equiv 3^7 \cdot (15\,908^2)^8 \equiv$$
$$\equiv 3^7 \cdot (8154^2)^4 \equiv 3^7 \cdot (6821^2)^2 \equiv 3^7 \cdot 5911^2 \equiv 4612 \pmod{32\,993};$$
$$3^{(m-1)/2} = 3^{2^4 \cdot 1031} = (3^{1031})^{16} \equiv (4612^2)^8 \equiv (23\,052^2)^4 \equiv$$
$$\equiv (9446^2)^2 \equiv 13\,844^2 \equiv 32\,992 \equiv -1 \pmod{32\,993}.$$

Наконец,

$$3^{m-1} = 3^{2^{15}+15^2-1} \equiv (-1)^2 \equiv 1 \pmod{32\,993}.$$

Итак,

$$3^{m-1} \equiv 1 \pmod{m},$$
$$3^{(m-1)/2} \not\equiv 1 \pmod{m},$$
$$3^{(m-1)/1031} \not\equiv 1 \pmod{m}.$$

Согласно тесту Люка число $m = 2^{15} + 15^2 = 32\,993$ — простое.

Читатель может убедиться самостоятельно, что для $b = 2$ тест даёт неопределённый ответ.

8. По условию имеем $p = 20k + 7$, где $k \in \mathbb{Z}$, $k \geqslant 0$. Тогда

$$(p-1)^p + p^{p-1} = (20k+6)^{20k+7} + (20k+7)^{20k+6} \equiv 1^{20k+7} + 2^{20k+6} \equiv$$
$$\equiv 1 + 4^{10k+3} \equiv 1 + (-1)^{10k+3} \equiv 1 - 1 \equiv 0 \pmod{5}.$$

9. По условию имеем $p = 17k_1 + 2$ и $p = 8k_2 + 5$, где $k_i \in \mathbb{Z}$, $k_i \geqslant 0$, $i = 1, 2$. Отсюда

$$(p-1)^p + p^{p-1} = (17k_1+1)^p + (17k_1+2)^{p-1} \equiv 1^p + 2^{8k_2+4} \equiv$$
$$\equiv 1 + 16^{2k_2+1} \equiv 1 + (-1)^{2k_2+1} \equiv 1 - 1 \equiv 0 \pmod{17}.$$

Замечание. С помощью китайской теоремы об остатках можно получить, что $p = 136k + 53$, где $k \in \mathbb{Z}$, $k \geqslant 0$.

Список литературы

[1] *Koninck J.-M. de., Mercier A.* 1001 Problemes en Théorie Classique Des Nombres. Problem 165 pp. 30, 160. Paris: Ellipses, 2004.

[2] *Diffie W., Hellman M. E.* New directions in cryptography // IEEE Trans. Inform. Theory. 1976. Vol. 22. P. 644–654.

[3] *Everest G., Poorten A. van der., Shparlinski I., Ward T.* Recurrence Sequences // Amer. Math. Soc., 2003; see esp. p. 255.

[4] *Pomerance C., Selfridge J. L., Wagstaff S. S., Jr.* The pseudoprimes to $25{\times}10^9$ // Math. Comp. 1980. Vol. 35, № 151. P. 1003–1026.

[5] *Rivest R., Shamir A., Adleman L.* A method for obtaining digital signatures and public-key cryptosystems (англ.) // Commun. ACM. 1978. Vol. 21, № 2. P. 120–126.

[6] *Варновский Н. П.* Криптография и теория сложности // Математическое просвещение. Сер. 3. Вып. 2. М.: МЦНМО, 1998. С. 71–86.

[7] *Виноградов И. М.* Основы теории чисел. М.: Ленанд, 2022.

[8] *Воробьёв Н. Н.* Признаки делимости. М.: Наука, 1980.

[9] *Горбачёв Н. В.* Сборник олимпиадных задач по математике. М.: МЦНМО, 2010.

[10] *Дайан-Дальмедико Эми.* Софи Жермен // В мире науки. 1992. № 2. С. 60–66.

[11] Задачник Кванта, М663 // Квант. 1981. № 1. С. 26.

[12] Зарубежные математические олимпиады. М.: Наука, 1987.

[13] *Кордемский Б. А., Ахадов А. А.* Удивительный мир чисел: Математические головоломки и задачи для любознательных. М.: Просвещение, 1986.

[14] *Коутинхо С.* Введение в теорию чисел. Алгоритм RSA. М.: Постмаркет, 2001.

[15] *Манин Ю. И., Панчишкин А. А.* Введение в современную теорию чисел. М.: МЦНМО, 2009.

[16] Математика в задачах. М.: МЦНМО, 2009.

[17] *Нестеренко Ю. В.* Алгоритмические проблемы теории чисел // Математическое просвещение. Сер. 3. Вып. 2. М.: МЦНМО, 1998. С. 87–114.

[18] *Оре О.* Приглашение в теорию чисел. М.: Наука, 1980. (Серия «Библиотечка „Квант“»; Вып. 3).

[19] *Прасолов В. В.* Доказательство квадратичного закона взаимности по Золотарёву // Математическое просвещение. Сер. 3. Вып. 4. М.: МЦНМО, 2000. С. 140–144.

[20] *Рудаков А. Н.* Числа Фибоначчи и простота числа $2^{127} - 1$ // Математическое просвещение. Сер. 3. Вып. 4. М.: МЦНМО, 2000. С. 127–139.

[21] *Суконник Я. Н.* Математические задачи повышенной трудности. Киев: Радянська школа, 1985.

[22] *Хооли К.* Применения методов решета в теории чисел. М.: Наука, 1987.

[23] *Шклярский Д. О., Ченцов Н. Н., Яглом И. М.* Избранные задачи и теоремы элементарной математики. Арифметика и алгебра. М.: Наука, 1976.

[24] *Ященко В. В.* Основные понятия криптографии // Математическое просвещение. Сер. 3. Вып. 2. М.: МЦНМО, 1998. С. 53–70.

[25] XV Всероссийская олимпиада по математике и физике // Квант. 1989. № 10. С. 67–70.

[26] https://ru.wikipedia.org/wiki/

[27] https://cocalc.com/

[28] http://oeis.org/

[29] https://primes.utm.edu/mersenne/index.html#known

Валерий Михайлович Журавлёв, ПАО «Туполев», Москва
zhuravlevvm@mail.ru

Пётр Исаакович Самовол, Беер-Шева, Израиль
pet12@012.net.il