ТЕСТ ФЕРМА НА ПРОСТОТУ

К. Конрад

1. Введение

Малая теорема Ферма утверждает, что для простого p и всех целых $a \not\equiv 0 \bmod p$ выполняется $a^{p-1} \equiv 1 \bmod p$. Рассмотрим это утверждение в том числе для составных модулей: для составного целого $n \geq 2$ и всех целых $a \not\equiv 0 \bmod n$

$$a^{n-1} \equiv 1 \bmod n.$$

Назовём это сравнение "малым сравнением Ферма".[1] *Оно может выполняться, а может и не выполняться.* Для простых n оно выполняется для всех $a \not\equiv 0 \bmod n$. Но для составных n можно привести контрпримеры.

Пример 1.1. В приведённой ниже таблице для $n = 15$ показано, что всего для четырёх значений $a \not\equiv 0 \bmod 15$ выполняется сравнение $a^{14} \equiv 1 \bmod 15$.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$a^{14} \bmod 15$	1	4	9	1	10	6	4	4	6	10	1	9	4	1

Пример 1.2. Среди всех целых $a \not\equiv 0 \bmod 91$, 36 из них (меньше половины) удовлетворяют $a^{90} \equiv 1 \bmod 91$. Ниже показано, как обстоит дело при небольших a.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	$\cdots$
$a^{90} \bmod 91$	1	64	1	1	64	64	77	64	1	1	64	1	78	14	64	$\cdots$

Если малое сравнение Ферма $a^{n-1} \equiv 1 \bmod n$ нарушается хотя бы при одном целом $a \not\equiv 0 \bmod n$, то число n не может быть простым и потому оно составное. К примеру, $2^{14} \not\equiv 1 \bmod 15$ и $2^{90} \not\equiv 1 \bmod 91$, поэтому 15 и 91 составные. Конечно, 15 и 91 небольшие числа, в составности которых нетрудно убедиться, разложив их на множители ($15 = 3 \cdot 5$ и $91 = 7 \cdot 13$). Нарушение малого сравнения Ферма на самом деле используется для значительно бóльших значений n, поскольку позволяет обосновать составность большого числа, не раскладывая его на множители. Этим мы и займёмся.

2. Три теста на простоту

Самый простой способ проверки составности числа $n > 1$ это *пробные деления* на числа до $\sqrt{n}$, т.е. надо проверить все целые a больше 1 и меньше либо равные $\sqrt{n}$, чтобы проверить $a \mid n$. Если такое a обнаруживается, то n составное. Если же такого a нет, значит n — простое. Потенциальные делители числа n можно искать только до $\sqrt{n}$ поскольку, если $n = ab$, где $a < n$ и $b < n$, то одно из значений a или b меньше или равно $\sqrt{n}$. Метод пробных делений доказывает составность n только если найден один из его нетривиальных делителей.

[1] В дальнейшем мне будет удобно пользоваться этой своей терминологией, хоть она и не стандартна.

Пример 2.1. Пусть $n = 415693$. Тогда $\sqrt{n} \approx 644,74$. Единственный подходящий нетривиальный делитель числа n это 593. Поскольку $593/\sqrt{n} \approx 0,92$, нам придётся проверить более 90% чисел до $\sqrt{n}$, прежде чем мы убедимся в составности числа n этим методом.

Незначительное улучшение алгоритма пробных делений можно получить при помощи вычисления НОД выбранного кандидата на делители и числа n: выберем случайное число a такое, что $1 \leq a \leq n-1$ и вычислим НОД (a, n) при помощи алгоритма Евклида. Поскольку $(a, n) \leq a < n$, если $(a, n) > 1$, то (a, n) это нетривиальный делитель числа n и n составное. С другой стороны, если равенство $(a, n) = 1$ нам ничего не даёт, надо выбрать другое случайное число a из диапазона от 1 до $n-1$ и попробовать снова. Назовём этот способ *НОД-тестом* на составность.

Пример 2.2. Возьмём $n = 415693$ из предыдущего примера. Заметим, что у числа n есть только один нетривиальный делитель до корня $\sqrt{n}$, а количество чисел a от 1 до $n-1$ таких, что $(a, n) > 1$ равно 1292. Так что вероятность попасть на число от 1 до $n-1$, имеющее общий нетривиальный с n делитель выше, чем вероятность угадать делитель среди чисел до $\sqrt{n}$. И всё же шансы получить работоспособный алгоритм, основанный на НОД-тестировании нескольких случайно выбранных значений невелики: $1292/(n-1) \approx .31\%$, что меньше $1/3$ одного процента.

Значительно улучшить качество проверки на простоту по сравнению с НОД-тестом можно, если попытаться найти опровержение малого сравнения Ферма $a^{n-1} \equiv 1 \bmod n$ для какого-то целого a от 1 до $n-1$.

Пример 2.3. Пусть снова $n = 415693$. Тогда $2^{n-1} \equiv 58346 \not\equiv 1 \bmod n$, так что после первой же попытки при $a = 2$ мы доказали, что число n составное. Количество чисел a от 1 до $n-1$, удовлетворяющих сравнению $a^{n-1} \not\equiv 1 \bmod n$, равно 415677, при этом $415677/(n-1)$ больше 99.99%. Надо быть крайне неудачливым, чтобы случайно выбранное вами число a от 1 до $n-1$ не доказало бы составность числа n.

Назовём только что описанный способ *тестом Ферма*:

$$\text{если } a^{n-1} \not\equiv 1 \bmod n \text{ хотя бы для одного целого } a \ (1 \leq a \leq n-1), \text{ тогда } n \text{ составное.}$$

В самом деле, если бы n было простым, то в силу малой теоремы Ферма $a^{n-1} \equiv 1 \bmod n$ для *всех целых* a от 1 to $n-1$. Если это неверно хотя бы для одного a, число n обязательно будет составным.

Целое число, меньшее n и доказывающее его составность, называется свидетелем составности n. Тип свидетеля зависит от вида используемого нами теста.

Определение 2.4. Пусть $1 \leq a \leq n-1$. Будем называть число a свидетелем *пробного деления* для числа n, если $a \mid n$ и $a > 1$.[2] Назовём число a *НОД-свидетелем* для n, если $(a, n) > 1$. Наконец, назовём число a *свидетелем Ферма* для n, если $a^{n-1} \not\equiv 1 \bmod n$.

Обнаружить составность числа n можно свидетелем пробного деления, если найден делитель n; НОД-свидетелем, если найдено число, НОД которого с n больше 1 и свидетелем Ферма, если найдено число, нарушающее малое сравнение Ферма.[3] Число 1 не

[2]Свидетели пробного деления не могут превышать $\sqrt{n}$, поскольку дальше этой границы проверка делимости не делается.

[3]Иногда с термином «свидетель Ферма» связывают условие $a^{n-1} \not\equiv 1 \bmod n$ *и* $(a, n) = 1$, более строгое, чем используемое нами. Мы не накладываем ограничение на НОД, поскольку условие $a^{n-1} \not\equiv 1 \bmod n$ показывает нам составность n вне зависимости от значения (a, n).

является свидетелем ни для одного из тестов, так что диапазон поиска можно сузить до $2 \le a \le n-1$. Также число $n-1$ не является свидетелем в тестах, кроме теста Ферма для случая чётного n.

Число 3 это свидетель пробного деления и НОД-свидетель числа 15, число 10 является НОД-свидетелем числа 15, но не свидетелем пробного деления для 15. А какие свидетели Ферма есть у 15?

Пример 2.5. Поскольку $2^{14} \equiv 4 \not\equiv 1 \bmod 15$ (см. таблицу в Примере 1.1), 2 это свидетель Ферма для 15, так же, как и любое число от 2 до 13, исключая 4 и 11.

Пример 2.6. Для числа $n = 415693$ из Примера 2.3 первая же проверка для числа 2 даёт $2^{n-1} \not\equiv 1 \bmod n$, то есть число 2 это свидетель Ферма для n. Мы определили, что число n составное, не находя никаких его нетривиальных делителей.

Пример 2.7. Пусть $n = 1387$. Сравнение $2^{1386} \equiv 1 \bmod 1387$ не даёт нам никакой информации о простоте или составности числа n. (Может 1387 простое, и сравнение с участием 2 это просто иллюстрация малой теоремы Ферма.) Однако, $3^{1386} \equiv 875 \not\equiv \not\equiv 1 \bmod 1387$, так что число 1387 составное и число 3 является свидетелем Ферма для 1387.

Пример 2.8. Пусть $n = 2^{2^5} + 1 = 4294967297$. Ферма полагал, что n простое, но это не так: хотя $2^{n-1} \equiv 1 \bmod n$, оказывается, что $3^{n-1} \equiv 3029026160 \not\equiv 1 \bmod n$. Таким образом, 3 это свидетель Ферма, доказывающий, что n составное без предъявления делителя. Эйлер обнаружил, что 641 является делителем n примерно через 100 лет после ошибочного предположения Ферма о простоте n.

Пример 2.9. Пусть $n = 2^{2^{14}} + 1$. В записи этого числа 4933 цифры. Первая проверка ничего не даёт: $2^{n-1} \equiv 1 \bmod n$, но уже для тройки компьютер за несколько секунд определяет, что $3^{n-1} \not\equiv 1 \bmod n$, поэтому n — составное. Этот факт впервые был доказан в 1961 году Гурвицем и Селфриджем (Hurwitz, Selfridge), которые показали, что $3^{(n-1)/2} \not\equiv \pm 1 \bmod n$. Нетривиальный делитель числа n впервые найден Раджалой и Волтманом (Rajala, Woltman) почти 50 лет спустя, в 2010 году: это 54-разрядное число

$$116928085873074369829035993834596371340386703423373313.$$

Второй делитель, соответствующий найденному, записывается 4880 цифрами и является составным (свидетель Ферма — число 3), но его разложение на множители до сих пор неизвестно.

Для составных чисел двойка часто оказывается свидетелем Ферма. То есть часто $2^{n-1} \not\equiv 1 \bmod n$, что немедленно показывает составность числа n. Среди чисел $n < 1000$ всего два — 341 and 561 — являются составными и $2^{n-1} \equiv 1 \bmod n$. Среди первых 10000 чисел всего двадцать два таких составных числа. Если же мы учтём несколько свидетелей Ферма, ещё меньше чисел окажутся «ложноположительно» простыми: почти у всех составных чисел, не превышающих 10000 числа 2 и 3 являются свидетелями Ферма (исключение составляют 1105, 1729, 2465, 2701, 2821, 6601 и 8911) и у всех составных чисел до 10000 свидетелем Ферма является одно из чисел 2, 3, 5 или 7. Очевидно, малое сравнение Ферма работает в качестве доказательства составности чисел лучше пробного деления и НОД-теста!

Как же соотносятся эти тесты друг с другом? Поскольку для $a \ge 2$ выполняется:

$$a^{n-1} \equiv 1 \bmod n \Longrightarrow (a, n) = 1 \Longrightarrow a \nmid n,$$

и переходя к противоположным утверждениям мы имеем для $a \geq 2$:

$$a \mid n \Longrightarrow (a,n) > 1 \Longrightarrow a^{n-1} \not\equiv 1 \bmod n,$$

таким образом свидетель пробного деления (т.е. делитель, бóльший единицы) является НОД-свидетелем, а НОД-свидетель является свидетелем Ферма. Потому свидетели Ферма так важны для нас — свидетелей этого типа *гораздо* больше, чем других.

Пример 2.10. В Примерах 2.1, 2.2 и 2.3 мы видели, что для $n = 415693$ доля свидетелей пробного деления и НОД-свидетелей меньше 1%, в том время, как доля свидетелей Ферма больше 99.99%.

Пример 2.11. У числа 1387 есть 2 свидетеля пробного деления, 91 НОД-свидетель и 1063 свидетелей Ферма. Доля первых двух менее 1%, а количество свидетелей Ферма примерно 77%. Это достаточно много для того, чтобы найти свидетеля Ферма, сделав несколько случайных попыток.

3. Количество свидетелей Ферма

Следующая теорема даёт условие на число $n > 1$, при выполнении которого у числа n достаточно много свидетелей Ферма среди чисел $\{1, \ldots, n-1\}$.

Theorem 3.1. *Пусть $n \geq 2$. Если некоторое число b удовлетворяет $b^{n-1} \not\equiv 1 \bmod n$ и $(b,n) = 1$, то*

$$|\{1 \leq a \leq n-1 : a^{n-1} \not\equiv 1 \bmod n\}| > \frac{n-1}{2}.$$

Иными словами, если существует свидетель Ферма взаимно простой с n, то более половины всех целых чисел от 1 до $n-1$ являются свидетелями Ферма для n.

Доказательство. Обозначим

$$\begin{aligned} A &= \left\{1 \leq a \leq n-1 : a^{n-1} \equiv 1 \bmod n\right\}, \\ B &= \left\{1 \leq a \leq n-1 : (a,n) = 1 \text{ and } a^{n-1} \not\equiv 1 \bmod n\right\}, \\ C &= \{1 \leq a \leq n-1 : (a,n) > 1\}. \end{aligned}$$

Множества A, B и C попарно не пересекаются (почему?) и содержат все числа от 1 до $n-1$. Объединение множеств B и C представляет собой множество свидетелей Ферма, а множество A содержит все остальные числа от 1 до $n-1$. (Элементы множества C это НОД-свидетели, и каждый НОД-свидетель это свидетель Ферма.) Число 1 принадлжит множеству A (но не B и C).

По предположению $B \neq \emptyset$, поэтому n должно быть составным, а значит C тоже непусто. Теорема утверждает, что если $B \neq \emptyset$, то $|B| + |C| > (n-1)/2$. Чтобы это показать, используем идею из доказательства малой теоремы Ферма: умножим каждый элемент в некотором множестве на одно и то же число.

Поскольку B непусто, возьмём какой-то его элемент b и рассмотрим множество $Ab = \{ab \bmod n : a \in A\}$, это подмножество B. Здесь "$ab \bmod n$" означает остаток при делении ab на n. В самом деле, для каждого $a \in A$, произведение ab взаимно просто с n и

$$(ab)^{n-1} \equiv a^{n-1}b^{n-1} \equiv b^{n-1} \not\equiv 1 \bmod n,$$

поэтому $ab \bmod n \in B$. Это верно для всех $a \in A$, поэтому $Ab \subset B$.

Если для двух элементов a и a' из множества A выполняется $ab \equiv a'b \bmod n$, мы можем сократить обе части на b. Получим $a \equiv a' \bmod n$, откуда следует, что $a = a'$, потому

что числа в множестве A находятся строго между 0 и n. Поэтому количество элементов в множестве Ab равно $|A|$, а из $Ab \subset B$ получаем $|A| = |Ab| \leq |B|$. Следовательно

$$n - 1 = |A| + |B| + |C| \geq |A| + |A| + 1 > 2|A|,$$

таким образом $|A| < (n-1)/2$, т.е. A содержит *менее половины* элементов множества $\{1, 2, \ldots, n-1\}$, а значит его дополнение $B \cup C$ содержит *более половины* элементов множества $\{1, 2, \ldots, n-1\}$:

$$|B| + |C| = (n-1) - |A| > (n-1) - \frac{n-1}{2} = \frac{n-1}{2}.$$

□

Замечание 3.2. Знакомые с теорией групп читатели узнают в множестве Ab класс смежности. Переформулируем для них наше доказательство на языке теории групп. Обратимые по модулю n числа представляют собой группу по умножению, а множество A решений малого сравнения Ферма $a^{n-1} \equiv 1 \bmod n$ образуют подгруппу этой группы. Если среди обратимых чисел найдётся контрпример к малому сравнению Ферма (*т.е.*, если $B \neq \emptyset$), то A это собственная подгруппа и значит её индекс *по меньшей мере* равен 2 и A содержит *не больше половины* всех обратимых чисел по модулю n.

Теорема 3.1 утверждает, что более половины целых чисел среди $\{1, \ldots, n-1\}$ являются свидетелями Ферма для n, если существует свидетель Ферма, взаимно простой с n. Число a, для которого $(a, n) > 1$ — очевидно свидетель Ферма для n, так что если существует "нетривиальный" свидетель Ферма (т.е. не являющийся НОД-свидетелем), то свидетелей Ферма должно быть достаточно много.

Число 1 не может быть свидетелм Ферма, поэтому мы не будем рассматривать его при изучении теста Ферма.

Следствие 3.3. *Если у числа $n \geq 2$ есть свидетель Ферма, взаимно простой с n*[4]*, то доля целых чисел от 2 до $n-1$, являющихся свидетелями Ферма для n составляет более 50%.*

Доказательство. Пусть W — количество свидетелей Ферма для n среди чисел от 1 до $n-1$. Из Теоремы 3.1 следует, что $W/(n-1) > 1/2$, значит доля свидетелей Ферма для n среди чисел $\{2, \ldots, n-1\}$ равна $W/(n-2) > W/(n-1) > 1/2$. □

Следствие 3.3 даёт нам следующий *вероятностный* тест на простоту: будем выбирать случайные числа из $\{2, \ldots, n-1\}$ и проверять — не нарушает какое-то из них малое сравнение Ферма. Если более половины чисел из $\{2, \ldots, n-1\}$ являются свидетелями Ферма для n, то вероятность *не найти* свидетеля Ферма среди, скажем, 10 случайно выбранных чисел будет меньше, чем вероятность увидеть один и тот же результат в серии из 10 подкидываний честной монеты (такая вероятность равна $1/2^{10} \approx 0,000976$). Так что можно утверждать, что n окажется простым с "вероятностью" по крайней мере $1 - 1/2^{10} \approx 0,99902$. Слово "вероятность" здесь мы взяли в кавычки, поскольку простота чисел всё же не предмет теории вероятностей.

Однако, у теста Ферма есть слабое место: существуют составные числа n, для которых Следствие 3.3 неприменимо: для каждого a, взаимно простого с n, выполняется $a^{n-1} \equiv 1 \bmod n$. В следующем разделе мы изучим эту проблему.

[4]Существование хотя бы одного свидетеля Ферма для n влечёт составность n.

Пример 3.4. Пусть $n = 13079177569$. Это число составное и оказывается, что $a^{n-1} \not\equiv \not\equiv 1 \bmod n$ лишь в случае $(a, n) > 1$. Свидетели Ферма для этого числа в точности совпадают с НОД-свидетелями. Количество НОД-свидетелей равно 18483553, что кажется вполне достаточным, но в записи этого числа всего 8 цифр против 11 цифр в числе n. Доля Ферма (и НОД) свидетелей для n равна примерно 0,14%. (Это не опечатка: именно $0,14\% = 0,0014$.) Автору потребовалось сделать 50 попыток, прежде чем случайно выбранное число оказалось свидетелем Ферма для n.

Пример 3.5. Число $n = 232250619601$ тоже составное, и снова $a^{n-1} \not\equiv 1 \bmod n$ выполняется лишь при $(a, n) > 1$, но в этом случае доля свидетелей Ферма немного превышает 37%. Здесь автору повезло больше — всего со второй попытки было выбрано случайное число, оказавшееся свидетелем Ферма для n.

Пример 3.6. Пусть $n = 56052361$. Применив тест Ферма и выбирая случайные значения $a \bmod n$, первый свидетель Ферма встретился на 59-й попытке.

Пример 3.7. Пусть $n = 11004252611041$. Это число составное (используя Wolfram Alpha, можно довольно быстро разложить его на множители), но сделав 100 попыток теста Ферма со случайными числами $a \bmod n$ автор не смог найти ни одного свидетеля Ферма. Попробуйте сами.

4. Ложноположительные свидетели Ферма: числа Кармайкла

Выходит, что запустив, скажем, 10 раз тест Ферма и не найдя свидетеля Ферма, мы не сможем обосновать простоту числа n, опираясь на вероятностные соображения: существуют составные числа, все свидетели Ферма которых это НОД-свидетели. В таком случае Следствие 3.3 неприменимо, да и нет уверенности в том, что доля свидетелей Ферма достаточно велика.

Определение 4.1. Составное число n, у которого нет взаимно простых с n свидетелей Ферма называется *числом Кармайкла*. Иными словами, n является числом Кармайкла, когда n составное и $(a, n) = 1 \Longrightarrow a^{n-1} \equiv 1 \bmod n$.

Названы они в честь Роберта Кармайкла (Robert Carmichael), который нашёл несколько таких чисел в начале 20 века. Несколько чисел Кармайкла приведены в конце работы [2], больше примеров можно найти в [3]. Вот первые пять чисел Кармайкла:

$$561, \quad 1105, \quad 1729, \quad 2465, \quad 2821.$$

Числа в Примерах 3.4, 3.5, 3.6 и 3.7 — тоже числа Кармайкла. Пока неизвестен эффективный алгоритм, определяющий является ли число Кармайкловым, но Алфорд, Гранвилл и Померанс (Alford, Granville, Pomerance) [1] доказали, что чисел Кармайкла бесконечно много, т.е. не существует границы, за которой этих чисел нет.

Как часто случается, Кармайкл был не первым, кто изучал числа Кармайкла. Двадцатью пятью годами раньше Шимерка (Šimerka [4]) нашёл первые семь чисел Кармайкла, но его работа была напечатана в чешском математическом журнале и её мало кто читал. Ниже приведена выдержка из его статьи [4], где мы видим числа $561, 1105, 1729, \ldots, 8911$. Было бы справедливо использовать термин числа Шимерки вместо чисел Кармайкла, но уже, видимо, поздно менять устоявшееся название.

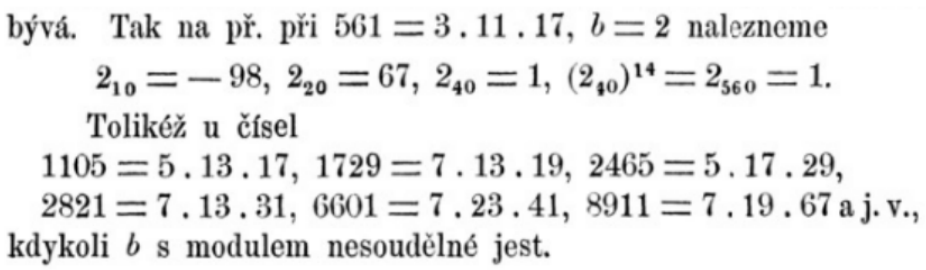
bývá. Tak na př. při $561 = 3 . 11 . 17$, $b = 2$ nalezneme
$2_{10} = -98$, $2_{20} = 67$, $2_{40} = 1$, $(2_{40})^{14} = 2_{560} = 1$.
Tolikéž u čísel
$1105 = 5 . 13 . 17$, $1729 = 7 . 13 . 19$, $2465 = 5 . 17 . 29$,
$2821 = 7 . 13 . 31$, $6601 = 7 . 23 . 41$, $8911 = 7 . 19 . 67$ a j. v.,
kdykoli b s modulem nesoudělné jest.

Рис. 1. Числа Кармайкла, найденные Шимеркой до Кармайкла.

Если запустить тест Ферма t раз, не найдя ни одного свидетеля Ферма (и при том t достаточно велико), можно быть практически уверенным в том, что n или простое или число Кармайкла.[5]

Сформулируем это утверждение на языке теории вероятностей. Если число n составное и не является числом Кармайкла, то Следствие 3.3 гарантирует, что более половины чисел от 2 до $n-1$ являются свидетелями Ферма для n, так что не найти свидетеля Ферма за t тестов настолько же вероятно, как и получить все "решки", подбросив монету t раз: вероятность последнего события равна $1/2^t$. А на самом деле даже *менее вероятно*, потому что доля свидетелей Ферма больше 50%. Поэтому "вероятность" того, что n простое или число Кармайкла, если свидетель Ферма не был найден после t попыток *больше, чем* $1 - 1/2^t$. Это эвристическое рассуждение имеет изъян, связанный с условной вероятностью, который можно устранить при помощи формулы Байеса, но пока обойдёмся без этого.

Подводя итог, **тест Ферма** для числа $n \geq 2$ заключается в следующем:

(1) Выбрать случайное число a от 2 до $n-1$ (при $n = 2$ делать это странно, равно как и применять тест Ферма к $n = 2$).
(2) Проверить $a^{n-1} \equiv 1 \bmod n$.
(3) Если $a^{n-1} \not\equiv 1 \bmod n$, остановить тест и сделать (верное) заключение "n составное." (Мы знаем, что у числа n есть нетривиальный делитель, хотя тест нам его не предъявляет.)
(4) Если $a^{n-1} \equiv 1 \bmod n$, повторить шаг 1.
(5) Если тест продолжается в течение t попыток, мы можем сказать "n простое или число Кармайкла с вероятностью больше, чем $1 - 1/2^t$."

Например, если выполнить тест 10 раз (т.е. $t = 10$) и всякий раз будет выполняться $a^{n-1} \equiv 1 \bmod n$ мы можем сказать, что "n простое или число Кармайкла с вероятностью больше, чем $1 - 1/2^{10} \approx 0,99902$."

Список литературы

[1] W. R. Alford, A. Granville, C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. **139** (1994), 703–722.
[2] R. D. Carmichael, *Note on a New Number Theory Function*, Bulletin Amer. Math. Soc. **16** (1910), 232–238.

[5] Как любит говорить Том Роби (Tom Roby), числа Кармайкла связаны с программой защиты свидетелей Ферма.

[3] R. D. Carmichael, *On composite P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \bmod P$*, Amer. Math. Monthly **19** (1912), 22–27.
[4] V. Šimerka *Zbytky z arithemetické posloupnosti* (*On the remainders of an arithmetic progression*), Časopis pro pěstování matematiky a fysiky **14** (1885), 221–225. URL https://eudml.org/doc/25400.