ПРОВЕРКА ЧИСЕЛ НА ПРОСТОТУ

Проверка чисел на простоту является составной частью алгоритмов генерации простых чисел, используемых в криптографии с открытым ключом. Алгоритмы проверки на простоту можно разделить на вероятностные и детерминированные.

Детерминированный алгоритм всегда действует по одной и той же схеме и гарантированно решает поставленную задачу (или не дает никакого ответа). *Вероятностный* алгоритм использует генератор случайных чисел и дает не гарантированно точный ответ. Вероятностные алгоритмы в общем случае не менее эффективны, чем детерминированные (если используемый генератор случайных чисел всегда дает набор одних и тех же чисел, возможно, зависящих от входных данных, то вероятностный алгоритм становится детерминированным).

5.1. Вероятностные алгоритмы проверки чисел на простоту

Для того чтобы проверить вероятностным алгоритмом, является ли целое число n простым, выбирают случайное число a, $1 < a < n$, и проверяют условие алгоритма. Если число n не проходит тест по основанию a, то алгоритм выдает результат «Число n составное», и число n действительно является составным (рис. 5.1 на стр. 170).

Если же n проходит тест по основанию a, ничего нельзя сказать о том, действительно ли число n является простым. Последовательно проведя ряд проверок таким тестом для разных a и получив для каждого из них ответ «Число n, вероятно, простое», можно утверждать, что число n является простым с вероятностью, близкой к 1. После t независимых

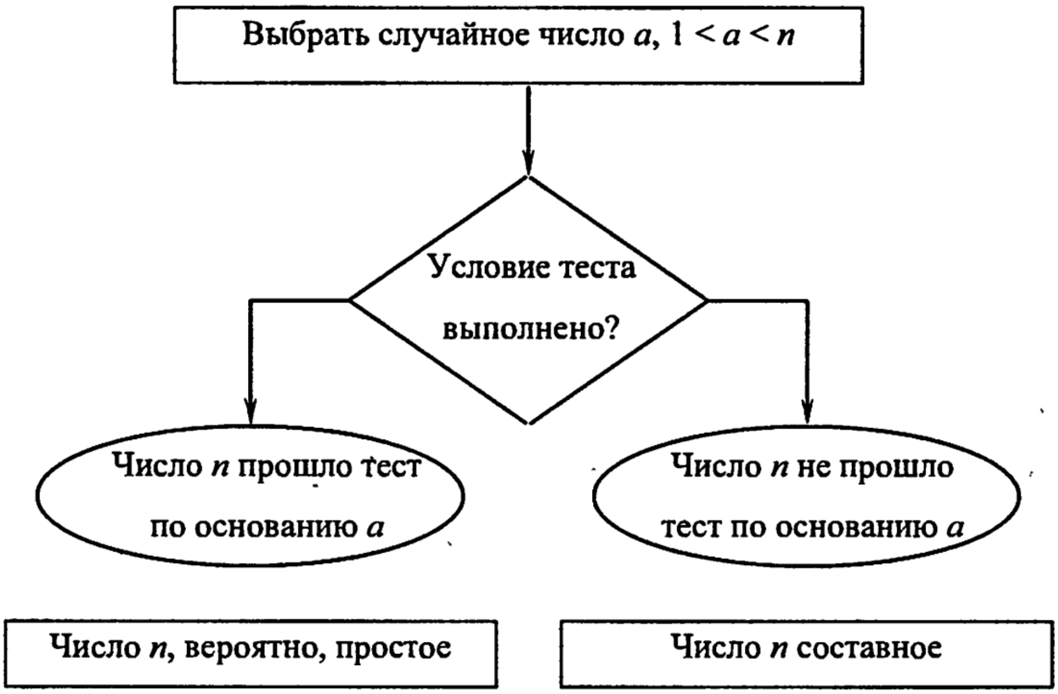

Рис. 5.1. Схема вероятностного алгоритма проверки числа на простоту

выполнений теста вероятность того, что составное число n будет t раз объявлено простым (вероятность ошибки), не превосходит $\frac{1}{2^t}$.

5.1.1. Тест Ферма

Согласно малой теореме Ферма для простого числа p и произвольного целого числа a, $1 \le a \le p - 1$, выполняется сравнение

$$a^{p-1} \equiv 1 \pmod{p}. \qquad (5.1)$$

Следовательно, если для нечетного n существует такое целое a, что $1 \le a < n$, НОД$(a, n) = 1$ и a^{n-1} $1 \pmod{n}$, то число n составное. Отсюда получаем следующий вероятностный алгоритм проверки числа на простоту.

Алгоритм 5.1. Тест Ферма.

Вход. Нечетное целое число $n \geq 5$.

Выход. «Число n, вероятно, простое» или «Число n составное».

1. Выбрать случайное целое число a, $2 \leq a \leq n-2$.
2. Вычислить $r \leftarrow a^{n-1} \pmod{n}$.
3. При $r = 1$ результат: «Число n, вероятно, простое». В противном случае результат: «Число n составное». □

На шаге 1 алгоритма мы не рассматриваем числа $a = 1$ и $a = n - 1$, поскольку $1^{n-1} \equiv 1 \pmod{n}$ для любого целого n и $(n-1)^{n-1} \equiv (-1)^{n-1} \equiv 1 \pmod{n}$ для любого нечетного n.

Сложность теста Ферма равна $O(\log^3 n)$ при умножении «в столбик» и $O(t \log^2 n \log\log n)$ при умножении алгоритмом Шенхаге–Штрассена.

Определение 5.1. Пусть число $n > 0$ нечетное составное и число a произвольное целое, взаимно простое с n, $1 \leq a \leq n-1$. Число n называется *псевдопростым по основанию a*, если выполняется сравнение (5.1), то есть если для числа n алгоритм 5.1 выдает результат «Число n, вероятно, простое».

Пример 5.1. Число $n = 527 = 17 \cdot 31$ является псевдопростым по основаниям 1, 154, 373, 526, поскольку $1^{526} \equiv 154^{526} \equiv 373^{526} \equiv 526^{526} \equiv 1 \pmod{527}$. □

Пример 5.2. Число $n = 629 = 17 \cdot 37$ является псевдопростым по основаниям 1, 38, 149, 154, 186, 191, 290, 302, 327, 339, 438, 443, 475, 480, 591, 628. □

Пример 5.3. В интервале от 8 до 10000 псевдопростыми по основанию 7 являются числа

$$25 = 5^2,\ \ 325 = 5^2 \cdot 13,\ \ 561 = 3 \cdot 11 \cdot 17,\ \ 703 = 19 \cdot 37,$$

$$817 = 19 \cdot 43,\ \ 1105 = 5 \cdot 13 \cdot 17,\ \ 1825 = 5^2 \cdot 73,\ \ 2101 = 11 \cdot 191,$$

$$2353 = 13 \cdot 181,\ \ 2465 = 5 \cdot 17 \cdot 29,\ \ 3277 = 29 \cdot 113,\ \ 4525 = 5^2 \cdot 181,$$

$$4825 = 5^2 \cdot 193,\ \ 6697 = 37 \cdot 181,\ \ 8321 = 53 \cdot 157. \qquad \square$$

Теорема 5.1. Для нечетного составного числа $n > 0$ справедливы следующие утверждения.

1. Число n является псевдопростым по основанию a тогда и только тогда, когда $n - 1$ делится на порядок числа a по модулю n.

2. Если число n псевдопростое по основаниям a и b, то n псевдопростое по основаниям $ab \pmod n$, $ab^{-1} \pmod n$ и $a^{-1}b \pmod n$.

3. Если число n не является псевдопростым хотя бы по одному основанию a, то n является псевдопростым не более чем по $\frac{\varphi(n)}{2}$ основаниям, где φ — функция Эйлера.

Доказательство. Если d — порядок числа a по модулю n и $n - 1 = kd$ для некоторого целого числа k, то, возводя обе части сравнения $a^d \equiv 1 \pmod n$ в степень k, получаем соотношение (5.1).

Обратно, пусть число n псевдопростое по основанию a, то есть $a^{n-1} \equiv 1 \pmod n$, и d — порядок числа a по модулю n. Разделим $n - 1$ с остатком на d: $n - 1 = qd + r$ для некоторых целых неотрицательных чисел q и r, тогда

$$1 \equiv a^{n-1} = a^{qd+r} = (a^d)^q \cdot a^r \equiv a^r \pmod n.$$

Но d — наименьшая степень, в которой a сравнимо с 1 по модулю n. Значит, $r = 0$ и $n - 1$ делится на d. Первое утверждение доказано.

Если $a^{n-1} \equiv 1 \pmod n$ и $b^{n-1} \equiv 1 \pmod n$, то, перемножая почленно эти сравнения, получаем $(ab)^{n-1} \equiv 1 \pmod n$. А из сравнения $a^{n-1} \equiv b^{n-1} \pmod n$ получаем $(ab^{-1})^{n-1} \equiv (a^{-1}b)^{n-1} \equiv 1 \pmod n$. Второе утверждение доказано.

Докажем утверждение 3. Пусть $\{a_1, a_2, \dots, a_k\}$ — множество всех тех оснований, по которым число n является псевдопростым, то есть $1 \le a_i \le n-1$, НОД$(a_i, n) = 1$ и $a_i^{n-1} \equiv 1 \pmod n$ для $1 \le i \le k$ (это множество непусто, поскольку хотя бы числа 1 и $n-1$ ему принадлежат). Пусть a — такое основание, по которому n не является псевдопростым, то есть $1 \le a \le n-1$, НОД$(a, n) = 1$ и $a^{n-1} \not\equiv 1 \pmod n$. Рассмотрим числа $b_1 \equiv aa_1 \pmod n$, $b_2 \equiv aa_2 \pmod n$, …, $b_k \equiv aa_k \pmod n$ и предположим, что число n является псевдопростым по основанию b_i хотя бы для одного i, $1 \le i \le k$. Тогда, согласно утверждению 2, число n является псевдопростым и по основанию $ba_i^{-1} \equiv (aa_i)a_i^{-1} \equiv a \pmod n$, а это не так. Следовательно, число n не является псевдопростым ни по одному из k различных оснований b_1, b_2, …, b_k. Таким образом, чисел, удовлетворяющих сравнению (5.1), по крайней мере не больше, чем чисел, которые этому сравнению не удовлетворяют, а из условия НОД$(a_i, n) = 1$ получаем, что их не больше, чем $\frac{\varphi(n)}{2}$. □

Из утверждения 3 следует, что если число n не является псевдопростым хотя бы по одному основанию, то оно не является псевдопростым по крайней мере по $\frac{n-1}{2}$ основаниям.

Для любого числа $a > 1$ существует бесконечно много чисел, псевдопростых по основанию a.

Пример 5.4. Покажем, что если число n псевдопростое по основанию 2, то число $2^n - 1$ тоже псевдопростое по основанию 2. Действительно, пусть $2^{n-1} \equiv 1 \pmod n$, то есть $2^{n-1} - 1 = kn$ для некоторого целого числа k. Тогда

$$2^{2^n-2} = 2^{2(2^{n-1}-1)} = 2^{2kn} = (2^n)^{2k} \equiv 1^{2k} = 1 \pmod{2^n - 1}.$$

Таким образом, существует бесконечно много чисел, псевдопростых по основанию 2. □

Определение 5.2. Нечетные составные числа n, для которых сравнение (5.1) выполняется при любом a, $1 \le a \le n-1$, взаимно простом с n, называются *числами Кармайкла* (R.D. Carmichael). Для этих чисел тест Ферма всегда выдает результат «Число n, вероятно, простое».

Пример 5.5. Самое маленькое число Кармайкла — $561 = 3 \cdot 11 \cdot 17$. Еще несколько чисел Кармайкла: $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, $6601 = 7 \cdot 23 \cdot 41$, $29341 = 13 \cdot 37 \cdot 61$, $41041 = 7 \cdot 11 \cdot 13 \cdot 41$, $278545 = 5 \cdot 17 \cdot 29 \cdot 113$, $949803513811921 = 17 \cdot 31 \cdot 191 \cdot 433 \cdot 21792241$, $651693055693681 = 72931 \cdot 87517 \cdot 102103$. □

Теорема 5.2 (критерий Корселта). Нечетное составное число n является числом Кармайкла тогда и только тогда, когда:

1) n свободно от квадратов;

2) для каждого простого делителя p числа n число $n-1$ делится на $p-1$.

Следствие. Любое число Кармайкла является произведением не менее трех различных простых чисел.

Замечание. Условие 2 в теореме 5.2 можно переписать так: число $n-1$ должно делиться на НОК(p_1-1, p_2-1, …, p_s-1). Отсюда получаем следующий способ генерации чисел Кармайкла.

Пример 5.6. Рассмотрим простые числа вида $p_1 = 6k+1$, $p_2 = 12k+1$, $p_3 = 18k+1$ (например, при $k=1$ получаем $p_1 = 7$, $p_2 = 13$, $p_3 = 19$). Докажем, что число $n = p_1p_2p_3$ является числом Кармайкла.

Согласно малой теореме Ферма, для любого числа a, взаимно простого с p_1, выполняется сравнение $a^{6k} \equiv 1 \pmod{p_1}$. Аналогично, $a^{12k} \equiv 1 \pmod{p_2}$, $a^{18k} \equiv 1 \pmod{p_3}$. Число $36k$ является наименьшим общим кратным чисел $6k$, $12k$ и $18k$, тогда по китайской теореме об остатках $a^{36k} \equiv 1 \pmod{n}$ для всех чисел a, взаимно простых с n. Но $n-1 = 1296k^2 + 396k + 36k = 36k(36k^2 + 11k + 1)$, значит, $a^{n-1} \equiv 1 \pmod{n}$ для всех чисел a, взаимно простых с n. □

Для генерации чисел Кармайкла общего вида можно воспользоваться следующим алгоритмом [7].

Алгоритм 5.2. Алгоритм Эрдеша (1956).

Вход. Сильно составное число $m > 0$.

Выход. Число Кармайкла.

1. Составить множество S простых чисел p, для которых m делится на $p-1$ и НОД(m, p) = 1.
2. Из множества S выбрать такие числа $p_1, p_2, \ldots, p_r$, $r \geq 3$, для которых $p_1p_2\ldots p_r \equiv 1 \pmod{m}$.
3. Положить $n \leftarrow p_1p_2\ldots p_r$.
4. Результат: n. □

П р и м е р 5.7. Пусть $m = 120 = 2^3 \cdot 3 \cdot 5$. Составляем множество $S = \{7, 11, 13, 31, 41, 61\}$. Чем больше множество S, тем больше чисел Кармайкла, возможно, нам удастся построить. Перебирая всевозможные произведения элементов множества S, получаем:

$$41041 = 7 \cdot 11 \cdot 13 \cdot 41 \equiv 1 \pmod{120},$$

$$172081 = 7 \cdot 13 \cdot 31 \cdot 61 \equiv 1 \pmod{120},$$

$$852841 = 11 \cdot 31 \cdot 41 \cdot 61 \equiv 1 \pmod{120},$$

— числа Кармайкла. □

Наиболее трудоемким в алгоритме Эрдеша является шаг 2. Следующая модификация этого шага, предложенная в 1994 году У. Альфордом (W. Alford), делает этот алгоритм пригодным для практического использования.

3.1. Найти такое подмножество $P \subseteq S$, что для любого числа a, $1 \le a \le m$, взаимно простого с m, найдутся числа $p_1, p_2, \ldots, p_r \in P$, для которых $p_1 p_2 \ldots p_r \equiv a \pmod{m}$.

3.2. Для любых чисел $q_1, q_2, \ldots, q_t \in S \setminus P$ вычислить $a \equiv (q_1 q_2 \ldots q_t)^{-1} \pmod{m}$. Тогда $p_1 p_2 \ldots p_r q_1 q_2 \ldots q_t$ — число Кармайкла.

Выбор множества P на шаге 3.1 можно выполнить так. Пусть элементы множества S упорядочены по возрастанию: $p_1 < p_2 < \ldots$. Обозначим R_j множество всевозможных произведений чисел $p_1, p_2, \ldots, p_j$ по модулю m. Множества R_j задаются рекуррентным соотношением $R_{j+1} = R_j \cup \{sp_{j+1} \pmod{m} \mid s \in R_j\}$. Тогда в качестве P нужно взять то множество R_j, которое представляет собой приведенную систему вычетов по модулю m: $R_j = \{a \mid 1 \le a \le m, \text{НОД}(a, m) = 1\}$.

На шаге 3.2 получаем $p_1p_2\ldots p_r \equiv a \equiv (q_1q_2\ldots q_t)^{-1} \pmod m$, откуда $p_1p_2\ldots p_rq_1q_2\ldots q_t \equiv 1 \pmod m$ — число Кармайкла, согласно шагу 2 алгоритма Эрдеша. Рассмотренный алгоритм позволяет найти $2^{\#(S\setminus P)} - 1$ чисел Кармайкла.

Приведем без доказательства еще один интересный критерий распознавания чисел Кармайкла. Нечетное составное число n, свободное от квадратов, является числом Кармайкла тогда и только тогда, когда оно делит знаменатель числа Бернулли B_{n-1} (числа Бернулли определяются из рекуррентного соотношения: $B_0 = 1$, $\sum_{k=0}^{n-1} \frac{n!}{k!(n-k)!} B_k = 0$ при $n \geq 1$). Например, для числа Кармайкла $n = 1105$ число Бернулли B_{1104} отрицательно, числитель имеет длину 2012 десятичных знаков, знаменатель равен

$$83985438810 = 1105 \cdot 76004922.$$

Числа Кармайкла встречаются довольно редко. От 1 до 10^5 всего 16 чисел Кармайкла: 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361. От 1 до $2{,}5 \cdot 10^{10}$ всего 2163 чисел Кармайкла; от 1 до 10^{15} всего 105212 чисел Кармайкла.

В то же время чисел Кармайкла бесконечно много: для любого достаточно большого n справедливо неравенство

$$n^{\frac{2}{7}} < C(n) < n \exp\left(-\frac{\ln n \ln\ln\ln n}{\ln\ln n}\right),$$

где $C(n)$ — количество чисел Кармайкла, меньших n [6].

Если n является числом Кармайкла и все его простые делители достаточно велики, то с большой вероятностью тест Ферма объявит n простым даже при большом числе итераций. Если в тесте Ферма использовать не случайные, а заранее определенные основания a, то его можно «обмануть» выбором соответствующего числа Кармайкла. Этот недостаток теста Ферма устраняется следующими тестами с более жесткими критериями.