5.1.4. Генерация простого числа

Существуют различные алгоритмы генерации простых чисел (см., например, работы [1, 5]). Многие из них вырабатывают числа, обладающие специальными свойствами. Рассмотрим способ генерации, использующий вероятностные алгоритмы проверки чисел на простоту.

Алгоритм 5.5. Генерация простого числа.

Вход. Разрядность k искомого числа p; параметр $t \geq 1$.

Выход. Число p, простое с вероятностью не менее $1 - \frac{1}{4^t}$.

1. Сгенерировать случайное k-битное число $p = (b_{k-1}b_{k-2}\ldots b_0)_2$.
2. Положить $b_{k-1} = 1$, $b_0 = 1$.
3. Проверить, что p не делится на простые числа 3, 5, 7, … .
4. Для $i = 1, 2, \ldots, t$ выполнить следующие действия.
   4.1. Выбрать случайное число a, $2 \leq a \leq p - 2$.
   4.2. Проверить число p тестом Миллера–Рабина для основания a. Если число p прошло тест, то вернуться на шаг 4.1. В противном случае вернуться на шаг 1.
5. Результат: p. □

Равенство $b_{k-1} = 1$ на шаге 2 гарантирует, что длина числа p в точности равна k бит, равенство $b_0 = 1$ обеспечивает нечетность числа p.

Число проверок на шаге 3 на практике варьируется от 256 до 2000. При проверке чисел 3, 5, 7 отбраковываются 54% нечетных составных чисел, при проверке простых чисел, меньших 100, — 76%, при проверке простых чисел, меньших 256, — 80%. Однако чем больше n и чем больше чисел мы проверяем, тем дольше шаг 3.

5.2. Детерминированные алгоритмы проверки чисел на простоту

Детерминированные тесты можно назвать тестами, *доказывающими* простоту. Эти тесты вычислительно более сложны, чем вероятностные, поэтому, прежде чем проверять число детерминированным тестом, необходимо проверить его, например, тестом Миллера–Рабина.

Всякий детерминированный тест, по сути, представляет собой доказательство теоремы о достаточном условии простоты числа. Поэтому числа, которые считаются простыми на основании прохождения ими детерминированного теста, называются *доказуемо простыми*.

Детерминированные тесты можно использовать и для генерации простых чисел. Для этого выбирают некоторую последовательность чисел специального вида, среди которых нужно найти простое число, и к каждому из этих чисел применяют детерминированный тест.

В некоторых детерминированных тестах используются случайные числа. Однако, в отличие от тестов Ферма, Соловэя–Штрассена или Миллера–Рабина, эти тесты дают ответ «Число n простое» или «Число n, вероятно, составное». Поэтому при проверке чисел на простоту можно параллельно выполнять какой-либо вероятностный и детерминированный тест до тех пор, пока один из них не даст определенный ответ.

5.2.1. Проверка чисел Мерсенна

Определение 5.5. Пусть $s \geq 2$ — целое число. *Числом Мерсенна* называется целое число $M_s = 2^s - 1$, где число s простое. Если число $2^s - 1$ простое, то оно называется *простым числом Мерсенна*.

Критерием простоты чисел Мерсенна служит следующее утверждение.

Теорема 5.9 (Люка–Лемер). Число Мерсенна $M_s = 2^s - 1$, где $s \geq 3$ — нечетное число, является простым тогда и только тогда, когда

1) число s простое;

2) выполняется сравнение $L_{s-2} \equiv 0 \pmod{M_s}$, где последовательность $\{L_k\}$ формируется по следующему правилу: $L_0 = 4$, $L_{k+1} \equiv L_k^2 - 2 \pmod{M_s}$ при $k \geq 0$.

Доказательство см., например, в работах [3, 4].

Это условие простоты числа Мерсенна было открыто Э. Люка в конце 1890-х годов, а в данной формулировке приведено около 1930 года в работах Д. Лемера. Теорема 5.9 положена в основу следующего алгоритма проверки числа Мерсенна на простоту.

Алгоритм 5.6. Алгоритм Люка–Лемера.

Вход. Число Мерсенна $M_s = 2^s - 1$, $s \geq 3$.

Выход. «Число M_s простое» или «Число M_s составное».

1. Методом пробного деления проверить, есть ли у числа s делители от 2 до $\left\lfloor \sqrt{s} \right\rfloor$. Если есть, то результат: «Число M_s составное».

2. Положить $L = 4$.

3. Для $k = 1, 2, \ldots, s - 2$ вычислять $L \leftarrow L^2 - 2 \pmod{M_s}$.

4. При $L = 0$ результат: «Число M_s простое». В противном случае результат: «Число M_s составное». □

Пример 5.16. Пусть $s = 11$ — простое число. Проверим, будет ли простым число $2^{11} - 1 = 2047$.

Строим последовательность L_i:

$L_0 = 4$, $L_1 = 4^2 - 2 = 14$, $L_2 = 14^2 - 2 = 194$,

$L_3 = 194^2 - 2 \equiv 788 \pmod{2047}$, $L_4 = 788^2 - 2 \equiv 701 \pmod{2047}$,

$L_5 = 701^2 - 2 \equiv 119 \pmod{2047}$, $L_6 = 119^2 - 2 \equiv 1877 \pmod{2047}$,

$L_7 = 1877^2 - 2 \equiv 240 \pmod{2047}$, $L_8 = 240^2 - 2 \equiv 282 \pmod{2047}$,

$L_9 = 282^2 - 2 \equiv 1736 \quad 0 \pmod{2047}$.

Значит, число 2047 составное. И в самом деле, $2047 = 23 \cdot 89$. □

Пример 5.17. Пусть $s = 13$ — простое число. Проверим, будет ли простым число $2^{13} - 1 = 8191$.

Строим последовательность L_i:

$L_0 = 4$, $L_1 = 4^2 - 2 = 14$, $L_2 = 14^2 - 2 = 194$,

$L_3 = 194^2 - 2 \equiv 4870 \pmod{8191}$, $L_4 = 4870^2 - 2 \equiv 3953 \pmod{8191}$,

$L_5 = 3953^2 - 2 \equiv 5970 \pmod{8191}$, $L_6 = 5970^2 - 2 \equiv 1857 \pmod{8191}$,

$L_7 = 1857^2 - 2 \equiv 36 \pmod{8191}$, $L_8 = 36^2 - 2 = 1294$,

$L_9 = 1294^2 - 2 \equiv 3470 \pmod{8191}$, $L_{10} = 3470^2 - 2 \equiv 128 \pmod{8191}$,

$L_{11} = 128^2 - 2 = 16382 \equiv 0 \pmod{8191}$.

Значит, число 8191 простое. □

В настоящее время неизвестно, конечно ли число простых чисел Мерсенна. В таблице 4.1 приведены известные на сегодняшний день простые числа Мерсенна (d_p означает число десятичных разрядов в числе M_p; 39?–42? означает, что неизвестно, есть ли еще простые числа Мерсенна между $2^{6972593} - 1$ и этими числами; см. также www.mersenne.org).

Таблица 5.1

Простые числа Мерсенна

№ п/п	p	d_p	Год открытия	Автор и год опубликования	Компьютер
1	2	1	–	–	
2	3	1	–	–	
3	5	2	–	–	
4	7	3	–	–	
5	13	4	1456[1]	Reguis, 1536; Pietro Cataldi, 1603	
6	17	6	1588	Pietro Cataldi, 1603	
7	19	6	1588	Pietro Cataldi, 1603	
8	31	10	1750	Leonhard Euler, 1772	
9	61	19	1883	Иван Михеевич Первушин 1883; Paul P. Seelhoff, 1886	
10	89	27	1911	Raymond E. Powers, 1911	
11	107	33	1913	Raymond E. Powers, 1914	
12	127	39	1876	François Lucas, 1876	
13	521	157	1952	Raphael M. Robinson, 1952	SWAC
14	607	183	1952	Derrick H. Lehmer, 1952–53; Raphael M. Robinson, 1952	SWAC
15	1279	386	1952	Derrick H. Lehmer,	SWAC

[1] По другим источникам, 1461 г.

№ п/п	p	d_p	Год открытия	Автор и год опубликования	Компьютер
				1952–53; Raphael M. Robinson, 1952	
16	2203	664	1952	Derrick H. Lehmer, 1952–53; Raphael M. Robinson, 1952	SWAC
17	2281	687	1952	Derrick H. Lehmer, 1952–53; Raphael M. Robinson, 1952	SWAC
18	3217	969	1957	Hans Riesel, 1957	BESK
19	4253	1281	1961	Alexander Hurwitz, John L. Selfridge, 1961	IBM 7090
20	4423	1332	1961	Alexander Hurwitz, John L. Selfridge, 1961	IBM 7090
21	9689	2917	1963	Donald B. Gillies, 1964	ILLIAC 2
22	9941	2993	1963	Donald B. Gillies, 1964	ILLIAC 2
23	11213	3376	1963	Donald B. Gillies, 1964	ILLIAC 2
24	19937	6002	1971	Bryant Tuckerman, 1971	IBM 360/91
25	21701	6533	1978	Landon C. Noll, Laura A. Nickel, 1980	Cyber 174
26	23209	6987	1979	Landon C. Noll, 1980	Cyber 174
27	44497	13395	1979	Harry L. Nelson, David Slowinski, 1979	Cray 1
28	86243	25962	1982	David Slowinski, 1982	Cray 1
29	110503	33265	1988	Walter N. Colquitt, Luther Welsh, Jr., 1991	SGI

№ п/п	p	d_p	Год открытия	Автор и год опубликования	Компьютер
30	132049	39751	1983	David Slowinski, 1988	Cray X-MP
31	216091	65050	1985	David Slowinski, 1989	Cray X-MP
32	756839	227832	1992	David Slowinski, Paul Gage, 1992	Cray 2
33	859433	258716	1994	David Slowinski, Paul Gage, 1994	Cray C90
34	1257787	378632	1996	David Slowinski, Paul Gage	Cray T94
35	1398269	420921	1996	Joel Armengaud, George F. Woltman и др. (GIMPS)	Pentium 90
36	2976221	895932	1997	Gordon Spence, George F. Woltman и др. (GIMPS)	Pentium 100
37	3021377	909526	1998	Roland Clarkson, George F. Woltman, Scott Kurowski и др. (GIMPS, PrimeNet)	Pentium 200
38	6972593	2098960	1999	Nayan Hajratwala, George F. Woltman, Scott Kurowski и др. (GIMPS, PrimeNet)	Pentium II 350
39?	13466917	4053946	2001	Michael Cameron, George F. Woltman, Scott Kurowski и др. (GIMPS, PrimeNet)	AMD T-Bird 800
40?	20996011	6320430	2003,	Michael Shafer,	Pentium 4,

№ п/п	p	d_p	Год открытия	Автор и год опубликования	Компьютер
			19 ноября	George F. Woltman, Scott Kurowski и др. (GIMPS, PrimeNet)	2 ГГц
41?	24036583	7235733	2004, 1 июня	Josh Findley и др. (GIMPS, PrimeNet)	Pentium 4, 2,4 ГГц
42?	25964951	7816230	2005, 18 февраля	Martin Nowak, George F. Woltman, Scott Kurowski и др. (GIMPS, PrimeNet)	Pentium 4, 2,4 ГГц

Числа Мерсенна M_s обладают тем свойством, что число $M_s + 1$ является сильно составным. Следующая теорема позволяет проверять на простоту произвольное число n, для которого известно разложение числа $n + 1$.

Теорема 5.10. Пусть целые числа p и q взаимно просты и пусть последовательность $\{U_i\}$ определяется соотношениями $U_0 = 0$, $U_1 = 1$, $U_{i+1} = pU_i - qU_{i-1}$ при $i \geq 1$. Положительное нечетное число n является простым, если выполнены следующие условия:

1) $p^2 - 4q$ — квадратичный невычет по модулю n;

2) $U_{n+1} \equiv 0 \pmod{n}$;

3) $U_{(n+1)/r} \not\equiv 0 \pmod{n}$ для всех простых делителей r числа $n + 1$.

Доказательство см. в работе [5].

Пример 5.18. Пусть $n = 350657$. Разложим на множители число $n + 1$:

$$350658 = 2 \cdot 3^2 \cdot 7 \cdot 11^2 \cdot 23.$$

Выберем $p=3$, $q=5$, то есть $p^2-4q=3^2-4\cdot 5=-11$, тогда $\left(\frac{-11}{n}\right)=-1$, и первое условие теоремы выполнено.

Строим последовательность $\{U_i\}$: $U_0=0$, $U_1=1$, $U_2=3$, ..., $U_{n-1}\equiv 280525 \pmod n$, $U_n\equiv 350656 \pmod n$, $U_{n+1}\equiv 0 \pmod n$. Второе условие теоремы выполнено.

Проверяем третье условие:

$$U_{(n+1)/2}\equiv 7281 \pmod n, \quad U_{(n+1)/3}\equiv 155139 \pmod n,$$
$$U_{(n+1)/7}\equiv 299210 \pmod n, \quad U_{(n+1)/11}\equiv 306723 \pmod n,$$
$$U_{(n+1)/23}\equiv 51824 \pmod n.$$

Следовательно, число 350657 простое. □

5.2.2. Проверка с использованием разложения числа $n-1$

Ряд критериев проверки на простоту основан на знании частичного или полного разложения числа $n-1$.

Лемма 5.11. Пусть целое число $n\geq 3$ имеет вид $n=q^sR+1$, где число q простое и R не делится на q. Если существует такое a, что $a^{n-1}\equiv 1 \pmod n$ и НОД$(a^{(n-1)/q}-1, n)=1$, то для любого простого делителя p числа n выполняется сравнение $p\equiv 1 \pmod{q^s}$.

Доказательство. Пусть p — простой делитель числа n. Тогда из $a^{n-1}\equiv 1 \pmod n$ следует, что $a^{n-1}\equiv 1 \pmod p$, то есть число $n-1=q^sR$ делится на порядок d числа a по модулю p.

Условие НОД$(a^{(n-1)/q}-1, n)=1$ означает, что $a^{(n-1)/q}\not\equiv 1 \pmod p$. Следовательно, число $q^{s-1}R$ на d не делится. Значит, d делится на q^s.

Согласно малой теореме Ферма, $a^{p-1}\equiv 1 \pmod p$, то есть $p-1$ делится на d, а значит, и на q^s. □

Теорема 5.12 (Поклингтон). Пусть целое число $n \geq 3$ имеет вид $n = QR + 1$, где НОД$(Q, R) = 1$, $R < Q$ и $Q = \prod_{j=1}^{t} q_j^{\alpha_j}$ — каноническое разложение числа Q. Если для каждого q_j существует целое число a_j, для которого $a_j^{n-1} \equiv 1 \pmod{n}$ и НОД$(a_j^{(n-1)/q_j} - 1, n) = 1$, то число n простое.

Пример 5.19. Покажем, как можно генерировать простые числа, используя теорему Поклингтона [1]. Пусть нужно найти простое число длины 8 десятичных знаков.

Выберем произвольное простое число $q_1 \geq 5$, например $q_1 = 19$, и выберем четное число R из интервала $[2, q_1 - 3] = [2, 16]$. Пусть $R = 12$. Положим $n = q_1 R + 1 = 19 \cdot 12 + 1 = 229$. Тогда, согласно теореме Поклингтона, чтобы n было простым, достаточно найти одно целое число a, для которого $a^{n-1} \equiv 1 \pmod{n}$ и НОД$(a^R - 1, n) = 1$. Этим условиям удовлетворяет, например, $a = 2$.

Обозначим $q_2 = n = 229$. Выберем четное число R из интервала $[2, q_2 - 3] = [2, 226]$. Пусть $R = 224$. Положим $n = q_2 R + 1 = 229 \cdot 224 + 1 = 51297$. Но при $a = 2$ получаем $a^{n-1} \equiv 4 \pmod{n}$. Это означает, что число n составное и нужно выбрать другое R. При $R = 222$ получаем $n = 50839$ и условия теоремы выполнены.

Полагаем $q_3 = n = 50839$. При $R = 300$ получаем $n = q_3 R + 1 = 50839 \cdot 300 + 1 = 15251701$. Условия теоремы выполнены, и число 15251701 — простое, требуемой длины.

Отметим, что здесь на каждом шаге неравенство $q_i \geq \sqrt{n}$ выполнено, поскольку

$$n = q_i R + 1 \leq q_i(q_i - 3) + 1 = q_i^2 - 3q_i + 1 \leq q_i^2 - 3 \cdot 5 + 1 < q_i^2. \qquad \square$$

Приведем без доказательства еще один критерий [5, 9], позволяющий судить о простоте числа n, зная разложение делителя числа $n-1$.

Пусть $n \geq 3$ — целое число вида $n = 2QR + 1$, где $Q = \prod_{j=1}^{t} q_j^{\alpha_j} \geq \sqrt[3]{n}$, $2R = xQ + y$, $x \geq 0$, $0 \leq y < Q$ и число $y^2 - 4x \neq 0$ не является полным квадратом. Если найдется целое число a, для которого $a^{n-1} \equiv 1 \pmod{n}$ и $\text{НОД}(a^{(n-1)/q_j} - 1, n) = 1$ для всех $1 \leq j \leq t$, то число n простое.

Пример 5.20. Пусть $n = 15486433 = 2QR + 1$, где $Q = 624 = 2^4 \cdot 3 \cdot 13 \geq \sqrt[3]{n} \approx 249{,}26$, $R = 12409$. Поделив с остатком $2R$ на Q, получим $24818 = 39 \cdot 624 + 482$, то есть $x = 39$, $y = 482$.

Вычисляем $y^2 - 4x = 482^2 - 4 \cdot 39 = 232168$ — делится на 2^3, а значит, не является полным квадратом.

При $a = 5$ получаем $a^{n-1} \equiv 1 \pmod{n}$ и

$$\text{НОД}(a^{7743216} \pmod{n}, n) = \text{НОД}(15486432, n) = 1,$$

$$\text{НОД}(a^{5162144} \pmod{n}, n) = \text{НОД}(8511400, n) = 1,$$

$$\text{НОД}(a^{1191264} \pmod{n}, n) = \text{НОД}(6618795, n) = 1,$$

значит, число 15486433 простое. □

Другой класс чисел специального вида — *числа Ферма* $F_k = 2^{2^k} + 1$. Еще в 1640 году П. Ферма предположил, что все такие числа являются

простыми. Однако на сегодняшний день известно лишь пять простых чисел Ферма: $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$.

Теорема 5.13 (Пепин). При $k \geq 1$ число Ферма F_k является простым тогда и только тогда, когда $3^{\frac{F_k-1}{2}} \equiv -1 \pmod{F_k}$.

Доказательство. Если число F_k простое, то по свойству 3 символа Лежандра

$$3^{\frac{F_k-1}{2}} \equiv \left(\frac{3}{F_k}\right) \pmod{F_k}.$$

Вычисляем

$$\left(\frac{3}{F_k}\right) = (-1)^{\frac{F_k-1}{2}} \left(\frac{F_k}{3}\right) = \left(\frac{2^{2^k}+1}{3}\right) = \left(\frac{(-1)^{2^k}+1}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Чтобы доказать достаточность, полагаем в теореме Поклингтона $Q = 2^{2^k}$, $R = 1$ и $a = 3$. □

Заметим, что вместо числа 3 в условиях теоремы 5.13 можно взять любой квадратичный невычет по модулю F_k, например 5 или 10.