Math-Net.Ru

Общероссийский математический портал

Е. В. Садовник, Проверка на простоту чисел вида $N = 2kp_1^{m_1}p_2^{m_2}\cdots p_n^{m_n} - 1$, *Дискрет. матем.*, 2008, том 20, выпуск 2, 15–24

DOI: <https://doi.org/10.4213/dm1000>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.157.27.8

26 апреля 2023 г., 16:21:22

Проверка на простоту чисел вида

$$N = 2k p_1^{m_1} p_2^{m_2} \dots p_n^{m_n} - 1$$

© 2008 г. Е. В. Садовник

Предлагается алгоритм проверки чисел вида $N = 2k p_1^{m_1} p_2^{m_2} \dots p_n^{m_n} - 1$ на простоту, где $2k < p_1^{m_1} p_2^{m_2} \dots p_n^{m_n}$, k — нечетное натуральное число, p_i — простое число, $i = 1, \dots, n$, и $p_1 p_2 \dots p_n \equiv 3 \pmod{4}$. Для построения алгоритма используются функции Люка. Приведенный алгоритм имеет сложность $\tilde{O}(\log^2 N)$.

1. Введение

В [1] Е. Люка предложил эффективный инструмент для проверки простоты числа N , если известно полное или частичное разложение числа $N + 1$ на множители. Используя функции, впоследствии названные его именем, он показал, как проверить на простоту числа Мерсенна (числа вида $2^n - 1$) за полиномиальное время. В дальнейшем с помощью функций Люка были получены тесты определения простоты чисел вида $A5^n - 1$, $A7^n - 1$ [2] и других.

Несмотря на то, что в 2002 году в [3] был предложен полиномиальный алгоритм определения простоты любого натурального числа, применение функций Люка для проверки простоты чисел до сих пор актуально. Это связано с тем, что тесты, основанные на функциях Люка, работают гораздо быстрее. Так, предложенный в данной работе алгоритм проверки числа $N = 2k p_1^{m_1} p_2^{m_2} \dots p_n^{m_n} - 1$ на простоту имеет сложность всего $\tilde{O}(\log^2 N)$.

2. Основные определения

Напомним определения из теории чисел [4]. Целые числа a и b сравнимы по модулю p , если существует такое целое c , что $a = b + cp$. В этом случае пишут $a \equiv b \pmod{p}$. Если число a является делителем числа b , то будем говорить, что a делит b и писать $a \mid b$, а если a не является делителем числа b , то будем писать $a \nmid b$. Запись $a^p \parallel b$ означает, что $a^p \mid b$ и $a^{p+1} \nmid b$. Наибольший общий делитель c натуральных чисел a и b обозначается $c = (a, b)$.

Пусть p — простое число. Тогда число $a \in \{1, 2, \dots, p-1\}$ называется квадратичным вычетом (невычетом) по модулю p , если сравнение $x^2 \equiv a \pmod{p}$ имеет (соответственно, не имеет) решений.

Символ Лежандра числа a относительно простого числа p — это число $\left(\frac{a}{p}\right)$, равное 1, если a — квадратичный вычет по модулю p , и равное -1 , если a — квадратичный невычет по модулю p (если $a \equiv 0 \pmod{p}$, то будем считать, что символ Лежандра равен нулю).

Символ Лежандра обладает следующими свойствами [5]:

$$\begin{aligned} \left(\frac{a}{p}\right) &= a^{(p-1)/2} \pmod{p}, & \left(\frac{1}{p}\right) &= 1, \\ \left(\frac{a_1 a_2 \dots a_k}{p}\right) &= \left(\frac{a_1}{p}\right) \left(\frac{a_2}{p}\right) \dots \left(\frac{a_k}{p}\right), & \left(\frac{p}{q}\right) &= (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right), \\ \left(\frac{ab^2}{p}\right) &= \left(\frac{a}{p}\right), & \left(\frac{2}{p}\right) &= (-1)^{(p^2-1)/8}, \end{aligned}$$

где p и q — различные простые числа.

Пусть $P = p_1 p_2 \dots p_k$ — каноническое разложение числа P на простые множители и число a взаимно просто с P . Тогда символом Якоби называется число

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_k}\right).$$

Для символа Якоби выполняются все перечисленные свойства, которым удовлетворяет символ Лежандра.

3. Функции Люка

Основным инструментом, используемым в данной статье для проверки чисел на простоту, являются функции Люка [1].

Пусть P и Q — два взаимно простых числа, а α и β — корни квадратного уравнения

$$x^2 - Px + Q = 0. \quad (1)$$

Функции Люка [1] определяются формулами

$$\begin{aligned} V_n(P, Q) &= \alpha^n + \beta^n, \\ U_n(P, Q) &= (\alpha^n - \beta^n)/(\alpha - \beta). \end{aligned}$$

Если $\delta = (\alpha - \beta)$ и $\Delta = (\alpha - \beta)^2$, то $\Delta = P^2 - 4Q$ является дискриминантом уравнения (1), и если $\Delta = 0$, то

$$U_n(P, Q) = \lim_{\beta \rightarrow \alpha} (\alpha^n - \beta^n)(\alpha - \beta) = n\alpha^{n-1}.$$

Отметим, что функции Люка всегда целые при $n \geq 0$ и удовлетворяют большому числу интересных тождеств, которые легко выводятся из определения [1]:

$$V_n^2 - \Delta U_n^2 = 4Q^n, \quad (2)$$

$$V_0 = 2, \quad U_0 = 0, \quad V_1 = P, \quad U_1 = 1, \quad (3)$$

$$2V_{n+1} = PV_n + \Delta U_n, \quad 2U_{n+1} = V_n + PU_n, \quad (4)$$

$$V_{m+n} = V_n V_m - Q^n V_{m-n}, \quad U_{m+n} = V_n U_m - Q^n U_{m-n}, \quad (5)$$

$$2V_{m+n} = V_n V_m + \Delta U_n U_m, \quad 2U_{m+n} = U_n V_m + V_n U_m, \quad (6)$$

$$V_{2n} = V_n^2 - 2Q^n, \quad U_{2n} = U_n V_n, \quad (7)$$

$$V_{3n} = V_n(V_n^2 - 3Q^n), \quad U_{3n} = U_n(V_n^2 - Q^n), \quad (8)$$

$$\delta\alpha^n U_m = V_n\alpha^n - Q^m V_{n-m}, \quad (9)$$

$$\frac{V_n + \sqrt{\Delta}U_n}{2} = \left(\frac{P + \sqrt{\Delta}}{2} \right)^n. \quad (10)$$

В дальнейшем мы будем рассматривать функции Люка по модулю некоторого натурального числа N . В этом случае требование взаимной простоты чисел P и Q не является обязательным. Вместо него необходимо, чтобы взаимно простыми были числа N и Q . Например, при $(N, Q) = 1$ из (3) и (4) следует, что если $P' = P$ и $Q' = Q \pmod{N}$, то

$$V_n(P', Q') = V_n(P, Q) \pmod{N}, \quad U_n(P', Q') = U_n(P, Q) \pmod{N}.$$

Кроме того, если $(Q, P) = 1$ и $QP' = P^2 - 2Q \pmod{N}$, то

$$\begin{aligned} Q^n V_n(P', 1) &= V_{2n}(P, Q) \pmod{N}, \\ PQ^{n-1} U_n(P', 1) &= U_{2n}(P, Q) \pmod{N}. \end{aligned} \quad (11)$$

Опишем, как можно вычислять $V_n(P, Q)$ и $U_n(P, Q)$ по некоторому натуральному модулю N при больших значениях n .

Заметим, что для любой пары значений V_j, U_j можно найти V_{2j}, U_{2j} с помощью (7), а также V_{j+1}, U_{j+1} по модулю N с помощью (4).

Запишем n в двоичном представлении, пусть

$$n = d_0 2^k + d_1 2^{k-1} + d_2 2^{k-2} + \dots + d_k,$$

где $d_0 = 1, d_j \in \{0, 1\}, j \geq 1, k = \lceil \log_2 n \rceil$. Тогда, если $s_0 = d_0 = 1$ и $s_{j+1} = 2s_j + d_{j+1}$, видно, что $s_k = n$. Введем две последовательности

$$r_j^U = U_{s_j} \pmod{N}, \quad r_j^V = V_{s_j} \pmod{N}.$$

Тогда

$$r_0^U = U_{s_0} = U_1 = 1, \quad r_0^V = V_{s_0} = V_1 = P,$$

По формулам (4) и (7) получаем, что

$$\begin{aligned} r_{j+1}^V &= V_{2s_j + d_{j+1}} = ((r_j^V)^2 - 2Q^{s_j}) \left(1 + \frac{(P-2)d_{j+1}}{2} \right) + \frac{1}{2} r_j^V r_j^U \Delta d_{j+1}, \\ r_{j+1}^U &= U_{2s_j + d_{j+1}} = r_j^V r_j^U + \frac{1}{2} d_{j+1} ((r_j^V)^2 + (P-2)r_j^V r_j^U - 2Q^{s_j}) \pmod{N}, \\ V_n(P, Q) &= r_k^V, \quad U_n(P, Q) = r_k^U \pmod{N}. \end{aligned}$$

Нетрудно видеть, что при подсчете U_n и V_n , было проделано k шагов, на каждом из которых вычислялись вспомогательные U_j, V_j для некоторых j . При вычислении U_j и V_j при фиксированном j производились сложения и умножения натуральных чисел по модулю N . Таким образом, сложность каждого шага есть $O(\log N \log \log N \log \log \log N)$ (по алгоритму Шёнхаге–Штрассена [6]) и сложность вычисления U_n и V_n по модулю N есть

$$O(\log n \log N \log \log N \log \log \log N).$$

Для сокращения записи введем обозначение $\hat{O}(N) = O(N \log^\alpha N)$, где α — постоянная. Следовательно, сложность вычисления U_n и V_n по модулю N при n порядка N есть $\hat{O}(\log^2 N)$.

Теперь приведем известные теоремы, на которые будем опираться в дальнейшем.

Теорема 1 ([1]). Если p — простое число и $(p, 2\Delta Q) = 1$, то $p \mid U_{\Phi(p)}(P, Q)$, где $\Phi(p) = p - \left(\frac{\Delta}{p}\right)$.

Теорема 2 ([1]). Пусть q — простое число такое, что $q^a \parallel m$. Если $(N, 2\Delta Q) = 1$, $U_m(P, Q) = 0$ по модулю N и $(U_{m/q}(P, Q), N) = 1$, то любой простой делитель p числа N должен иметь вид $p = \left(\frac{\Delta}{p}\right) + kq^a$, то есть $\Phi(p) = 0 \pmod{q^a}$.

Теорема 3 ([1]). Пусть $N + 1 = FR$, где число F полностью разложено на множители и для каждого делителя q_i числа F существует последовательность Люка $\{U_k^i\} = \{U_k(P_i, Q_i)\}$ с одним и тем же дискриминантом Δ , для которого $\left(\frac{\Delta}{N}\right) = -1$, $N \mid U_{N+1}^{(i)}$, и $(N, U_{(N+1)/q_i}) = 1$. Тогда каждый простой делитель p числа N должен удовлетворять условию $\Phi(p) = 0 \pmod{F}$, то есть $p = \pm 1 + cF$.

4. Применение функций Люка для доказательства простоты чисел

Теорема 3 является аналогом малой теоремы Ферма для случая, когда известно разложение на множители числа $N + 1$. Благодаря этому, около половины из всех известных больших простых чисел имеют вид $N = A - 1$, где A легко разложимо на множители.

К примеру, функции Люка применяются для проверки на простоту чисел Мерсенна [1] (чисел вида $2^n - 1$), а также чисел вида $A5^n - 1$, $A7^n - 1$ [2] и других.

Далее приводится способ применения функций Люка для доказательства простоты числа вида $N = 2kp_1^{m_1}p_2^{m_2}\dots p_n^{m_n} - 1$, где k — нечетное натуральное число. Сначала докажем лемму, которая понадобится нам в дальнейшем.

Лемма 1. Для любой последовательности Люка $\{U_k(P, Q)\}$ и любого нечетного k

$$U_{nk} = U_n f_k(V_n, Q),$$

где f_k — функция, зависящая только от V_n и Q .

Доказательство. По определению

$$U_{nk} = \left(\frac{\alpha^{nk} - \beta^{nk}}{\alpha - \beta} \right) = \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \right) (\alpha^{n(k-1)} - \alpha^{n(k-2)}\beta^n + \dots + \beta^{n(k-1)}).$$

Покажем, что последняя скобка есть функция, зависящая только от V_n и Q . Нетрудно видеть, что

$$\begin{aligned} & \alpha^{n(k-1)} - \alpha^{n(k-2)}\beta^n + \dots + \beta^{n(k-1)} \\ &= (\alpha^{n(k-1)} + \beta^{n(k-1)}) - \alpha^n\beta^n(\alpha^{n(k-3)} + \beta^{n(k-3)}) + \dots \pm \alpha^{n(k-1)/2}\beta^{n(k-1)/2} \\ &= V_{n(k-1)} - Q^n V_{n(k-3)} + \dots \pm Q^{n(k-1)/2}. \end{aligned}$$

Осталось показать, что V_{nl} , $l = 1, 2, \dots$, можно выразить через V_n и Q . Но это сразу вытекает из (5). Лемма 1 доказана.

Теперь можно приступить к доказательству теоремы.

Теорема 4. Пусть $N = 2kp_1^{m_1}p_2^{m_2}\dots p_n^{m_n} - 1$, где p_i — простые числа, $n, m_i, i = 1, \dots, n$, — натуральные числа, и k — нечетное натуральное число. Пусть $2k < p_1^{m_1}p_2^{m_2}\dots p_n^{m_n}$ и $p_1p_2\dots p_n \equiv 3 \pmod{4}$. Пусть $Q = \pm p_1p_2\dots p_n$, а P — произвольное решение уравнения

$$P^2 = p_1p_2\dots p_n(d^2 \pm 4), \quad (12)$$

где d — натуральное число (это уравнение имеет бесконечно много решений). Тогда, если $V_{(N+1)/(2p_i)} \not\equiv 0 \pmod{N}$ при всех $i = 1, \dots, n$, то N — простое тогда и только тогда, когда $N \mid U_{N+1}(P, Q)$ и $(U_{(N+1)/p_i}(P, Q), N) = 1$ при всех $i = 1, \dots, n$.

Доказательство. Нам известно частичное разложение числа $N + 1$ на множители. Не ограничивая общности будем считать, что $(k, 2p_1p_2\dots p_n) = 1$.

Рассмотрим последовательность Люка $\{U_k(P, Q)\}$, где P и Q выбираются таким образом, чтобы выполнялись условия

$$\left(\frac{\Delta}{N}\right) = -1, \quad \left(\frac{Q}{N}\right) = -1. \quad (13)$$

Ниже будет показано, что значения P и Q из условия теоремы удовлетворяют этим условиям.

Докажем необходимость. Пусть N — простое число, тогда в силу того, что $\left(\frac{\Delta}{N}\right) = -1$, по теореме 1 получаем, что $N \mid U_{N+1}(P, Q)$.

По лемме 1 получаем, что $U_{N+1}(P, Q) = U_{(N+1)/p_i}(P, Q)f_{p_i}(V_{(N+1)/p_i}, Q)$. Допустим, что $N \mid U_{(N+1)/p_i}(P, Q)$. Тогда из (2) следует, что

$$\begin{aligned} V_{(N+1)/p_i}^2 &= 4Q^{(N+1)/p_i} \pmod{N}, \\ V_{(N+1)/p_i}^{p_i} &= \pm 2^{p_i} Q^{(N+1)/2} \pmod{N}. \end{aligned}$$

В предположении, что $N \mid U_n$ (откуда по свойству (2) следует, что справедливо сравнение $V_n^2 = 4Q^n \pmod{N}$), выведем рекуррентно формулу для $V_{(2l+1)n}$:

$$\begin{aligned} V_{(2l+1)n} &= V_n(\alpha^{2ln} - \alpha^{(2l-1)n}\beta + \alpha^{(2l-2)n}\beta^2 - \dots - \alpha\beta^{(2l-1)n} + \beta^{2ln}) \\ &= V_n(V_{2ln} - Q^n(\alpha^{2(l-1)n} - \dots + \beta^{2(l-1)n})) = V_nV_{2ln} - Q^nV_{(2l-1)n} \\ &= (1/2)V_n(V_{(2l-1)n}V_n + \Delta U_{(2l-1)n}U_n) - Q^nV_{(2l-1)n} \\ &= V_{(2l-1)n}((1/2)V_n^2 - Q^n) + U_n(1/2)V_n\Delta U_{(2l-1)n} \\ &= V_{(2l-1)n}((1/2)V_n^2 - Q^n) \pmod{N}. \end{aligned}$$

Следовательно,

$$V_{(2l+1)n} = ((1/2)V_n^2 - Q^n)^l V_n = \pm Q^{nl} 2Q^{n/2} = \pm 2Q^{n(2l+1)/2} \pmod{N}.$$

Отсюда получаем, что

$$V_{N+1} = V_{p_i(N+1)/p_i} = \pm 2Q^{(N+1)/2} = \pm 2QQ^{(N-1)/2} = \pm 2Q(Q/N) \pmod{N}.$$

С другой стороны, используя тождество (6), получим, что

$$\frac{V_{N+1} + \sqrt{\Delta}U_{N+1}}{2} = \left(\frac{P + \sqrt{\Delta}}{2}\right)^{N+1} \pmod{N}.$$

Отсюда находим, что

$$\begin{aligned}
 V_{N+1} &= 2((P + \sqrt{\Delta})/2)^{N+1} = 2/(2^{N+1})(P + \sqrt{\Delta})^{N+1} = (1/2)(P + \sqrt{\Delta})(P + \sqrt{\Delta})^N \\
 &= (1/2)(P + \sqrt{\Delta})(P^N + NP^{N-1}\sqrt{\Delta} + (N(N-1)/2)P^{N-2}(\sqrt{\Delta})^2 + \dots + (\sqrt{\Delta})^N) \\
 &= (1/2)(P + \sqrt{\Delta})(P^N + (\sqrt{\Delta})^N) = (1/2)(P + \sqrt{\Delta})(P^{N-1}P + \Delta^{(N-1)/2}\sqrt{\Delta}) \\
 &= (1/2)(P + \sqrt{\Delta})(P - \sqrt{\Delta}) = (1/2)(P^2 - \Delta) \\
 &= (1/2)(P^2 - (P^2 - 4Q)) = 2Q \pmod{N},
 \end{aligned}$$

то есть при условии, что $V_{(N+1)/p_i}^{p_i} \neq -2^{p_i} Q^{(N+1)/2} \pmod{N}$, с одной стороны $V_{N+1} \neq 2Q \pmod{N}$ и с другой стороны $V_{N+1} = 2Q \pmod{N}$. Таким образом, получили противоречие. Значит, наше предположение о том, что $N \mid U_{(N+1)/p_i}(P, Q)$ при условии $V_{(N+1)/p_i}^{p_i} \neq -2^{p_i} Q^{(N+1)/2} \pmod{N}$ (или $V_{(N+1)/p_i} \neq -2Q^{(N+1)/2p_i} \pmod{N}$), что тоже самое) неверно. Следовательно, $(U_{(N+1)/p_i}, N) = 1$.

Докажем достаточность.

Пусть $N \mid U_{N+1}$ и $(U_{(N+1)/p_i}, N) = 1$ при $i = 1, \dots, n$. Тогда по теореме 3 всякий простой делитель p' числа N должен иметь вид $\pm 1 + l_i p_i^{m_i}$ для любого $i = 1, \dots, n$. А значит, $p' = \pm 1 + l p_1^{m_1} \dots p_n^{m_n} > \sqrt{N}$. Отсюда следует, что N — простое число.

По формуле (7) условие $V_{(N+1)/p_i} \neq -2Q^{(N+1)/2p_i} \pmod{N}$ можно заменить на $V_{(N+1)/2p_i} \neq 0 \pmod{N}$.

Теперь покажем, что значения P и Q из формулировки теоремы удовлетворяют условиям (13).

Сначала рассмотрим Q . Справедливы равенства

$$\left(\frac{-1}{N}\right) = (-1)^{(N-1)/2} = (-1)^{(2kp_1^{m_1} \dots p_n^{m_n} - 2)/2} = (-1)^{kp_1^{m_1} \dots p_n^{m_n} - 1} = 1,$$

то есть,

$$\left(\frac{-Q}{N}\right) = \left(\frac{Q}{N}\right),$$

и

$$\begin{aligned}
 \left(\frac{Q}{N}\right) &= \left(\frac{\pm p_1^{m_1} \dots p_n^{m_n}}{N}\right) = \left(\frac{p_1^{m_1} \dots p_n^{m_n}}{N}\right) \\
 &= (-1)^{(N-1)(p_1^{m_1} \dots p_n^{m_n} - 1)/4} \left(\frac{p_1^{m_1} \dots p_n^{m_n} - 1}{p_1^{m_1} \dots p_n^{m_n}}\right) \\
 &= \left(\frac{-1}{p_1^{m_1} \dots p_n^{m_n}}\right) = (-1)^{(p_1^{m_1} \dots p_n^{m_n} - 1)/2} = -1.
 \end{aligned}$$

Величина P выбирается так, чтобы $\Delta = d^2|Q|$ (так как $\left(\frac{d^2Q}{N}\right) = \left(\frac{p_1^{m_1} \dots p_n^{m_n}}{N}\right) = -1$), где d — натуральное число, то есть $\Delta = P^2 - 4Q = d^2|Q|$. После преобразования получим уравнение (12)

$$P^2 = d^2|Q| + 4Q = |Q|(d^2 \pm 4) = p_1 p_2 \dots p_n (d^2 \pm 4).$$

Ниже будет показано, что это уравнение всегда разрешимо в целых числах.

Теорема 4 доказана.

На основании теоремы 4 можно построить тест для проверки простоты чисел вида $N = 2kp_1^{m_1}p_2^{m_2}\dots p_n^{m_n} - 1$. Сложность этого теста будет равна $\hat{O}(\log^2 N)$, так как его суть заключается в построении чисел Люка V_{N+1} и U_{N+1} по модулю N .

5. Непрерывные дроби

Чтобы использовать приведенную выше теорему для определения простоты числа N , необходимо уметь находить числа P . Для этого нужно решить уравнение

$$P^2 = p_1 p_2 \dots p_n (d^2 \pm 4).$$

Проще всего это сделать, используя теорию непрерывных дробей.

Введем несколько определений [7].

Пусть α — некоторое действительное число. Обозначим через q_0 целую часть α , то есть наибольшее целое число не превосходящее α . Тогда $\alpha = q_0 + \alpha'$, где α' — дробная часть α , удовлетворяющая неравенству $0 \leq \alpha' < 1$. Если $\alpha' > 0$, то положим $\alpha' = 1/\alpha_1$, тогда $\alpha = q_0 + 1/\alpha_1$ и $\alpha_1 > 1$. Далее повторяем эту операцию с α_1 , представив его в виде $\alpha_1 = q_1 + 1/\alpha_2$, где $\alpha_2 > 1$ (если α_1 не является целым числом). Затем выполняем ту же операцию для $\alpha_3 > 1$, $\alpha_4 > 1$ и так далее.

Если число α рациональное, то на очередном шаге получим, что α_m целое. В итоге получим представление рационального числа α в виде непрерывной дроби

$$\alpha = q_0 + \frac{1}{q_1 + \dots + \frac{1}{q_{m-1} + \frac{1}{q_m}}},$$

где $q_1, \dots, q_m$ — натуральные числа, q_0 — целое число.

Если же число α иррациональное, то этот процесс можно продолжать бесконечно и в итоге получим представление иррационального числа α в виде бесконечной непрерывной дроби

$$q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots}}},$$

где $q_1, \dots, q_m, \dots$ — натуральные числа, q_0 — целое число.

Для удобства печати используют сокращенную запись непрерывных дробей в виде

$$q_0 + \frac{1}{q_1 +} \frac{1}{q_2 +} \dots \frac{1}{q_n +} \dots$$

или просто в виде последовательности

$$q_0, q_1, \dots, q_n, \dots$$

Если оборвать запись непрерывной дроби для числа α на некотором числе q_n , то получим новую непрерывную дробь, которую называют подходящей дробью к данной

непрерывной дроби. Эта подходящая дробь выражает рациональное число, которое записывают как A_n/B_n , где A_n и B_n — целые числа. Для этих чисел выполняются рекуррентные соотношения

$$A_0 = q_0, \quad A_1 = q_1 q_0 + 1, \quad A_m = q_m A_{m-1} + A_{m-2}, \quad (14)$$

$$B_0 = 1, \quad B_1 = q_1, \quad B_m = q_m B_{m-1} + B_{m-2}, \quad (15)$$

$$A_m B_{m-1} - B_m A_{m-1} = (-1)^{m-1}, \quad (16)$$

$$\alpha = \frac{\alpha_{n+1} A_n + A_{n-1}}{\alpha_{n+1} B_n + B_{n-1}}. \quad (17)$$

Если бесконечная непрерывная дробь, начиная с некоторого момента, начинает повторяться, то такую дробь называют периодической и записывают в виде $q_0, q_1, \dots, q_n, \overline{q_{n+1}, q_{n+2}, \dots, q_{n+m}}$. Эта запись означает, что период начинается с q_{n+1} и длина периода равна m .

Рассмотрим натуральное число N , не являющееся полным квадратом. Непрерывная дробь для числа $\sqrt{N}$ всегда [7] имеет вид $q_0, q_1, q_2, \dots, q_2, q_1, 2q_0$, то есть является периодической дробью. Период у этой дроби начинается сразу же после первого элемента q_0 и состоит из симметричной части $q_1, q_2, \dots, q_2, q_1$, после которой следует $2q_0$. Симметричная часть может иметь или не иметь центрального элемента.

6. Нахождение пар P и Q с использованием непрерывных дробей

Теперь приведем алгоритм, по которому можно вычислять значение P (see [7]).

По условию теоремы 4, величина P должна удовлетворять уравнению (12)

$$P^2 = p_1 p_2 \dots p_n (d^2 \pm 4),$$

Обе части этого уравнения делятся на $p_1 p_2 \dots p_n$. В силу того, что $p_1 p_2 \dots p_n$ — произведение различных простых чисел, P должно делиться на $p_1 p_2 \dots p_n$. Получаем, что $P = p_1 p_2 \dots p_n c$, где c — натуральное число. Подставив это значение в уравнение (12), получаем, что

$$p_1 p_2 \dots p_n c^2 = d^2 \pm 4.$$

После переноса d^2 влево уравнение принимает вид

$$d^2 - p_1 p_2 \dots p_n c^2 = \mp 4.$$

Предположим, что $2 \mid d$ и $2 \mid c$, и разделим обе части уравнения на 4, тогда

$$(d/2)^2 - p_1 p_2 \dots p_n (c/2)^2 = \mp 1.$$

Для краткости записи введем обозначения $x = d/2$, $y = c/2$, $M = p_1 p_2 \dots p_n$ и получим уравнение

$$x^2 - M y^2 = \mp 1. \quad (18)$$

Рассмотрим непрерывную дробь для числа $\sqrt{M}$

$$\sqrt{M} = q_0 + \frac{1}{q_1 + \frac{1}{q_m + \frac{1}{2q_0 + \frac{1}{q_1 + \dots}}}}$$

По формуле (17),

$$\sqrt{M} = \frac{\alpha_{m+1}A_m + A_{m-1}}{\alpha_{m+1}B_m + B_{m-1}}$$

где α_{m+1} — полное частное, стоящее за q_m , то есть

$$\alpha_{m+1} = 2q_0 + \frac{1}{q_1 +} \dots = \sqrt{M} + q_0.$$

Подставляя это значение для α_{m+1} и производя умножение, получаем уравнение

$$\sqrt{M}(\sqrt{M} + q_0)B_m + \sqrt{M}B_{m-1} = (\sqrt{M} + q_0)A_m + A_{m-1}$$

Так как $\sqrt{M}$ иррационально, а остальные числа целые, из этого уравнения следуют равенства

$$MB_m = q_0A_m + A_{m-1}, \quad q_0B_m + B_{m-1} = A_m.$$

Их можно рассматривать как выражение A_{m-1} и B_{m-1} в терминах A_m и B_m :

$$A_{m-1} = MB_m - q_0A_m, \quad B_{m-1} = A_m - q_0B_m.$$

Подставив эти равенства в (16) получим, что

$$A_m(A_m - q_0B_m) - B_m(MB_m - q_0A_m) = (-1)^{m-1}$$

или

$$A_m^2 - MB_m^2 = (-1)^{m-1}.$$

Значит, $x = A_m$ и $y = B_m$ являются решением уравнения $x^2 - My^2 = (-1)^{m-1}$, а следовательно, для $Q = (-1)^m p_1 p_2 \dots p_n$ получаем решение уравнения (12)

$$P = p_1 p_2 \dots p_n c = 2p_1 p_2 \dots p_n B_m$$

Следует также отметить, что решений уравнений (18) бесконечно много, так как при любом натуральном r , подставляя в (16) вместо m значение $r(m+1) + m$ и проводя те же рассуждения, получим уравнение

$$A_{r(m+1)+m}^2 - MB_{r(m+1)+m}^2 = (-1)^{r(m+1)+m-1},$$

а так как последовательность B_i возрастающая, что следует из (15), получим бесконечно много решений уравнений (12), а следовательно, и бесконечно много различных значений P для $Q = \pm p_1 p_2 \dots p_n$.

В заключение приведем в табл. 1 несколько значений P , вычисленных по этому алгоритму.

Используя различные значения P , вычисленные по приведенному алгоритму, можно строить эффективные тесты проверки простоты чисел вида $N = 2kp_1^{m_1} p_2^{m_2} \dots p_n^{m_n} - 1$.

Таблица 1. Значения P и Q для построения последовательностей Люка

N	Q	$\sqrt{ Q }$	P
$2k3^{m_1}5^{m_2} - 1$	-15	3; 1, 6	30
$2k5^{m_1}7^{m_2} - 1$	-35	5; 1, 10	70
$2k3^{m_1}13^{m_2} - 1$	-39	6; 4, 12	312

Список литературы

1. Lucas E., Théorie des fonctions numériques simplement périodiques. *Am. J.* (1878) **1**, 184–239, 289–321.
2. Williams H. C., Effective primality tests for some integer of the form $A5^n - 1$ and $A7^n - 1$. *Math. Comput.* (1987) **48**, 385–403.
3. Agrawal M., Kayal N., Saxena N., *Primes is in P*. Dept. Computer Sci. and Engineering, Indian Inst. Technology, Kanpur, Kanpur-208016, 2002.
4. Виноградов И. М., *Основы теории чисел*. Наука, Москва, 1972.
5. Грушо А. А., Применко Э. А., Тимонина Е. Е., *Криптографические протоколы*. Марийский филиал Московского Открытого Социального Университета, Йошкар-Ола, 2001.
6. Ахо А., Хопкрофт Дж., Уллман Дж., *Построение и анализ вычислительных алгоритмов*. Мир, Москва, 1979.
7. Дэвенпорт Г., *Высшая арифметика. Введение в теорию чисел*. Наука, Москва, 1965.

Статья поступила 21.06.2006.

Переработанный вариант поступил 30.01.2007.