Math-Net.Ru

Общероссийский математический портал

Е. В. Садовник, Проверка на простоту некоторых чисел вида $N = 2kp^m - 1$, *Дискрет. матем.*, 2006, том 18, выпуск 1, 146–155

DOI: <https://doi.org/10.4213/dm38>

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: 54.80.73.141

26 апреля 2023 г., 12:20:00

Проверка на простоту некоторых чисел вида

$$N = 2kp^m - 1$$

© 2006 г. Е. В. Садовник

Предлагается алгоритм проверки на простоту чисел вида $N = 2kp^m - 1$, где $2k < p^m$, k — нечетное натуральное число, $2k < p^m$, p — простое число и $p \equiv 3 \pmod{4}$. Для построения алгоритма используются функции Люка. Вначале приводится алгоритм для проверки чисел вида $N = 2k3^m - 1$. Затем та же техника применяется для более общих случаев $N = 2kp^m - 1$. Все приведенные в этой статье алгоритмы имеют сложность $O((\log N)^2 \log \log N \log \log \log N)$.

1. Введение

Задача проверки простоты натуральных чисел издавна привлекала внимание математиков. Она имеет как теоретический, так и большой практический интерес. Например, большую роль простые числа играют в криптографии. Многие математики с древних времен искали эффективный способ проверки чисел на простоту. Вершиной этих исследований на данный момент является метод, предложенный в статье [1], где описан алгоритм для проверки простоты числа, работающий полиномиально от длины проверяемого числа N время. Его сложность равна $O(\log^{12} N)$, а при условии, что верна гипотеза о числе простых Софи Жермен, он требует всего $O(\log^6 N)$ операций. До этого в 1983 году Адлеман, Померанс и Румели сформулировали детерминированный алгоритм проверки на простоту, имеющий время исполнения $(\log N)^{O(\log \log \log N)}$.

В настоящее время помимо задачи проверки на простоту чисел важна также тесно связанная с ней задача нахождения больших простых чисел. Например, система шифрования RSA основана на том, что все еще не существует достаточно быстрого алгоритма факторизации чисел. Для построения шифра, как правило, выбираются два больших простых числа и в качестве открытого ключа используется их произведение. Построение больших простых чисел ведется на основе тестов на простоту чисел специального вида.

На сегодняшний день предложено много инструментов проверки числа N на простоту, если известно полное или частичное разложение на множители чисел $N + 1$, $N - 1$, $N^2 + N - 1$ и т. д. Они позволяют строить большие простые числа, если даны небольшие простые числа.

В данной статье предлагаются алгоритмы проверки числа N на простоту, если известно полное или частичное разложение на множители числа $N + 1$.

2. Основные определения и теоремы

Введем основные определения из теории чисел [4].

Сложность алгоритма — это число выполняемых им битовых арифметических операций. Обычно сложность алгоритма представляют в виде какой-либо функции от длины входа, то есть от числа битов k , требуемых для записи входных данных. Если эта функция — многочлен от k , то говорят, что алгоритм имеет полиномиальную сложность (полиномиальный алгоритм), а если это полином первой степени, то алгоритм имеет линейную сложность.

Целые числа a и b сравнимы по модулю p , если существует целое число c такое, 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 двух натуральных чисел a и b обозначается (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 решение (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 (см., например, [2]):

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

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 свойства, которым удовлетворяет символ Лежандра.

Основным инструментом, используемым в данной статье для проверки чисел на простоту, являются функции Люка [3].

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

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

Функции Люка [3] 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 положить $\delta = (\alpha - \beta)$ и $\Delta = (\alpha - \beta)^2$, то $\Delta = P^2 - 4Q$ является дискриминантом уравнения (1). Заметим, что 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 ряду используемых далее тождеств, которые легко выводятся из определения:

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

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

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

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

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

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

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

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

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

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 . Так, при $(N, Q) = 1$ из (3) и (4) следует, что если $P' = P$ и $Q' = Q \pmod{N}$, то

$$\begin{aligned} V_n(P', Q') &= V_n(P, Q), \\ U_n(P', Q') &= U_n(P, Q) \pmod{N}. \end{aligned}$$

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

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

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

Для любой пары значений V_j, U_j можно найти V_{2j}, U_{2j} с помощью (7), а также $V_{j+1}, U_{j+1} \pmod{N}$ с помощью (4).

Запишем n в двоичном представлении

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

где $d_0 = 1, d_j \in \{0, 1\}, j \geq 1, k = [\log_2 n]$. Тогда если $s_0 = d_0 = 1$ и $s_{j+1} = 2s_j + d_{j+1}$, видно, что $s_k = n$. Пусть $r_j^U = U_{s_j} \pmod{N}$ и $r_j^V = V_{s_j} \pmod{N}$, тогда

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

Тогда по формулам (4) и (7) получаем, что

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

Заметим, что сложность вычисления V_n и U_n есть $O((\log n)^2 \log \log n \log \log \log n)$ так как сложность умножения двух чисел, меньших n , с помощью алгоритма Шенхаге-Штрассена есть $O(\log n \log \log n \log \log \log n)$, возведения в степень по модулю n выполняется за $O(\log n)$ операций, а сложение двух чисел по модулю n требует $O(\log n)$ битовых операций.

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

Теорема 1 ([3]). Пусть p — простое число, такое что $(p, 2\Delta Q) = 1$, тогда $p \mid U_{\Phi(p)}(P, Q)$, где $\Phi(p) = p - (\Delta \mid p)$ и $(\Delta \mid p)$ — символ Лежандра.

Теорема 2 ([3]). Пусть q — простое число, такое что $q^a \parallel m$. Если выполняются условия $(N, 2\Delta Q) = 1$, $U_m(P, Q) = 0 \pmod{N}$ и $(U_{m/q}(P, Q), N) = 1$, то любой простой делитель p числа N должен иметь вид $p = (\Delta \mid p) + kq^a$, то есть $\Phi(p) = 0 \pmod{q^a}$.

Теорема 3 ([3]). 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 $(\Delta \mid N) = -1$, $N \mid U_{N+1}^{(i)}$, 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 $p = \pm 1 + cF$.

3. 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 Мерсена [3] (чисел вида $2^n - 1$), а также чисел вида $A5^n - 1$, $A^n - 1$ [5] и других.

Далее приводится способ применения функций Люка для доказательства простоты числа N , если известно частичное разложение на множители числа $N+1$. Сначала рассмотрим частный случай, когда $N = 2k3^m - 1$, а затем применим эту же технику и для случая, когда $N = 2kp^m - 1$, где k — нечетное натуральное число.

Теорема 4. Пусть $N = 2k3^m - 1$, где m — натуральное число, k — нечетное натуральное число и $2k < 3^m$. Запишем число k в двоичном виде $k = (a_0 a_1 \dots a_t)_2$. Положим

$$\begin{aligned} S'_1 &= -14, & S'_{l+1} &= ((S'_l)^2 - 2)(1 - 8a_l) + 96a_l S'_l S'_1 \pmod{N}, \\ S''_1 &= 1, & S''_{l+1} &= \frac{1}{2} a_l ((S'_l)^2 - 2) + (1 - 8a_l)(S'_l S'_1) \pmod{N}, \\ S_1 &= S'_{t+1}, & S_{l+1} &= S_l(S_l^2 - 3) \pmod{N}. \end{aligned}$$

Тогда если $S_m \not\equiv -2 \pmod{N}$, то N — простое тогда и только тогда, когда $N \mid (S_m^2 - 1)$.

Доказательство. В соответствии с теоремой 3, если мы найдем такие числа P и Q , что $(\Delta \mid N) = -1$, $N \mid U_{N+1}(P, Q)$ и $(N, U_{(N+1)/3}) = 1$, то каждый простой делитель числа N должен иметь вид $p = \pm 1 + cF = \pm 1 + c3^m$, но так как $2k < 3^m$, получим, что $N < p^2$. Значит, любой простой делитель числа N больше чем $\sqrt{N}$, то есть число N не имеет нетривиальных делителей, а следовательно, оно простое.

Возьмем P и Q такими, что $(\Delta \mid N) = -1$, $(Q \mid N) = -1$ (их значения мы определим позже).

Докажем необходимость.

Пусть N — простое число, тогда в силу того, что $(\Delta \mid N) = -1$, согласно формуле (8) и теореме 1

$$N \mid U_{N+1}(P, Q), \quad U_{N+1}(P, Q) = U_{(N+1)/3}(P, Q)(V_{(N+1)/3}^2 - Q^{(N+1)/3}).$$

Если $N \mid U_{(N+1)/3}(P, Q)$, то из (2) получим, что

$$V_{(N+1)/3}^2 = 4Q^{(N+1)/3} \pmod{N}, \quad V_{(N+1)/3}^3 = \pm 2^3 Q^{(N+1)/2} \pmod{N},$$

а из (8)

$$\begin{aligned} V_{N+1} &= V_{(N+1)/3}(V_{(N+1)/3}^2 - 3Q^{(N+1)/3}) = V_{(N+1)/3} \left(V_{(N+1)/3}^2 - \frac{3}{4} V_{(N+1)/3}^2 \right) \\ &= \frac{1}{4} V_{(N+1)/3}^3 = \pm \frac{1}{4} 2^3 Q^{(N+1)/2} = \pm 2 Q^{(N+1)/2} \pmod{N}. \end{aligned}$$

Воспользовавшись первым свойством символа Лежандра, получим, что

$$V_{N+1} = \pm 2 Q^{(N+1)/2} = \pm 2 Q Q^{(N-1)/2} = \pm 2 Q (Q \mid N) = \mp 2 Q \pmod{N},$$

то есть, если $V_{(N+1)/3}^3 \not\equiv -2^3 Q^{(N+1)/2} \pmod{N}$ или $V_{(N+1)/3} \not\equiv -2 Q^{(N+1)/6} \pmod{N}$, то получаем, что $V_{N+1} = -2 Q \pmod{N}$.

С другой стороны, используя тождество (10), получим соотношения

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

то есть в случае, когда $V_{(N+1)/3} \not\equiv -2 Q^{(N+1)/6} \pmod{N}$, с одной стороны справедливо сравнение $V_{N+1} = -2 Q \pmod{N}$, а с другой стороны $V_{N+1} = 2 Q \pmod{N}$.

Таким образом, при условии, что $V_{(N+1)/3} \neq -2Q^{(N+1)/6} \pmod{N}$, получили противоречие. Значит, наше предположение о том, что $N \mid U_{(N+1)/3}(P, Q)$ неверно, и тогда $N \mid (V_{(N+1)/3}^2 - Q^{(N+1)/3})$.

По формуле (7)

$$V_{(N+1)/3} = V_{(N+1)/6}^2 - 2Q^{(N+1)/6} \pmod{N}.$$

Значит, условие

$$V_{(N+1)/3} \neq -2Q^{(N+1)/6} \pmod{N}$$

эквивалентно условию

$$V_{(N+1)/6} \neq 0 \pmod{N}.$$

Докажем достаточность.

Предположим, что $N \mid (V_{(N+1)/3}^2 - Q^{(N+1)/3})$. Используя тождество (2), получаем равенство $V_{(N+1)/3}^2 - Q^{(N+1)/3} = 3Q^{(N+1)/3} + \Delta U_{(N+1)/3}^2$, а так как $(Q, N) = 1$ получаем, что $(U_{(N+1)/3}, N) = 1$. Из (8) следует, что $N \mid U_{N+1}$, то есть по теореме 3 всякий простой делитель p числа N должен иметь форму $\pm 1 + \epsilon 3^m > \sqrt{N}$. Отсюда следует, что N — простое число.

Теперь подберем значения P и Q . Сначала подберем значение Q . Ясно, что

$$\left(\frac{-1}{N}\right) = (-1)^{(N-1)/2} = (-1)^{(2k3^m-2)/2} = (-1)^{k3^m-1} = 1,$$

то есть $\left(\frac{-Q}{N}\right) = \left(\frac{Q}{N}\right)$. Нам подходит $Q = \pm 3$, так как

$$\left(\frac{Q}{N}\right) = \left(\frac{\pm 3}{N}\right) = \left(\frac{3}{N}\right) = (-1)^{(N-1)/2} \left(\frac{2}{3}\right) = -1$$

Подберем P так, чтобы $|Q| \mid P$ (это свойство нам понадобится в дальнейшем, для упрощения алгоритма) и $\Delta = d^2|Q|$ (так как $\left(\frac{\Delta}{N}\right) = \left(\frac{d^2Q}{N}\right) = \left(\frac{3}{N}\right) = -1$), где d — натуральное число, откуда следует, что $P = tQ$. Найдем t . Ясно, что

$$\Delta = P^2 - 4Q = t^2Q^2 - 4Q = d^2|Q| \implies t^2|Q| \mp 4 = d^2.$$

В нашем случае $3t^2 \mp 4 = d^2$. Ясно, что

$$t = 2 \implies 3t^2 + 4 = 4^2 \implies P = 6, \quad Q = -3, \quad \Delta = 48.$$

В итоге получили следующий алгоритм для проверки простоты чисел вида $N = 2k3^m - 1$.

Строим последовательность Люка $V_n(6, -3)$ и проверяем условие

$$N \mid (V_{(N+1)/3}(6, -3)^2 - (-3)^{(N+1)/3}).$$

Если оно выполняется, то число N — простое, в противном случае N — составное при условии, что $V_{(N+1)/6}(6, -3) \neq 0 \pmod{N}$.

Для упрощения вычислений можно строить последовательность $V_n(P', 1)$, где P' определяется из условия, что $QP' = P^2 - 2Q \pmod{N}$ ($P' = -14$), и проверять условие $N \mid (V_{(N+1)/6}(P', 1)^2 - 1)$. Так как по формуле (11)

$$(-3)^n V_n(-14, 1) = V_{2n}(6, -3) \pmod{N},$$

находим, что

$$\begin{aligned} V_{(N+1)/3}(6, -3) &= (-3)^{(N+1)/6} V_{(N+1)/6}(-14, 1) \pmod{N}, \\ V_{(N+1)/3}^2(6, -3) - (-3)^{(N+1)/3} &= ((-3)^{(N+1)/6} V_{(N+1)/6}(-14, 1))^2 - (-3)^{(N+1)/3} \\ &= (-3)^{(N+1)/3} (V_{(N+1)/6}^2(-14, 1) - 1) = 0 \pmod{N}, \end{aligned}$$

а условие $V_{(N+1)/6}(6, -3) \neq 0 \pmod{N}$ примет вид $V_{(N+1)/12}(-14, 1) \neq 0 \pmod{N}$, или

$$V_{(N+1)/6}(-14, 1) \neq -2Q^{(N+1)/12} = -2 \pmod{N}.$$

Определим число арифметических операций (сложность алгоритма) необходимых для проверки числа на простоту с помощью доказанного алгоритма. Суть алгоритма сводится к построению члена $V_{(N+1)/6}$ последовательности Люка. Как было показано выше, число арифметических операций, за которое вычисляют члены V_n и U_n последовательностей Люка есть $O(\log_2 n)$. Значит, и сложность доказанного алгоритма есть $O((\log N)^2 \log \log N \log \log \log N)$.

Теорема 4 доказана.

В качестве следствия рассмотрим случай, когда $k = 1$.

Теорема 5. Пусть $N = 2 \cdot 3^m - 1$, где m — натуральное число и последовательность S_k определяется соотношениями $S_1 = 14$ и

$$S_{k+1} = S_k(S_k^2 - 3) \pmod{N}, \quad r = 1, 2, \dots$$

Тогда, если $S_m \neq 2 \pmod{N}$, то N — простое число тогда и только тогда, когда $N \mid (S_m^2 - 1)$.

Доказательство. Воспользуемся теоремой 4. Так как $k = 1$, то $S'_{t+1} = -14$, то есть $S_1 = -14$. Для удобства заменим знак у S_1 на противоположный. Это можно сделать потому, что в формуле для S_{i+1} , в скобках при вычитании фигурирует лишь квадрат значения S_i . Следовательно, S_i при $S_1 = 14$ и S_i при $S_1 = -14$ при любом i различаются только знаком. Значит и условие $S_m \neq -2 \pmod{N}$, заменяется на $S_m \neq 2 \pmod{N}$.

Теорема 5 доказана.

Расширим теорему 4 на случай, когда $N = 2kp^m - 1$, где m — натуральное число, k — нечетное натуральное число, $2k < p^m$.

Теорема 6. Пусть $N = 2kp^m - 1$, где m — натуральное число, k — нечетное натуральное число, $2k < p^m$, p — простое число и $p \equiv 3 \pmod{4}$. Пусть $Q = \pm p$ и P такое, что $P^2 = p(d^2 \pm 4)$, где d — натуральное число.

Тогда, если $V_{(N+1)/(2p)} \neq 0 \pmod{N}$, то N — простое число тогда и только тогда, когда $(U_{(N+1)/p}(P, Q), N) = 1$ и $N \mid U_{N+1}(P, Q)$.

Доказательство. Доказательство проводится по тому же принципу, что и для случая $p = 3$.

Выбираем P и Q такими, что выполняются условия $(\Delta \mid N) = -1$, и $(Q \mid N) = -1$.

Докажем необходимость.

Пусть N — простое число, тогда в силу того, что $(\Delta \mid N) = -1$, согласно теореме 1 верно соотношение $N \mid U_{N+1}(P, Q)$.

По определению $U_{N+1}(P, Q) = U_{(N+1)/p}(P, Q) \cdot f_p(V_{(N+1)/p}, Q)$, так как для любого нечетного p верно, что

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

Покажем, что выражение в последней скобке есть функция, зависящая от V_n и Q . Действительно,

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

Осталось показать, что V_{nk} , $k = 1, 2, \dots$, можно выразить через V_n и Q . Это сразу вытекает из (5).

Если $N \mid U_{(N+1)/p}(P, Q)$, то из (2) получим, что

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

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

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

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

Итак, получаем, что

$$\begin{aligned} V_{N+1} &= V_{2kp^m} = V_{p(2kp^{m-1})} = \pm 2Q^{2kp^{m-1}p/2} \\ &= \pm 2Q^{(N+1)/2} = \pm 2Q Q^{(N-1)/2} = \pm 2Q(Q/N) \pmod{N}. \end{aligned}$$

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

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

Итак, при условии, что

$$V_{(N+1)/p}^p \not\equiv -2^p Q^{(N+1)/2} \pmod{N},$$

с одной стороны $V_{N+1} \not\equiv 2Q \pmod{N}$ и с другой стороны $V_{N+1} = 2Q \pmod{N}$. Таким образом, получили противоречие. Значит, наше предположение о том, что $N \mid U_{(N+1)/p}(P, Q)$ при условии, что $V_{(N+1)/p}^p \not\equiv -2^p Q^{(N+1)/2} \pmod{N}$, или что $V_{(N+1)/p} \not\equiv -2Q^{(N+1)/2p} \pmod{N}$ неверно. Следовательно, $(U_{(N+1)/p}, N) = 1$.

Докажем достаточность.

Пусть $(U_{(N+1)/p}, N) = 1$ и $N \mid U_{N+1}$. Тогда по теореме 3 всякий простой делитель p' числа N должен иметь форму $\pm 1 + lp^m > \sqrt{N}$. Отсюда следует, что N — простое число.

Условие

$$V_{(N+1)/p} \not\equiv -2Q^{(N+1)/(2p)} \pmod{N}$$

согласно (7) можно заменить на

$$V_{(N+1)/(2p)} \not\equiv 0 \pmod{N}.$$

Подберем значения P и Q . Сначала подберем значение Q . Ясно, что

$$\left(\frac{-1}{N}\right) = (-1)^{(N-1)/2} = (-1)^{(2kp^m-2)/2} = (-1)^{kp^m-1} = 1,$$

то есть $\left(\frac{-Q}{N}\right) = \left(\frac{Q}{N}\right)$. Нам подходит $Q = \pm p$, так как

$$\left(\frac{Q}{N}\right) = \left(\frac{\pm p}{N}\right) = \left(\frac{p}{N}\right) = (-1)^{(N-1)(p-1)/2} \left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = -1$$

Значение P подбирается так, чтобы $\Delta = d^2|Q|$ (так как $\left(\frac{d^2Q}{N}\right) = \left(\frac{p}{N}\right) = -1$), где d — натуральное число, то есть

$$\Delta = P^2 - 4Q = d^2|Q| \implies P^2 = d^2|Q| + 4Q = |Q|(d^2 \pm 4).$$

Таблица 1. Значения P и Q для построения последовательностей Люка

p	P	Q	P'
3	6	-3	-14
7	42	-7	-254
11	66	-11	-398
19	1482	-19	-115598

Рассмотрим вопрос о существовании решения уравнения $P^2 = |Q|(d^2 \pm 4)$ в целых числах. Обе части этого уравнения делятся на $|Q|$. В силу того, что $|Q|$ — простое число, P должно делиться на $|Q|$. Получаем, что $P = |Q|c^2$, а значит,

$$|Q|c^2 = d^2 \pm 4.$$

Перенеся d^2 влево, получаем равенство

$$d^2 - |Q|c^2 = \mp 4.$$

Предполагая, что $d/2$ и $c/2$ и деля обе части уравнения на 2, приходим к равенству

$$(d/2)^2 - |Q|(c/2)^2 = \mp 1.$$

Получили уравнение Пелля, которое, как известно [6], всегда имеет решение (если $|Q|$ не является квадратом целого числа, что в нашем случае выполняется).

Сложность алгоритма будет равна $O((\log N)^2 \log \log N \log \log \log N)$, так как суть алгоритма заключается в построении чисел Люка V_{N+1} и U_{N+1} .

Теорема 6 доказана.

В заключение приведем значения P и Q для построения последовательностей Люка $\{U_n(P, Q)\}$ и $\{V_n(P, Q)\}$ при различных значениях p . В последней колонке приводятся значения P' , для построения последовательности $\{U_n(P', 1)\}$.

Список литературы

1. Agrawal M., Kayal N., Saxena N., *Primes is in P*. Dept. Computer Sci. and Engineering, Indian Inst. Technology, Kanpur, Kanpur-208016, 2002.
2. Грушо А. А., Применко Э. А., Тимонина Е. Е., *Криптографические протоколы*. Йошкар-Ола, 2001.
3. Lucas E., Theorie des fonctions numeriques simplement periodiques. *Amer. J. Math.* (1878) **1**, 184-239, 289-321.
4. Виноградов И. М., *Основы теории чисел*. Наука, Москва, 1972.
5. Williams H. C., Effective primality tests for some integer of the form $A5^n - 1$ and $A7^n - 1$. *Mathematics of Computation* (1987) **48**, №177, 385-403.
6. Дзвенпорт Г., *Высшая арифметика. Введение в теорию чисел*. Наука, Москва, 1965.

Статья поступила 14.06.2005.