Математика и ее приложения : ЖИМО. 2012. Вып. 1 (9). С. 95–106

УДК 512.543

С. И. Хашин[1]

Свойства BPSW-псевдопростых чисел

Ключевые слова: псевдопростые числа, проверка простоты, BPSW тест.

Доказываются некоторые свойства $BPSW$-псевдопростых чисел. Как результат, доказывается отсутствие $BPSW$-псевдопростых, меньших 2^{60}. Основными результатами работы являются теоремы 4, 5, 7, 9, 10, 11.

Key words: pseudoprimes, primality test, BPSW.

Some properties of $BPSW$-pseudoprimes are proved. As a result, we prove the absence of $BPSW$-pseudoprimes, less 2^{60}. The main results of the paper are theorems 4, 5, 7, 9, 10, 11.

1. Введение

Важной задачей теории чисел до сих пор остается разработка эффективных методов проверки простоты чисел. Разработано множество самых разнообразных алгоритмов таких проверок [5, 3, 7]. Эти методы дают лишь вероятностный ответ: число может оказаться гарантировано составным, или «вероятно простым». То есть каждый из этих методов может принять некоторое составное число за простое, но не наоборот. Такие числа называются «псевдопростыми». Наиболее простой метод основан на малой теореме Ферма.

Определение 1. *Составное число n называется псевдопростым по основанию a, если $a^{n-1} \equiv 1 \mod n$.*

К сожалению, псевдопростых чисел оказывается достаточно много. Например, среди чисел, меньших 2^{64}, их оказывается 118 968 378 [6]. Проверка по нескольким различным основаниям существенно сокращает количество ошибок, но не позволяет полностью от них избавиться. Разработано несколько вариантов усиления метода [5, 7]: «сильно псевдопростые числа», «метод Миллера-Рабина» и некоторые другие. Они в разы сокращают вероятность ошибок, но даже не на порядки, что, конечно же, недостаточно.

В тоже время, существуют методы, которые, хотя и дают довольно много ошибок, но на совершенно других числах, чем методы, основанные на теореме Ферма. Один из них – метод Лукаса [5, 7]. Некоторый вариант его

[1]Ивановский государственный университет; E-mail: khash2@mail.ru. Работа выполнена при поддержке гранта РФФИ 10-07-00350а

совместного применения с методом Ферма и называется BPSW-методом. На сегодняшний день неизвестно ни одного составного числа, на котором BPSW-метод ошибается. Более того, используя полный список [6] псевдопростых по модулю 2 чисел, меньших 2^{64}, можно проверить, что этот BPSW-алгоритм дает точный ответ для всех чисел до 2^{64}.

Однако хотелось бы получить и независимую от списка [6] проверку этого факта. Эта проверка и является одним из основных результатов работы.

2. Последовательности Лукаса

Определение 2. *[7, 5] Пусть P, Q – два целых числа. Последовательностями Лукаса $U_n = U_n(P,Q)$ и $V_n = V_n(P,Q)$ называются последовательности, удовлетворяющие рекуррентному соотношению*

$$\begin{aligned} U_n &= PU_{n-1} - QU_{n-2}, \\ V_n &= PV_{n-1} - QV_{n-2} \end{aligned} \tag{1}$$

при $n \geq 2$ и начальным условиям

$$\begin{aligned} U_0 &= 0, \quad U_1 = 1\,, \\ V_0 &= 2, \quad V_1 = P\,. \end{aligned} \tag{2}$$

При $P = 1$ и $Q = -1$ последовательность U_n является последовательностью чисел Фибоначчи. В применениях параметр P всегда будет равен 1, а параметр Q выбираться из последовательности $-1, 2, -3, \ldots$. Число $D = P^2 - 4Q$ называется дискриминантом последовательности. В содержательных случаях оно не должно быть полным квадратом. Для чисел Фибоначчи дискриминант равен 5.

Свойство 1. *[7, 5] Пусть*

$$\alpha, \beta = \frac{P \pm \sqrt{D}}{2}, \quad \alpha + \beta = P, \quad \alpha\beta = Q.$$

Тогда

$$U_n = U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad V_n = V_n(P,Q) = \alpha^n + \beta^n\,.$$

Из этого свойства можно вывести следующее ограничение.

Следствие 1. *Ограничение сверху:*

$$U_n < A \cdot B^n\,,$$

где A, B в случае $D = P^2 - 4Q > 0$ таковы:

$$A = \frac{1}{\sqrt{D}}, \quad B = \frac{P + \sqrt{D}}{2}\,,$$

а в случае $D < 0$*:*

$$A = \frac{2}{\sqrt{-D}}, \quad B = \sqrt{\frac{P^2 - D}{2}}\,.$$

Теорема 1. *[5] Пусть* p *– простое число и символ Якоби* $j(c/p)$ *равен* -1*. Обозначим через* $\gamma \in \mathbb{Z}_p[\sqrt{Q}\,]$ *отношение:*

$$\gamma = \frac{\alpha}{\beta} = \frac{P + \sqrt{Q}}{P - \sqrt{Q}} = \frac{P}{Q}\alpha - 1.$$

Тогда

а) $U_n \equiv 0 \mod p \Leftrightarrow \gamma^n = 1 \in GF(p^2)$*,*
б) $V_n \equiv 0 \mod p \Leftrightarrow \gamma^n = -1 \in GF(p^2)$*.*

Теорема 2. *(Критерий Лукаса) [7, 5] Пусть* n *– нечетное простое,* $\varepsilon = J(D/n)$ *и* $gcd(n, Q) = 1$*. Тогда*

а) $U_{n-\varepsilon} \equiv 0 \mod n$*;*
б) $V_{n-\varepsilon} \equiv 2Q^{(1-\varepsilon)/2} \mod n$*;*
в) $U_n \equiv \varepsilon \mod n$*;*
г) $V_n \equiv P \mod n$*;*

Определение 3. *Для натурального числа* n *через* $\rho(n) = \rho(n, P, Q)$ *обозначим наименьшее натуральное* k *такое, что* $U_k = U_k(P, Q) \equiv 0 \mod n$*. Если таких* k *нет, будем считать, что* $\rho(n) = 0$*.*

Теорема 3. *Пусть* p *– простое и* $J(D, p) = 1$*. Тогда* γ *из теоремы (1) принадлежит* $\mathbb{Z}_p$ *и* $\rho(p) = order(\gamma, p)$*.*

Теорема 4. *Для* $\rho(n) = \rho(n, P, Q)$ *можно выписать оценку сверху:*

$$\rho(n) \geq \frac{\ln n - lnA}{\ln B}\,,$$

где A, B *– как в следствии (1). Несколько загрубляя оценку, можно сказать, что при* $P = 1, |Q| < 100$ *справедливо* $\rho(n) > 1 + ln(n)/2$*.*

Доказательство. Так как $U_{\rho(n)} \geq n$, можем воспользоваться следствием (1).

Подробнее: если $J(D/n) = 1$, то $U_{n-1} \equiv 0 \mod n$, если $J(D/n) = -1$, то $U_{n+1} \equiv 0 \mod n$. ■

Определение 4. *Тест Лукаса – Сельфиджа. Пусть* n *– натуральное нечетное число. Среди последовательности чисел* $5, -7, 9, \ldots$ *возьмем наименьшее* D *такое, что символ Якоби* $J(D/n) = -1$ *и рассмотрим последовательность Лукаса с параметрами* $(P = 1, Q = (1 - D)/4)$*. Число* n *будем называть псевдопростым по Лукасу, если*

$$U_{n+1} = U_{n+1}(P, Q) \equiv 0 \mod n\,.$$

Этот тест можно несколько усилить. Выделим из $n+1$ степень двойки: $n+1 = 2^s \cdot k$, где k – нечетно. Пусть, например, $n+1 = 8k$. Тогда

$$U_{8k} = U_k V_k V_{2k} V_{4k}$$

и условие $U_{n+1} \equiv 0 \mod n$ для простого n означает, что в выражении

$$U_{8k} = U_k V_k V_{2k} V_{4k} \equiv 0 \mod n$$

хотя бы один из множителей обращается в 0. Такие числа будем называть сильно псевдопростыми по Лукасу. Эксперименты показывают, что в случае составных из двух простых множителей количество ошибок сокращается примерно в три раза и позволяют ожидать, что в случае m простых сомножителей количество ошибок сократится в 3^{m-1} раз. Объем же вычислений практически не меняется по сравнению с обычным тестом Лукаса.

Теорема 5. *Пусть в тесте Лукаса – Сельфиджа для нечетного n оказался выбран параметр D. Тогда*

а) $d = |D|$ – либо простое, либо $D = -15$,

б) если $|D| \geq 15$, то $J(n/d) = -1$ и для всех нечетных простых $q < d$: $J(n/q) = 1$.

Замечание 1. Для $|D| < 15$ тоже можно выписать необходимые условия:

- $D = 5$: $J(n/5) = -1$.
- $D = -7$: $J(n/5) = +1$, $J(n/7) = -1$.
- $D = -11$: $J(n/5) = J(n/7) = +1$, $J(n/11) = -1$.
- $D = 13$: $J(n/5) = (n/7) = J(n/11) = +1$, $J(n/13) = -1$.

Лемма 1. *Пусть d – натуральное и нечетное а $D = (-1)^{\frac{d-1}{2}} d$ (если d пробегает значения $5, 7, 9, 11, \ldots$, то D будет пробегать $5, -7, 9, -11, \ldots$ и $d = |D|$). Тогда для любого нечетного n: $J(D/n) = J(n/d)$.* ■

3. BPSW-тест

Для проверки чисел на простоту очень эффективным оказывается следующий метод [7, 5, 1]. Пусть n – нечетное натуральное число, которое мы хотим проверить на простоту. Это предлагается делать следующим образом.

Шаг 1. Тест Миллера – Рабина по основанию 2.

Шаг 2. Тест Лукаса – Сельфиджа. Отметим, что если в тесте из последовательности $5, -7, 9, \ldots$ выбран параметр D, то, фактически при этом

проверяется, что число n взаимно-просто со всеми числами, не превосходящими $|D|$.

Числа, проходящие эти два теста будем называть BPSW-псевдопростыми.

Определение 5. *Для натурального n и целых (P, Q) обозначим через $R(n) = R(n, P, Q)$ функцию (здесь $D = P^2 - 4 * Q$):*

$$R(n,P,Q) = \begin{cases} 0, & J(D,n) = 0 \\ gcd(2^{n-1} - 1,\, U_{n-1}(P,Q)), & J(D,n) = 1 \\ gcd(2^{n-1} - 1,\, U_{n+1}(P,Q)), & J(D,n) = -1 \end{cases}$$

Теорема 6. *Если p – простое, и взаимно-простое с $PQ(1-4Q)$, то $R(p)$ делится на p.* ■

Значения функции R не очень велики и могут быть вычислены при не слишком больших n ($\approx$ до 2^{18}).

Теорема 7. *Пусть n – BPSW-псевдопростое, $n = pq$, где p – простое. Тогда p – простой делитель $R(q)$.*

Доказательство. Так как $2^{pq-1} \equiv 1 \mod p$, то

$$2^{pq-1} = 2^{(p-1)q+(q-1)} \equiv 2^{q-1} \equiv 1 \mod p,$$

т. е. $2^{q-1} - 1$ делится на p.

Пусть тест Лукаса выполнялся с параметром Q, $D = 1 - 4Q$. По условию, $J(D/n) = -1$. Пусть $J(D/p) = +1$. Тогда $J(D/q) = -1$. Так как $U_{p-1} = U_{p-1}(P,Q) \equiv 0 \mod p$ и

$$U_{pq+1} = U_{(p-1)q+q+1} \equiv U_{q+1} \equiv 0 \mod p\,,$$

т. е. U_{q+1} делится на p. Таким образом, число p должно делить $2^{q-1} - 1$ и U_{q+1}, т. е. p – простой делитель $R(q)$.

Пусть теперь $J(D/p) = -1$. Тогда $J(D/q) = +1$. Так как $U_{p+1} \equiv 0 \mod p$ и

$$U_{pq+1} = U_{(p+1)q-q+1} \equiv U_{(p+1)-(q-1)} \equiv 0 \mod p\,.$$

Отсюда следует, что $U_{q-1} \equiv 0 \mod p$, т. е. p – простой делитель U_{q-1}, а значит, p опять будет делителем $R(q)$. ■

Эта теорема позволяет эффективно проверить на псевдопростоту числа вида pq, где q – произвольное натуральное, не превышающее некоторого предела, а p – простое. Например, пои $q < 100\,000$ и $|D| \le 21$ таких чисел не обнаружено. С помощью библиотеки GMP можно проверить все числа в пределах до 2^{18} и даже несколько больше.

Кроме того, нет ни одного простого числа q, меньшего 2^{20} такого, что $J(5,q) = -1$ и у R-функции которого $R(q) = R(q,P,Q)$ был бы простой делитель, больший q.

Также можно проверить и следующее утверждение.

Теорема 8. *При $|D| < 128$ среди чисел $q < 2^{18}$, $J(D,q) = -1$ нет ни одного, у которого был бы простой делитель числа $R(q)$ больший q.*

Теорему (7) можно несколько уточнить:

Теорема 9. *Пусть n – BPSW-псевдопростое, $n = pq$, где p – простое при некотором $D = 1 - 4Q$. Тогда:*

если $J(D/p) = +1$, то p – простой делитель одного из четырех чисел

$$gcd(2^k - 1, U_k), \quad gcd(2^k - 1, V_k), \quad gcd(2^k + 1, U_k), \quad gcd(2^k + 1, V_k)\,;$$

если $J(D/p) = -1$, то p – простой делитель одного из четырех чисел

$$gcd(2^k - 1, U_{k+1}), \quad gcd(2^k - 1, V_{k+1}), \quad gcd(2^k + 1, U_{k+1}), \quad gcd(2^k + 1, V_{k+1})\,,$$

где $k = (q-1)/2$.

Доказательство. Следует из того, что $2^{2k} - 1 = (2^k - 1)(2^k + 1)$ и $U_{2k} = U_k V_k$. ■

При конкретных вычислениях эта теорема удобнее, чем (7), так как имеет дело с числами вдвое меньшей длины.

3.1. Простой множитель p с $J(D/p) = +1$

Пусть n – BPSW-псевдопростое, $n = pq$, где p – простое и $J(D/p) = 1$. Теорема (7) утверждает в этом случае, что p – простой делитель $2^{q-1} - 1$ и U_{q+1}, или

$$\begin{aligned} a)\, 2^{q-1} &\equiv 1 \mod p, \\ b)\, U_{q+1} &\equiv 0 \mod p. \end{aligned} \tag{3}$$

Обозначим $(q-1)/2$ через k. Тогда (напомним, $U_{2n} = U_n V_n$):

$$\begin{aligned} a)\, (2^k - 1)(2^k + 1) &\equiv 0 \mod p, \\ b)\, U_{k+1} V_{k+1} &\equiv 0 \mod p. \end{aligned} \tag{4}$$

Пусть γ – как в теореме (1):

$$\gamma = \frac{\alpha}{\beta} = \frac{P + \sqrt{Q}}{P - \sqrt{Q}} = \frac{P}{Q}\alpha - 1.$$

Так как $J(D/p) = 1$, то $\sqrt{Q}$ принадлежит $\mathbb{Z}_p$, а значит и $\gamma \in \mathbb{Z}_p$. Поэтому условия (4) можно записать так (напомню, $k = (q-1)/2$):

$$\begin{aligned} a)\, 2^k &\equiv \pm 1 \mod p, \\ b)\, \gamma^{k+1} &\equiv \pm 1 \mod p. \end{aligned} \tag{5}$$

Теорема 10. *Пусть n – $BPSW$-псевдопростое, $n = pq$, где p – простое и $J(D/p) = 1$. Тогда*

а) число p удовлетворяет условию:

$$gcd(\, ord(2,p),\, \rho(p,P,Q)\,) \le 2,$$

б) при фиксированном p, число q удовлетворяет условию:

$$q \equiv q_0 \mod LCM(ord(2,p),\, \rho(p,P,Q)),$$

где q_0 находится из условий

$$\begin{aligned} a)\, q_0 &\equiv \quad 1 \mod ord(2,p), \\ b)\, q_0 &\equiv -1 \mod \rho(p,P,Q). \end{aligned}$$

Напомним, что в этом случае и $ord(2,p)$, и $\rho(p,P,Q)$ являются делителями $p-1$, а $LCM(ord(2,p),\, \rho(p,P,Q))$ будет делителем $2(p-1)$.

Доказательство. Пусть $n = pq$. Так как $2^{pq-1} \equiv 1 \mod p$ то $2^{q-1} \equiv 1 \mod p$ или $q - 1 \equiv 0 \mod ord(2,p)$ или

$$q \equiv 1 \mod ord(2,p)\,. \tag{6}$$

Далее,

$$U_{pq+1}(P,Q) \equiv 0 \mod n \Rightarrow U_{pq+1}(P,Q) \equiv 0 \mod p\,.$$

Имеем: $U_{p-1} \equiv 0 \mod p$, поэтому

$$U_{pq+1} = U_{(p-1)q+q+1} \equiv U_{q+1} \equiv 0 \mod p,$$

т. е. $q+1$ делится на $\rho(p,P,Q)$ или

$$q \equiv -1 \mod \rho(p,P,Q)\,. \tag{7}$$

Итак, q должно удовлетворять условиям:

$$\begin{aligned} a)\, q &\equiv \quad 1 \mod ord(2,p)\,, \\ b)\, q &\equiv -1 \mod \rho(p,P,Q)\,, \end{aligned}$$

что доказывает (б), причем и $ord(2,p)$, и $\rho(p,P,Q)$ являются делителями $p-1$. Предположим, что

$$d = GCD(ord(2,p),\, \rho(p,P,Q)) > 2.$$

Тогда

$$\begin{aligned} a)\, q &\equiv \quad 1 \mod d\,, \\ b)\, q &\equiv -1 \mod d \end{aligned}$$

– противоречие. ■

Числа, удовлетворяющие условиям теоремы, существуют, но их не так много. Для их поиска можно воспользоваться следующим утверждением.

Следствие 2. *Пусть n – BPSW-псевдопростое, p – простой делитель n и $J(D/p) = 1$. Тогда*

$$ord(2,p) \cdot \rho(p,P,Q)\,) \le 2(p-1).$$

Так как у нас есть ограничение снизу на $\rho(n)$ (следствие 4), то можно написать следующее неравенство.

Следствие 3. *Пусть n – BPSW-псевдопростое, $|Q| < 100$, p – простой делитель n и $J(D/p) = 1$. Тогда*

$$\frac{p-1}{ord(2,p)} > ln(p)/4 + 1/2.$$

Теорема 11. *Пусть n – BPSW-псевдопростое, p – простой делитель n и $J(D/p) = 1$. Тогда*

а) если $p-1$ делится на 2^k, $k > 1$, то либо $2^s = 1$, либо $U_s = 0$, где $s = (p-1)/2^{k-1}$;

б) если r – нечетный простой делитель $p-1$ кратности $k \ge 1$, то либо $2^s = 1$, либо $U_s = 0$, где $s = (p-1)/r^k$.

Доказательство. Следует из того, что

$$gcd(\,ord(2,p),\,\rho(p,P,Q)\,) \le 2.$$

■

Числа p, меньшие 2^{34} (17.17 млрд), удовлетворяющие условиям теоремы (10), найдены при $|D| < 128$ и приведены в файле GCD_le_2bb.txt. При простых D и $D = -15$ их оказалось 170, из них 5 – при $Q = -1$. Это 61 681, 363 101 449, 4 278 255 361, 4 562 284 561 и 4 582 537 681.

3.2. Простой множитель p, с $J(D/p) = -1$

Теорема 12. *(повтор) При $|Q| < 32$ среди чисел $q < 2^{18}$, $J(1-4Q,q) = -1$ нет ни одного, у которого был бы простой делитель числа $R(q)$ больший q.*

Определение 6. *Для простого p и целых P, Q через $L(p) = L(p,P,Q)$ обозначим число*

$$L = LCM(ord(2,p),\,\rho(p,P,Q))\,.$$

Теорема 13. *Пусть n – BPSW-псевдопростое, $n = pq$, где p – простое и $J(D,p) = -1$. Тогда*

$$q \equiv 1 \mod L(p,P,Q))$$

Напомним, что в этом случае $ord(2,p)$ – делитель $p-1$, а $\rho(p,P,Q)$ – делитель $p+1$.

Доказательство. Так как $J(D/p)=-1$, то $U_{p+1}\equiv 0 \mod p$. Мы знаем, что

$$U_{pq+1}\equiv 0 \mod pq, \quad 2^{pq-1}\equiv 1 \mod pq\,,$$

или, учитывая, что $U_{p+1}\equiv 0 \mod p$,

$$U_{q-1}\equiv 0 \mod p, \quad 2^{q-1}\equiv 1 \mod p\,,$$

или

$$q-1\equiv 0 \mod \rho(p,P,Q), \quad q-1\equiv 0 \mod ord(2,p)\,,$$

или

$$q\equiv 1 \mod \rho(p,P,Q), \quad q\equiv 1 \mod ord(2,p).$$

Эти два условия можно объединить в одно:

$$q\equiv 1 \mod LCM(ord(2,p),\, \rho(p,P,Q),)\,.$$

■

Теорема 14. *Пусть n – BPSW-псевдопростое, $n=pq$, где p – простое и $J(D/p)=-1$. Обозначим $LCM(ord(2,p),\, \rho(p,P,Q))$ через L. Тогда*

а) если L делится на 5 и $J(p/5)=-1$, то $D=5$;

б) если L делится на 5 и $J(p/5)=+1$, то $|D|>5$;

в) если L делится на простое $s>5$ и $J(p/s)=-1$, то $|D|\le s$;

г) если L делится на 3 и $J(p/3)=-1$, то $|D|\le 15$.

Сформулируем чуть по-другому.

Теорема 15. *Пусть n – BPSW-псевдопростое, $n=pq$, где p – простое и $J(D/p)=-1$. Обозначим $LCM(ord(2,p),\, \rho(p,P,Q))$ через L. Тогда*

а) если L делится на простое s большее 3 и $J(p/s)=-1$, то $|D|\le s$;

б) если L делится на 3 и $J(p/3)=-1$, то $|D|\le 15$.

Следствие 4. *Пусть n – BPSW-псевдопростое, $n=pq$, где p – простое и $J(D/p)=-1$. Тогда*

а) если $ord(2,p)$ делится на простое s большее 3 и $J(p/s)=-1$, то $|D|\le s$;

б) если $ord(2,p)$ делится на 3 и $J(p/3)=-1$, то $|D|\le 15$.

3.3. Произведение двух простых

Соберем вместе все, что известно, в случае $n=pq$ – произведение двух простых сомножителей. Так как $J(D/n)=-1$, то пусть $J(D/p)=-1$, $J(D/q)=+1$. Будем полагать также, что $|Q|<32$. Тогда

(1) $J(D_0/n) = J(D_0/p)J(D_0/q) = 1$ при всех $D_0 = 5, -7, \ldots$ меньших по модулю $|D|$.

(2) p – простой делитель $R(q) = gcd(2^{q-1} - 1,\, U_{q-1}(P,Q))$.

Это же можно сформулировать так:

а) p – простой делитель $2^{q-1} - 1$,

б) p – простой делитель $U_{q-1}(P,Q)$.

(3) q – простой делитель $R(p) = gcd(2^{p-1} - 1,\, U_{p+1}(P,Q))$.

Это же можно сформулировать так:

а) q – простой делитель $2^{p-1} - 1$,

б) q – простой делитель $U_{p+1}(P,Q)$.

(4) $p, q > 2^{18}$ (граница может быть расширена).

(5) $gcd(\, ord(2,q),\, \rho(q,P,Q)\,) \le 2$.

(6) Для $q < 2^{34}$ имеется фиксированный список (331 число).

(7) $p \equiv 1 \mod ord(2,q)$, (здесь $ord(2,q)$ будет делителем $q-1$).

(8) $p \equiv -1 \mod \rho(q,P,Q)$, (здесь $\rho(q,P,Q)$ будет делителем $q-1$).

(9) $q \equiv 1 \mod ord(2,p)$, (здесь $ord(2,p)$ будет делителем $p-1$).

(10) $q \equiv 1 \mod \rho(p,P,Q)$, (здесь $\rho(p,P,Q)$ будет делителем $p+1$).

(11) $q > ord(2,p) \cdot \rho(p,P,Q)$.

(12) $(p-1)/ord(2,p) > ln(p)/4 + 1/2$.

3.4. Произведение нескольких простых с $J(D/p_i) = -1$

Напомним (определение 6), что через $L(p) = L(p,P,Q)$ обозначено число $LCM(ord(2,p),\, \rho(p,P,Q))$.

Теорема 16. *Пусть n – BPSW-псевдопростое, $n = p_1 \ldots p_k q$, где p_i – простые и $J(D,p_i) = -1$ при $i = 1,\ldots,k$ а q – произвольное. Обозначим через S_i произведение всех p_j, кроме p_i:*

$$S_i = p_1 \ldots p_k / p_i = n/(qp_i)\,.$$

Тогда

а) $qS_i \equiv 1 \mod L(p_i,P,Q) \quad i = 1,\ldots k$;

б) пусть d_{ij} – наибольший общий делитель $d_{ij} = gcd(L(p_i), L(p_j))$ для произвольных i,j. Тогда $(p_i - p_j)S_{ij}$ делится на d_{ij}, где $S_{ij} = S_i/p_j = S_j/p_i$ – произведение всех p_m, кроме p_i и p_j.

Следствие 5. *Пусть n – BPSW-псевдопростое, $n = p_1p_2q$, где p_i – простые и $J(D, p_i) = -1$ при $i = 1, 2$ а q – произвольное. Тогда*

а1) $qp_2 \equiv 1 \mod L(p_1)$,

а2) $qp_1 \equiv 1 \mod L(p_2)$,

б) $p_1 - p_2$ *делится на* $d_{12} = gcd(L(p_1), L(p_2))$.

Следствие 6. *Пусть n – BPSW-псевдопростое, $n = p_1p_2q$, где p_i – простые и $J(D, p_i) = -1$ при $i = 1, 2$ а q – произвольное. Тогда $p_1 - p_2$ делится на $gcd(ord(2, p_1), ord(2, p_2))$.*

4. BPSW-псевдопростые до 2^{64}

В этой главе рассматриваются только числа n, меньшие 2^{64}, BPSW-псевдопростые с параметром D, по модулю меньшим 128. Все вычисления проводились на процессоре AMD Athlon II X2 240, 2.8 GHz.

Согласно теореме (5), параметр D либо простой по модулю, либо равен -15.

Алгоритм проверки таков.

Шаг 1. Не существует BPSW-псевдопростых чисел вида $n = pq$, где p – простое, и $q < 2^{19}$.

Проверка с помощью теоремы (9). Проверять можно как на Мапле, так и на $C++$ с помощью GMP. Время – порядка суток.

Шаг 2. Не существует BPSW-псевдопростых чисел вида $n = pq$, где p – простое, $J(D/p) = +1$ и $p < 2^{34}$.

Числа p, меньшие 2^{34} (17.17 млрд), удовлетворяющие условиям теоремы (10) найдены при $|D| < 128$ и приведены в файле GCD_le_2bb.txt. При простых D и $D = -15$ их оказалось 170.

Эти 170 чисел надо проверять отдельно.

Шаг 3. Не существует BPSW-псевдопростых чисел вида $n = pq$, где p, q – простые, $J(D/p) = -1$, $J(D/q) = +1$, и $2^{19} < p < 2^{30}$.

Проверка с помощью теоремы (13). Для каждого простого p из указанного интервала перебираем все D, для каждой пары (p, D) находим $L = LCM(ord(2, p), \rho(p, P, Q))$ и перебираем все q, удовлетворяющие сравнению $q \equiv 1 \mod L(p, P, Q))$ и меньшие $2^{64}/p$.

При больших p величина L обычно оказывается большой и количество допустимых q либо вообще не будет, либо их будет мало. Поэтому перебор оказывается не слишком большим. Время – порядка двух суток.

После этих шагов можно сделать вывод, что не существует BPSW-псевдопростых чисел, меньших 2^{64}, являющихся произведением двух простых.

Список литературы

1. *Chen Z., Greene J.* Some Comments on Baillie–PSW Pseudoprimes // Fib. Quart. 2003. V. 41, № 4. P. 334–344.
2. *Crandall R. E.,Pomerance C.* Prime Numbers: a computational perspective, second edition. Springer : New York, 2005. 597 p.
3. *Jameson G.J.O.* Carmichael numbers and pseudoprimes. Lancaster Univ. UK. URL: http://www.maths.lancs.ac.uk/ jameson/carpsp.pdf (дата обращения: 20.09.2012).
4. *Lehmer D. H.* On Fermat's quotient, base two // Math. Comput., 1981. V. 36, № 153. P. 289–290.
5. *Ribenboim P.* My numbers, my friends: popular lectures on number theory. Springer, 2000. 392 p.
6. *Galway W.* Tables of pseudoprimes and related data. URL: http://www.cecm.sfu.ca/Pseudoprimes/index-2-to-64.html (дата обращения: 20.09.2012).

Поступила в редакцию 26.11.2012.