Известия вузов. Математика
2024, №4, с. 80–88

https://kpfu.ru/science/nauchnye-izdaniya/ivrm
e-mail: izvuz.matem@kpfu.ru

Краткое сообщение

Ш.Т. ИШМУХАМЕТОВ, Б.Г. МУБАРАКОВ, Р.Г. РУБЦОВА, Е.В. ОЛЕЙНИКОВА

О BAILLIE-PSW ГИПОТЕЗЕ

Аннотация. Baillie PSW-гипотеза была сформулирована в 1980 году и получила название по именам авторов (R. Baillie, C. Pomerance, J. Selfridge и S.Wagstaff). Гипотеза связана с проблемой существования нечетных чисел $n \equiv \pm 2 \pmod 5$, являющихся одновременно Ферма- и Лукас-псевдопростыми (кратко, FL-псевдопростыми). Ферма псевдопростым по базе a называется составное число n, удовлетворяющее условию $a^{n-1} \equiv 1 \pmod n$. База a выбирается равной 2. Псевдопростое по Лукасу - это составное n, удовлетворяющее $F_{n-e(n)} \equiv 0 \pmod n$, где $e(n)$ — символ Лежандра $e(n) = \left(\frac{n}{5}\right)$, F_m — m-й член ряда Фибоначчи.

Согласно Baillie PSW-гипотезе FL-псевдопростых чисел не существует. Если гипотеза верна, то комбинированный тест простоты, проверяющий условия Ферма и Лукаса для нечетных чисел, не делящихся на 5, дает верный ответ для всех чисел вида $n \equiv \pm 2 \pmod 5$, что порождает новый детерминированный полиномиальный тест простоты, определяющий простоту шестидесяти процентов всех нечетных чисел всего за две проверки.

В этой работе мы продолжили исследование FL-псевдопростых чисел, начатое в нашей статье "Об одном комбинированном тесте простоты", опубликованной в журнале "Изв. вузов. Матем." (12) за 2022, установили новые ограничения на вероятные FL-псевдопростые числа и описали новые алгоритмы проверки FL-простоты, с помощью которых доказали отсутствие таких чисел до границы $B = 10^{21}$, что больше, чем в тридцать раз превышают известную ранее границу 2^{64}, найденную J. Gilchrist в 2013 году. Также была исправлена неточность в формулировке теоремы 4 упомянутой статьи.

Ключевые слова: тест простоты Лукаса, тест Ферма, вероятностный тест простоты, детерминированный тест простоты.

УДК: 511.1

DOI: 10.26907/0021-3446-2024-4-80-88

Введение

Baillie-PSW тест — это комбинация теста Ферма с базой 2 и теста Лукаса. Впервые он был упомянут R. Baillie [1] и исследован в [2]. Этот тест используется для нечетных чисел, не делящихся на 5, и состоит из двух проверок. Первым проверяется условие Ферма

$$2^{n-1} \equiv 1 \pmod n. \tag{1}$$

Поступила в редакцию 25.12.2023, после доработки 25.12.2023. Принята к публикации 26.12.2023.

Благодарности. Работа выполнена за счет средств Программы стратегического академического лидерства Казанского (Приволжского) федерального университета ("ПРИОРИТЕТ-2030").

Если (1) ложно, то число n составное. Иначе проверим n тестом Лукаса ([3], с. 142)

$$F_{n-e(n)} \equiv 0 \pmod{n}, \tag{2}$$

где $\{F_n\} = \{0, 1, 1, 2, 3, 5, 8, \ldots\}$ — ряд Фибоначчи, и $e(n)$ — символ Лежандра

$$e(n) = \left(\frac{n}{5}\right) = \begin{cases} 1, & \text{если } n \equiv \pm 1 \pmod 5; \\ -1, & \text{если } n \equiv \pm 2 \pmod 5; \\ 0, & \text{если } n \equiv 0 \pmod 5. \end{cases}$$

Тест Лукаса основан на теореме Лукаса, которая утверждает, что для всех простых чисел $n > 5$, условие (2) истинно. Оба теста Ферма и Лукаса имеют собственные списки псевдопростых чисел, т. е. составных чисел, удовлетворяющие (1) и (2) [4]. Также существуют составные числа, проходящие оба этих теста. Однако не было найдено ни одного составного n, проходящего тесты (1) и (2) и эквивалентного $\pm 2 \pmod 5$. Проблема существования FL-псевдопростых чисел такого вида была также упомянута в 1984 году К. Померансом [5]. Некоторые модификации теста были рассмотрены Baillie, Fiori and Wagstaff [6] в 2018 году. В этой статье указана наивысшая нижняя граница 2^{64} для потенциальных FL-псевдопростых чисел.

Также эта проблема упомянута в работе [7] и Википедии [4]. В работе [8] нами были выведены некоторые ограничения на возможные FL-псевдопростые числа. Близкие результаты можно найти в [9].

1. Основные определения.

Определение 1. FL-*псевдопростым по базе* 2 (FLpp) *называется нечетное составное число* n, *удовлетворяющее условиям* (1) *и* (2). FLpp *число* n, *удовлетворяющее условию* $n \equiv \pm 2 (\mathrm{mod}\, 5)$, *будем называть* FL2-*псевдопростым* (FL2pp).

Определение 2. *Пусть произвольное* n *удовлетворяет условию* $2^{n-1} \equiv 1 (\mathrm{mod}\ n)$. *Через* $ord_2 n$ *обозначим наименьшее* k *такое, что* $2^k \equiv 1 (\mathrm{mod}\ n)$.

Определение 3. *Пусть число* n *удовлетворяет условию* $F_k \equiv 0 (\mathrm{mod}\ n)$ *для некоторого числа* k. *Обозначим через* $ord_F n$ *наименьшее* k *такое, что выполняется* $F_k \equiv 0 (\mathrm{mod}\ n)$.

2. Формулы для вычисления членов ряда Фибоначчи. Напомним основные формулы для вычисления членов ряда Фибоначчи:

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n;$$

$$\begin{aligned} F_{2n} &= F_n(2F_{n+1} - F_n), \\ F_{2n+1} &= F_{n+1}^2 + F_n^2; \end{aligned} \tag{3}$$

$$\begin{aligned} F_{k+m} &= F_{m-1}F_k + F_m F_{k+1}, \\ F_{k+m+1} &= F_m F_k + F_{m+1}F_{k+1}. \end{aligned} \tag{4}$$

3. Основные результаты. При желании эти результаты читатель может найти в монографии [10].

Лемма 1. *Пусть* a *и* k *— произвольные числа. Тогда*

$$F_a \,|\, F_{ka}. \tag{5}$$

Схема доказательства. Покажем (5) индукцией по k. Случай $k = 2$ следует из формул (3). Индукционное утверждение вытекает из

$$F_{(k+1)a} = F_{ka+a} = F_{ka-1}F_a + F_{ka}F_{a+1}$$

и индукционного предположения $F_a \,|\, F_{ka}$.

Лемма 2. *Пусть a и m — положительные числа. Если выполняется $F_m \equiv 0 \,(\mathrm{mod}\, a)$, то $ord_F a \,|\, m$.*

Схема доказательства. Для $a = 1$ утверждение очевидно, поэтому рассмотрим случай $a \geq 2$. Обозначим $h = ord_F a$. Если m не кратно h, то остаток r от деления m на h больше нуля. Обозначим $t = (m - r)/h$. Тогда $m = r + th$ и по формулам (4)

$$F_m = F_{r+th} = F_r F_{th-1} + F_{th} F_{r+1},$$

F_m кратно a по условию, F_h кратно a по определению, F_{th} кратно a по лемме 1, значит, $F_r F_{th-1}$ тоже кратно a, причем F_{th-1} не делится на a (иначе, все слагаемые ряда Фибоначчи делятся на a). Значит, F_r делится на a, и h не является наименьшим числом со свойством $F_h \equiv 0 \,(\mathrm{mod}\, a)$.

Лемма 3. *Пусть a и k — произвольные числа. Тогда*

$$ord_F a \,|\, ord_F ka.$$

Схема доказательства. Пусть h и m обозначают $ord_F a$ и $ord_F ka$ соответственно. По определению $F_m \equiv 0 (\mathrm{mod}\ ka)$. Значит, $F_m \equiv 0 (\mathrm{mod}\ a)$ и $h | m$ по лемме 2.

В следующей теореме мы сформулируем ограничения, которым должны удовлетворять FL2-псевдопростые числа. Часть утверждений была доказана раньше в статье [8]. К сожалению, утверждение теоремы 4 этой статьи содержало ошибку. Сейчас мы устранили эту ошибку и установили новые ограничения на FL2-псевдопростые числа.

Введем обозначения: $A \bmod B$ — положительный остаток от деления A на B, $Inv(a, b)$ — наименьшее положительное решение уравнения $a \cdot x \bmod b = 1$. Для произвольного r обозначим $d(r) = GCD(ord_2 r, ord_F r)$ и $H(r) = LCM(ord_2 r, ord_F r)$.

Теорема 1. *Пусть n является* FL2pp*-числом. Тогда*

1) *если r — произвольный делитель числа n, то оба порядка $ord_2 r$, $ord_F r$ существуют и*

$$d(r) \in \{1, 2\}; \tag{6}$$

2) *если r — простой делитель n, $m = n/r$, то*

$$r \mid GCD(2^{m-1} - 1, F_{m+e(r)}); \tag{7}$$

3) *если p — простой делитель n, удовлетворяющий $p \equiv \pm 2 \pmod 5$, то*

$$H(p) \mid m - 1, \quad m = n/p; \tag{8}$$

4) *если q — простой делитель n, удовлетворяющий $q \equiv \pm 1 \pmod 5$, то*

$$H(q) \mid q - 1; \tag{9}$$

5) *если $q \equiv \pm 1 \pmod 5$ — простой делитель n, то*

$$m = m_0 + t \cdot H(q), \ \text{где } m = n/q, \ t \in N,$$

и значение m_0 зависит от четности порядков $ord_2 q$, $ord_F q$.

Схема доказательства. 1) По условию теоремы $2^{n-1} \equiv 1 \pmod n$, откуда $2^{n-1} \equiv 1 \pmod r$ и $ord_2 r \mid n-1$. Далее n удовлетворяет (2) и $e(n) = \left(\frac{n}{5}\right) = -1$, отсюда $ord_F n \mid n+1$. Значит, $F_{n+1} \equiv 0 \pmod n$ и $F_{n+1} \equiv 0 \pmod r$. По лемме 2 $ord_F r \mid n+1$. Из условий $ord_2 r \mid n-1$ и $ord_F r \mid n+1$ сразу получим (6).

2) По условию теоремы $ord_2 r \,|\, n-1$ и по малой теореме Ферма $ord_2 r \,|\, r-1$. Так как $n-1 = rm-1 = (r-1)m + m - 1$, то $ord_2 r \,|\, m-1$. Последнее эквивалентно условию $2^{m-1} \equiv 1 (\mathrm{mod}\, r)$, или $2^{m-1} - 1 \equiv 0 (\mathrm{mod}\, r)$. Также по условию теоремы $ord_F r \,|\, n+1$ и по теореме Лукаса $ord_F r \,|\, r - e(r)$. Поскольку $n+1 = rm+1 = (r-e(r))m + e(r)m + 1$, то $ord_F r \,|\, e(r)m+1$. Если $r \equiv \pm 1 \pmod 5$, то $e(r) = 1$ и $ord_F r \,|\, m+1$. В случае $r \equiv \pm 2 \pmod 5$, $e(r) = -1$ и $ord_F r \,|\, m-1$. Значит, $F_{m+e(r)} \equiv 0 \pmod r$. Отсюда получим (7).

3) Далее, пусть p — простой делитель n, $p \equiv \pm 2 \pmod 5$, $m = n/p$. По п. 1) теоремы $ord_2 p \mid n-1$, $ord_F p \mid n+1$. Согласно малой теореме Ферма $ord_2 p \mid p-1$. Из соотношения $n-1 = pm-1 = (p-1)m + m - 1$ получим $ord_2 p \mid m-1$. По теореме Лукаса $ord_F p \mid p+1$. Из равенства $n+1 = pm+1 = (p+1)m - (m-1)$ получим $ord_F p \mid m-1$. Отсюда $H(p) \,|\, m-1$.

4) Пусть теперь q — простой делитель n, удовлетворяющий $q \equiv \pm 1 \pmod 5$. Тогда оба порядка $ord_2 q$ и $ord_F q$ являются делителями $q-1$. Так как $H(q) = LCM(ord_2 q, ord_F q)$, то $H(q) \,|\, (q-1)$.

5) Обозначим $h_1 = ord_2 q$, $h_2 = ord_F q$. Аналогично п. 3) можно доказать $h_1 \,|\, m-1$, $h_2 \,|\, m+1$, отсюда

$$m + 1 = 2 + t_1 h_1 = t_2 h_2, \quad t_1, t_2 \in N.$$

Рассмотрим два случая:

1. h_1 и h_2 взаимно просты. Обозначим $g = inv(h_2, h_1)$. Имеем $t_2 h_2 \equiv 2 \,(\mathrm{mod}\, h_1)$, откуда $t_2 \equiv 2g \,(\mathrm{mod}\, h_1)$. Подставляя t_2 в выражение для m, получим $m_0 = -1 + 2g \cdot h_2$.

2. $GCD(h_1, h_2) = 2$. Обозначим $h_1' = h_1/2$, $h_2' = h_2/2$, $g = inv(h_2', h_1')$. Теперь $t_2 h_2' \equiv 1 \,(\mathrm{mod}\, h_1')$, и $t_2 \equiv g \,(\mathrm{mod}\, h_1')$. Подставляя t_2 в выражение для m, получим $m_0 = -1 + g \cdot h_2$. □

Формула (10) ниже заменяет неверное утверждение теоремы 4 из [8] (отличается дополнительным множителем t перед функцией $H(p)$).

Следствие. *Пусть* FL2pp *число n содержит простой делитель $p \equiv \pm 2 \pmod 5$, тогда*

$$n = p(1 + tH(p)), \quad \textit{где } t \in \mathbf{N}. \tag{10}$$

Схема доказательства. Представление (10) непосредственно следует из условия (8).

В следующих пунктах мы опишем алгоритмы для поиска FL2pp чисел. Отметим, что потенциальное FL2pp число n представляет собой произведение нечетного числа простых чисел вида $p \equiv \pm 2 \pmod 5$ и произвольного числа простых чисел вида $q \equiv \pm 1 \pmod 5$. Простейшее FL2pp число имеет вид $n = pq$, где $p \equiv \pm 2 \pmod 5$ и $q \equiv \pm 1 \pmod 5$ — простые числа.

4. Вспомогательные алгоритмы. Рассмотрим сначала алгоритм отсеивания простых чисел $q \equiv \pm 1 \pmod 5$, не удовлетворяющих одновременно (6) и (9). Отметим, что вычисление обоих порядков $ord_2 q$ и $ord_F q$ требует разложения на множители числа $q-1$, что является процедурой с экспоненциальной сложностью.

Алгоритм 1.1. *Поиск простых $q \equiv \pm 1 \pmod 5$, не удовлетворяющих одновременно* (6) *и* (9).

Выполняем цикл по всем простым числам вида $q \equiv \pm 1 \pmod 5$ до некоторой границы B_0. Для каждого такого q вычислим $h_1 = ord_2 q$, $t = (q-1)/h_1$, $g = GCD(h_1, t)$ и $h = 2t/g$. По выбору h должно выполняться условие $ord_F q \,|\, h$. Проверим условие $F_h \equiv 0 \pmod q$. Если оно выполняется, то сохраним q как потенциальный делитель FL2-псевдопростого n.

Рассмотрим далее некоторую оптимизацию этого алгоритма, основанную на том, что для большинства простых чисел q порядки $ord_2 q$ и $ord_F q$ близки к q. Тогда $ord_2 q \cdot ord_F q > 2(q-1)$ и (9) не выполняется.

Алгоритм 1.1m. Перебираем простые числа $q \equiv \pm 1 \pmod 5$ и, используя пробные деления, раскладываем $q-1$ в произведение $m \cdot s$, где s — произведение всех простых делителей $q-1$ до некоторой небольшой границы, например, $B = 23$. Далее ρ-методом Полларда находим простой делитель d сомножителя m. Очевидно, $d > B$. Пусть $t = (p-1)/d$. Далее, вычисляем $b_1 = 2^t \bmod p$ и $b_2 = F_t \bmod p$. Если d является делителем обоих порядков $ord_2 q$ и $ord_F q$, то выполняются условия $b_1 \neq 1$ и $b_2 \neq 0$ и можно отбросить q, как не удовлетворяющий (6). В противном случае надо проверить q с помощью алгоритма 1.

Эмпирические вычисления показали, что менее 1% чисел q проходит положительную проверку алгоритмом 1m, поэтому модифицированный алгоритм работает на порядок быстрее. Мы реализовали данный алгоритм на мультипроцессорном кластере Казанского федерального университета и выполнили этот алгоритм до границы $B_0 = 3,25 \cdot 10^{12}$. Обозначим через L_0 список найденных чисел q. На текущий момент L_0 состоит из семи чисел:

$$L_0 = \{61681, 363101449, 4562284561, 4582537681, 26509131221, 422013019339, 2502586966001\}.$$

Алгоритм 1.2. *Отсеивание нечетных* $m \equiv \pm 2 \pmod 5$, *не являющихся делителями* FL2pp *чисел* $n = mq$, q *простое.*

Пусть m удовлетворяет $m \equiv \pm 2 \pmod 5$. Если найдется FL2pp число $n = mq$ с делителем $q \equiv \pm 1 \pmod 5$, то согласно теореме 1 для m выполняется условие

$$q \,|\, D(m) = GCD(2^{m-1} - 1, F_{m+1}).$$

В силу этого условия строим наш алгоритм. Для уменьшения размера рассматриваемых чисел разбиваем $2^{m-1} - 1$ в произведение $(2^{(m-1)/2} - 1)(2^{(m-1)/2} + 1)$.

1. Перечисляем нечетные числа $m \equiv \pm 2 \pmod 5$, начиная с 3, и вычисляем $M_1(m) = 2^{(m-1)/2} - 1$ и $M_2(m) = 2^{(m-1)/2} + 1$.

2. Вычисляем $h_1 = F_{m+1} \bmod M_1(m)$, $h_2 = F_{m+1} \bmod M_2(m)$, $g_1 = GCD(h_1, M_1(m))$, $g_2 = GCD(h_2, M_2(p))$, $D = g_1 \cdot g_2$. Методом пробных делений отсекаем от D небольшие делители, например, до $d = 31$.

3. Используя ρ-метод Полларда, раскладываем $D(m)$ в произведение простых чисел: $D = \prod_i q_i^{s_i}$. Возможные делители q находятся среди сомножителей q_i. Искомые делители должны удовлетворять условиям $q_i \equiv \pm 1 \pmod 5$ и $q_i > B_0$. Если такое q найдется, то $n = mq$ проверим тестами (1) и (2).

Этот алгоритм работает достаточно быстро, так как очень небольшое число делителей $D(m)$ оказывается больше B_0. Мы проверили с помощью данного алгоритма все нечетные $m \equiv \pm 2 \pmod 5$ до границы $B_1 = 1,54 \cdot 10^6$.

Алгоритм 1.3. *Просеивание потенциальных* FL2pp *чисел* $n = mq$, $q \in L_0$.

1. Для каждого $q \in L_0$ вычисляем $h_1 = ord_2 q$ и $h_2 = ord_F q$. Значение m вычисляется по формулам п. 5) теоремы 1. Если порядки h_1, h_2 взаимно просты, то вычисляем $g = Inv(h_2, h_1)$ и $m_0 = -1 + 2gh_2$. В противном случае $g = Inv(h_2/2, h_1/2)$ и $m_0 = -1 + gh_2$.

2. Открываем новый цикл по t и проверяем потенциальные FL2pp числа $n = m_t q$, где $m_t = m_0 + tH(p)$ тестами (1) и (2).

С помощью этого алгоритма мы проверили всевозможные пары $n = mq$, $q \in L_0$, до границы $B = 2^{80}$. Значит, до этой границы не найдется FL2pp чисел, содержащих элементы списка L_0 в качестве делителей. Отсюда также получаем, что наименьший простой делитель $q \equiv \pm 1 \pmod 5$ FL2pp числа $n \le 2^{80} \approx 10^{24,2}$ должен быть больше $B_0 \approx 2,5 \cdot 10^{12}$. Если принять гипотезу о том, что $H(q) \ge (q-1)/4$, выполняющееся для всех $q < B_0$, кроме единственного $q = 4562284561$, то по п. 5) теоремы 1 оставшийся множитель m будет больше $H(q) > B_0/4$, что дает нижнюю оценку для FL2pp чисел, содержащих делитель $q \equiv \pm 1 \pmod 5$ не ниже $B_0^2/4 \approx 10^{24} \approx 2^{80}$.

5. Поиск FL2pp чисел n с делителем $q \equiv \pm 1 \pmod 5$. Отметим, что каждое такое FL2pp число должно содержать также делитель $p \equiv \pm 2 \pmod 5$, который будет больше $B_0 B_1 \approx 5 \cdot 10^{18}$. Уточним эту границу с помощью следующих алгоритмов.

Алгоритм 2. *Поиск* FL2pp $n = pq$, p, q *простые,* $p \equiv \pm 2 \pmod 5$.

Организуем внешний цикл по простым $p \equiv \pm 2 \pmod 5 > B_1$. Для каждого такого p открываем внутренний цикл по переменной t и вычисляем $q_t = 1 + tH(m)$, $q_t > B_0$, $q_t \equiv \pm 1 \pmod 5$. Проверяем q_t на простоту алгоритмом Миллера–Рабина и далее алгоритмом 1.1m. В случае положительного прохождения проверяем $n = pq_t$ тестами (1) и (2). Алгоритм 2 работает быстро. Он был реализован до границы $B = 2^{76} \approx 4,7 \cdot 10^{21}$.

Если n содержит более двух простых делителей, то возможны следующие варианты:

1. n содержит два или более делителей $\equiv \pm 1 \pmod 5$. Также n должно содержать как минимум один делитель $p \equiv \pm 2 \pmod 5$, значит, $n > B_0^2 \cdot B_1 > 8 \cdot 10^{30}$.

2. n содержит три или более делителей $\equiv \pm 2 \pmod 5$ и как минимум один делитель $\equiv \pm 1 \pmod 5$. Тогда $n > B_0 B_1^3 > 7,5 \cdot 10^{30}$.

3. n не содержит делителей $\equiv \pm 1 \pmod 5$ и представляет собой произведение k простых делителей $\equiv \pm 2 \pmod 5$, $k \ge 3$ нечетно. Каждый делитель такого числа больше $B_1 = 1,25 \cdot 10^6$, значит, при $k \ge 5$ $n \ge B_1^5 \approx 3 \cdot 10^{25}$. Поэтому достаточно рассмотреть случай $k = 3$.

6. FL2pp числа, не содержащие делителей $q \equiv \pm 1 \pmod 5$. Для проверки чисел этого типа понадобится

Теорема 2. *Пусть* FL2-*псевдопростое число* $n = pqm$ *содержит простые делители* p *и* q, *эквивалентные* $\pm 2 \pmod 5$. *Тогда оставшийся делитель* $m = n/pq = m_0 + tH(p)H(q)/d$, *где* $t \in N$,

$$m_0 = q' + ((p'-q')H'/d) \bmod H(q)\cdot H(p),\ p' = Inv(p, H(q)),\ q' = Inv(q, H(p)),$$
$$d = GCD(p'-q', H(p)),\ H' = Inv(H(p)/d, H(q)). \tag{11}$$

Схема доказательства. Согласно п. 3) теоремы 1 $H(p) \mid qm - 1$, отсюда $qm \equiv 1 \pmod{H(p)}$. Аналогично $pm \equiv 1 \pmod{H(q)}$. Значит,

$$\begin{aligned} qm &\equiv 1 \pmod{H(p)}, \\ pm &\equiv 1 \pmod{H(q)}. \end{aligned} \tag{12}$$

Обозначим $p' = Inv(p, H(q))$, $q' = Inv(q, H(p))$. Если система (12) имеет решение, найдутся целые числа t_1, t_2 такие, что $m = q' + t_1 H(p) = p' + t_2 H(q)$. Следовательно, $t_1 H(p) \equiv p' - q' \pmod{H(q)}$. Пусть $d = GCD(p'-q', H(p))$. Система (12) имеет решение только в случае, если $H(p)/d$ и $H(q)$ взаимно-простые. Это решение определяется формулой (11).

Пример. Пусть $p = 7$, $q = 233$. Тогда $H(p) = 24$, $H(q) = 377$, $p' = Inv(7, 377) = 54$, $q' = Inv(233, 24) = 17$, $d = 1$, $H' = Inv(24, 377) = 110$. Значит, $m_0 = 17+24((54-17)110 \bmod 377) = 17 + (37 \cdot 110 \bmod 377) \cdot 24 = 7217$, $\quad m = m_0 + tH(p)H(q) = 7217 + 9048t,\ t \in Z$.

Алгоритм 2. *Поиск* FL2pp *чисел* $n = pqr$, $p, q, r \equiv \pm 2 \pmod 5$ *простые.*

1. Для каждого простого $p \equiv \pm 2 \pmod 5$ $B_1 \le p < 10^7$ вычислим $H(p)$ и сохраним пары $(p, H(p))$ в текстовый файл *List.txt*.

2. В цикле перебираем пары простых чисел p, q из файла *List.txt* и для каждой пары вычисляем $H(p)$, $H(q)$ и d. Вычисляем $GCD(H(p), H(q)/d$. Если он не равен 1, то отбрасываем пару p, q. Иначе, вычисляем r_0 и $h = H(p)H(q)/d$ и переходим к следующему пункту.

3. Открываем новый цикл по переменной t и вычисляем $r_t = r_0 + t \cdot h \equiv \pm 2 \pmod 5$, $B_1 < r_t < 10^7$. Проверяем s_t тестом Миллера–Рабина. Если s_t не просто, то отбрасываем его. Иначе, проверим $n = pqs_t$ тестами (1) и (2).

Этот алгоритм был выполнен для всех $p, q, s < 10^7$, что показывает отсутствие FLM2pp чисел, представляющих собой произведение трех простых чисел: $p, q, s \equiv \pm 2 \pmod 5$ до границы 10^{21}.

Заключение. В нашей статье мы получили новые ограничения на потенциальные FL2pp числа, на основе которых построили эффективные алгоритмы поиска таких чисел. С помощью компьютерных вычислений была найдена нижняя граница для потенциальных FL2pp чисел, равная $10^{21} \approx 2^{69}$, что примерно в тридцать раз выше границы 2^{64}, известной ранее.

Литература

[1] Baillie R., Wagstaff S.S., Jr. *Lucas Pseudoprimes* (PDF), Math. Comp. **35** (152), 1391–1417 (1980). http://mpqs.free.fr/LucasPseudoprimes.pdf

[2] Pomerance C., Selfridge J.L., and Wagstaff S.S., Jr. *The Pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (151), 1003–1026 (1980). https://doi.org/10.1090/S0025-5718-1980-0572872-7, https://math.dartmouth.edu/ carlp/PDF/paper25.pdf

[3] Crandall R., Pomerance C.B. *The Prime Numbers: A Computational Perspertive*. R. Crandall, C. Pomerance. – sec. ed. (Springer–Verlag, Berlin, 2005).

[4] Wikipedia. Baillie–PSW primality test. https://en.wikipedia.org/wiki/Baillie–PSW_primality_test

[5] Pomerance C. *Are There Counterexamples to the Baillie–PSW Primality Test*? In H.W. Lenstra, Jr., J.K. Lenstra, and P. Van Emde Boas (Eds.), Amsterdam, 1984. http://www.pseudoprime.com/dopo.pdf

[6] Baillie R., Fiori A., Wagstaff S.S., Jr. *Strengthening the Baillie-PSW primality test*. Zbl 1478.11152 Math. Comput. **90** (330), 1931–1955 (2021).

[7] Weisstein E.W. *Baillie-PSW Primality Test*. http://mathworld.wolfram.com/Baillie-PSWPrimalityTest.html

[8] Ишмухаметов Ш.Т., Антонов Н.А., Мубараков Б.Г., Рубцова Р.Г. *Об одном комбинированном тесте простоты*, Изв. вузов. Матем. (12), 123–129 (2022). DOI: https://doi.org/10.26907/0021-3446-2022-12-123-129.

[9] Ishmukhametov S., Antonov N., Mubarakov B. *On a modification of the Lucas Primality Test*, Lobachevskii J. Math. **50** (7), 1–8 (2023).

[10] Wall D.D. *Fibonacci series modulo m*, Amer. Math. Monthly **67** (6), 525–532 (1960).

Шамиль Талгатович Ишмухаметов

Казанский федеральный университет,
ул. Кремлевская, д. 18, г. Казань, 420008, Россия,

e-mail: sishmukh@kpfu.ru

Булат Газинурович Мубараков

Казанский федеральный университет,
ул. Кремлевская, д. 18, г. Казань, 420008, Россия,

e-mail: mubbulat@mail.ru

Рамиля Гакилевна Рубцова

Казанский федеральный университет,
ул. Кремлевская, д. 18, г. Казань, 420008, Россия,

e-mail: rrubtsov@kpfu.ru

Елизавета Витальевна Олейникова

Московский политехнический университет,
ул. Большая Семеновская, д. 38, г. Москва, 107023, Россия,

e-mail: liz.ol@mail.ru

Sh.T. Ishmukhametov, B.G. Mubarakov, R.G. Rubtsova, and E.V. Oleynikova

On the Baillie PSW-conjecture

Abstract. The Baillie PSW hypothesis was formulated in 1980 and was named after the authors R. Baillie, C. Pomerance, J. Selfridge and S. Wagstaff. The hypothesis is related to the problem of the existence of odd numbers $n \equiv \pm 2 \pmod 5$, which are both Fermat and Lucas-pseudoprimes (in short, FL-pseudoprimes). A Fermat pseudoprime to base a is a composite number n satisfying the condition $a^{n-1} \equiv 1 \pmod n$. Base a is chosen to be equal to 2. A Lucas pseudoprime is a composite n satisfying $F_{n-e(n)} \equiv 0 \pmod n$, where $n(e)$ is the Legendre symbol $e(n) = \left(\frac{n}{5}\right)$, F_m the mth term of the Fibonacci series.

According to Baillie's PSW conjecture, there are no FL-pseudoprimes. If the hypothesis is true, the combined primality test checking Fermat and Lucas conditions for odd numbers not divisible by 5 gives the correct answer for all numbers of the form $n \equiv \pm 2 \pmod 5$, which generates a new deterministic polynomial primality test detecting the primality of 60 percent of all odd numbers in just two checks.

In this work, we continue the study of FL-pseudoprimes, started in our article "On a combined primality test" published in the journal "Izvestia VUZov.Matematika" No. 12 in 2022. We have established new restrictions on probable FL-pseudoprimes and described new algorithms for checking FL-primality, and with the help of them we proved the absence of such numbers up to the boundary $B = 10^{21}$, which is more than 30 times larger than the previously known boundary 2^{64} found by J. Gilchrist in 2013. An inaccuracy in the formulation of theorem 4 in the mentioned article has also been corrected.

Keywords: primality test, Lucas primality test, Fermat Small theorem, deterministic primality test.

Shamil Talgatovich Ishmukhametov

Kazan Federal University,
18 Kremlyovskaya str., Kazan, 420008 Russia,

e-mail: sishmukh@kpfu.ru

Bulat Gazinurovich Mubarakov

Kazan Federal University,
18 Kremlyovskaya str., Kazan, 420008 Russia,

e-mail: mubbulat@mail.ru

Ramilya Gakilevna Rubtsova

Kazan Federal University,
18 Kremlyovskaya str., Kazan, 420008 Russia,

e-mail: rrubtsov@kpfu.ru

Elizaveta Vitalievna Oleynikova

Moscow Polytechnic University,
38 Bolshaya Semenovskaya str., Moscow, 107023 Russia,

e-mail: liz.ol@mail.ru