**Выводы**. То, будет ли у задачи линейного программирования решение или нет (функция цели $(C, X) \to -\infty$), не зависит от $B$, а определяется лишь $A$ и $C$. Матрица $B$ влияет на то, пусто множество $M$ или нет.

***Библиографический список***

1. *Гасс С.* Линейное программирование : (методы и приложения). М. : Физматгиз, 1961. 303 с.
2. *Гельфанд И. М.* Лекции по линейной алгебре. М. : ГИТТЛ, 1951. 252 с.
3. *Данциг Дж.* Линейное программирование, его применения и обобщения. М. : Прогресс, 1966. 600 с.

**УДК 519.67**

***В. Д. Голубев, С. И. Хашин***

# ЧИСЛА, ПСЕВДОПРОСТЫЕ ПО ФРОБЕНИУСУ, БЕЗ БОЛЬШИХ ДЕЛИТЕЛЕЙ

Доказано, что если метод Фробениуса проверки чисел на простоту ошибается на некотором числе $n \equiv 3 \pmod 4$, то у него обязательно есть простой делитель, больший 2707. Таким образом, найден еще один факт, свидетельствующий в пользу гипотезы о том, что чисел, псевдопростых по Фробениусу, не существует.

***Ключевые слова:*** проверка простоты числа, метод Фробениуса, метод Миллера — Рабина.

It is proved that if the Frobenius method of primality test have an error on number $n \equiv 3 \pmod 4$, then it necessarily has a prime divisor greater than 2707. Thus, we find one more fact that supports the hypothesis that there are no Frobenius pseudoprimes.

***Key words:*** prime numbers, primality test, Frobenius method, Miller — Rabin method.

## 1. Введение

**Определение 1.** Пусть $n$ — нечетное натуральное число, не являющееся полным квадратом. Его *индексом Фробениуса* $\mathrm{Ind}_F(n)$ будем называть наименьшее среди чисел $[-1, 2, 3, 4, 5, 6, \dots]$ такое, что символ Якоби $J(c/n) \neq 1$.

**Определение 2.** Пусть $n$ — нечетное натуральное число, не являющееся полным квадратом, и пусть $c = \mathrm{Ind}_F(c)$ — его индекс Фробениуса. Пусть

$$z = \begin{cases} 2 + \sqrt{c}, & c = -1, 2; \\ 1 + \sqrt{c}, & c \geq 3. \end{cases}$$

Будем называть $n$ *простым по Фробениусу* [2, 3, 6], если

$$z^n \equiv \overline{z} \pmod n.$$

**Определение 3.** Если составное число просто по Фробениусу, то будем называть его *псевдопростым по Фробениусу (Frobenius pseudoprime, FPP).*

**Пример 1.** Пусть $n = 19$. Тогда $c = -1$, $z = 2 + i$,

$$z^n = -3565918 + 2521451i \equiv 2 - i \pmod{n}.$$

**Пример 2.** Пусть $n = 33$. Тогда $c = -1$, $z = 2 + i$,

$$z^n \equiv 2 + 22i \neq \overline{z} \pmod{n}.$$

**Пример 3.** Пусть $n = 17$. Тогда $c = 3$, $z = 1 + \sqrt{3}$,

$$z^n = 13160704 + 7598336\sqrt{3} \equiv 1 - \sqrt{3} \pmod{n}.$$

Известно [3], что не существует FPP, меньших $2^{64}$. Также доказано [1], что не существует кратных множителей, меньших $2^{32}$.

В настоящей работе рассматриваются числа $n$, псевдопростые по Фробениусу, такие, что $n \equiv 3 \pmod 4$, и доказывается, что у них обязательно должен быть простой множитель, больший 2707.

## 2. Согласованные простые делители

Пусть $n$ есть FPP и пусть $p$ — его простой делитель. Тогда

$$n \equiv p \pmod{Q_p},$$

где $Q_p$ — порядок числа $z$ по модулю $p$.

Если мы рассмотрим два простых делителя $p_1$ и $p_2$, то получим:

$$n \equiv p_1 \pmod{Q_{p_1}},$$
$$n \equiv p_2 \pmod{Q_{p_2}}.$$

Объединяя эти два сравнения, получим:

$$p_1 \equiv p_2 \pmod{\mathrm{GCD}(Q_{p_1}, Q_{p_2})}.$$

Такую пару простых чисел будем называть согласованной.

## 3. Алгоритм работы

Представим алгоритм для поиска псевдопростых по Фробениусу чисел. Возьмем 30 000 простых чисел, у которых индекс Фробениуса равен $-1$, т. е. $n \equiv 3 \pmod 4$, будем называть их допустимыми.

Будем предполагать, что $n$ раскладывается на нечетное количество различных допустимых множителей $n = p_0 p_1 \cdots p_k$. Как было сказано выше, каждая пара этих простых чисел должна быть согласованной.

Алгоритм состоит в переборе всех подмножеств множества допустимых простых чисел, каждая пара в котором является согласованной.

Возьмем допустимое $p_0$. Строим для него список согласованных с ним чисел. Выбираем из него по очереди всевозможные числа $p_1$, согласованные с $p_0$, и строим список чисел, согласованных с $p_0$, $p_1$. Выбираем из него по очереди всевозможные $p_2$, строим список согласованных с $p_0$, $p_1$, $p_2$ чисел. Проверяем, не является ли произведение чисел $p_0 p_1 p_2$ FPP.

Далее выбираем из построенного списка по очереди $p_3$. Строим список согласованных чисел с $p_0$, $p_1$, $p_2$, $p_3$ и т. д., пока не переберем все.

Алгоритм был реализован с помощью обхода дерева в глубину:

1) пытаемся добавить еще один множитель в произведение, т. е. увеличить текущее количество согласованных сомножителей, при этом заполняя массив, состоящий из простых чисел;

2) если добавить сомножитель не получается, пытаемся «пойти вправо» на дереве;

3) если «пойти вправо» не получается, то уменьшаем высоту и снова идем вправо.

## 4. Результаты работы

Для реализации описанных алгоритмов была написана программа на языке C++ (Visual C++ 2013 [4]). Для работы с числами произвольной длины на сегодняшний день наиболее популярны и эффективны библиотеки GMP [5] и MPIR [7]. В нашем случае более подходящей оказалась библиотека MPIR.

Вычисления были выполнены на компьютере с процессором Intel ® Pentium ® CPU G4500 @ 3.50GHz.

При всех вычислениях требуемое количество памяти было сравнительно незначительным, нигде не требовался даже 1 Гбайт, поэтому объем памяти ограничителем не являлся, проблему составляло только время работы.

Если взять одну сотню простых чисел (максимальное $p = 1223$), то полный перебор всех возможных произведений — менее минуты. Но для обработки 200 простых чисел (до 2707) потребовалось уже более суток! Учитывая столь быстрый рост объема вычислений, следует признать, что дальнейшее увеличение границы подобным способом практически невозможно. Для этого требуется разработать существенно более эффективные методы.

В результате работы программы получились следующие результаты: не существует чисел, псевдопростых по Фробениусу, раскладывающихся в произведение множителей, каждый из которых не превосходит 2707.

Таким образом, найден еще один факт, свидетельствующий в пользу гипотезы о том, что чисел, псевдопростых по Фробениусу, не существует.

### *Библиографический список*

1. *Хашин С. И.* Кратные множители псевдопростых чисел // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2013. Вып. 2. С. 102—107.
2. *Хашин С. И.* Натуральные числа с большим индексом Фробениуса // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2015. Вып. 2. С. 75—78.
3. *Хашин С. И., Хашина Ю. А.* Свойства чисел, псевдопростых по Фробениусу // Вестник Ивановского государственного университета. Сер.: Естественные, общественные науки. 2014. Вып. 2. С. 104—108.
4. Центр загрузки Microsoft. URL: https://www.microsoft.com/ru-ru/download (дата обращения: 20.03.2018).
5. GMP: The GNU Multiple Precision Arithmetic Library. URL: http://gmplib.org (дата обращения: 20.03.2018).
6. *Khashin S. I.* Counterexamples for Frobenius primality test // arXiv:1307.7920. URL: https://arxiv.org/abs/1307.7920 (дата обращения: 06.04.2018).
7. MPIR: Multiple Precision Integers and Rationals. URL: http://www.mpir.org (дата обращения: 20.03.2018).