# Об использовании малой теоремы Ферма и ее аналогов в криптографии

Ш. Т. Ишмухаметов*, А. А. Курбангалеев‡, Б. Г. Мубараков§, Р. Г. Рубцова¶

В этой статье мы рассмотрим важную задачу криптографии: построение тестов простоты для генерации простых чисел большой размерности. Мы предлагаем усиление существующих методов путем использования аналогов малой теоремы Ферма.

**Ключевые слова:** тест простоты, конечные поля, факторизация, криптографические протоколы, эллиптические кривые, метод Люка, метод Вильямса.

## 1. Введение

Мы опишем новый подход к построению тестов простоты. Тест простоты – это процедура, определяющая, является ли заданное натуральное число простым или составным. В настоящее время в криптографии используются вероятностные тесты, которые иногда делают ошибки, оценивая составные числа как вероятно простые. Наш подход заключается в уменьшении вероятности ошибок или сведению их к нулю путем комбинирования применяемых в криптографии методов с малой теоремой Ферма или ее аналогов ([1], [2], [3]). Сформулируем малую теорему Ферма. Пусть $p$–простое число, $a \not\equiv 0 \pmod{p}$, тогда

$$a^{p-1} \equiv 1 \pmod{p} \tag{1}$$

Обращение этой теоремы неверно. С другой стороны, вероятность выполнения соотношения (1) для составного числа достаточна мала и позволяет

* *Ишмухаметов Шамиль Талгатович* — докт. физ.-мат. наук, проф. каф. САИТ, ИВМиИТ КФУ, e-mail: ishm2010@yandex.ru, ORCID: 0000-0003-2554-2351.

*Ishmukhametov Shamil Talgatovich* — professor, Kazan Federal University.

‡ *Курбангалеев Артур Аскарович* — канд. техн. наук, доцент каф. САИТ, ИВМиИТ КФУ, e-mail: arturkurbangaleev@rambler.ru, ORCID: 0000-0002-6881-1075.

*Kurbangaleev Artur Askarovich* — docent, Kazan Federal University.

§ *Мубараков Булат Газинурович* — канд. техн. наук, доцент каф. САИТ, ИВМиИТ КФУ, e-mail: mubbulat@mail.ru, ORCID: 0000-0002-7628-9870.

*Mubarakov Bulat Gazinurovich* — docent, Kazan Federal University.

¶ *Рубцова Рамиля Гакилевна* — ст.преподаватель каф. САИТ, ИВМиИТ КФУ, e-mail: dearr2003@mail.ru, ORCID: 0000-0002-3555-4834.

*Rubtsova Ramilya Gakilevna* — senior lecturer, Kazan Federal University.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

использовать его в тестах простоты. Малая теорема Ферма используется также для факторизации составных чисел. Известный $(p-1)$–метод Полларда работает следующим образом. Пусть $p > 2$ – простой делитель составного числа $n$. Возьмем произвольный элемент, например, число 2, и будем возводить его в большую степень $N(B)$, находя остаток по модулю $n$. Если выполнится соотношение $(p-1)|\ N(B)$ , тогда $2^{N(B)} \bmod\ p = 2^{(p-1)k} \bmod\ p = 1$, и $2^{N(B)} = 1 + kp$ для некоторого $k$, откуда $GCD(2^N(B) - 1, n) = p$.

Рассмотрим конечное поле $F_{p^2}$, построенное на неприводимом многочлене $f(x) = x^2 - ax - b$. Эндоморфизм Фробениуса, определенный на элементах этого поля, $\Phi(z) :\ z \to z^p$, оставляет простое подполе $F_p$ на месте. Также для корней $f(x)$ выполняется соотношение $\Phi(z) = a - z$ и $\Phi(a - z) = z$, то есть отображение Фробениуса переставляет элементы $z$ и $a - z$. Отсюда $z^{p+1} \equiv z(a - z) \equiv (a - z)^{p+1} (\mathrm{mod}\ p)$, откуда

$$z^{p+1} - (a - z)^{p+1} \equiv\ 0 (\mathrm{mod}\ p). \tag{2}$$

Формула (2) так же, как и малая теорема Ферма, может быть использована для построения тестов простоты и алгоритмов факторизации. Приведем пример теста простоты, использующего ряд Фибоначчи: $R_0 = 0,\ R_1 = 1,\ R_{n+2} = R_n + R_{n+1}$. Элементы ряда Фибоначчи можно представить в виде:

$$R_n \equiv \frac{x^n - (1 - x)^n}{2x - 1}\ (\mathrm{mod}\ f(x), p),$$

где $f(x) = x^2 - x - 1$ – характеристический многочлен последовательности Фибоначчи с дискриминантом $D = 5$. Рассмотрим кольцо $F$, состоящее из многочленов 1-й степени $ax + b$ по составному модулю $\{f(x), p\}$, где $p \neq 5$ – простое число. Если $p \bmod\ D$ является квадратичным вычетом в $F_5$, то $F$ изоморфно $Z_p \times Z_p$. Иначе, $F$ – квадратичное поле порядка $p^2$. Отсюда вытекает следующая теорема Люка, являющаяся в некотором смысле аналогом малой теоремы Ферма . Если простое $p \equiv \pm 1\ (\mathrm{mod}\ 5)$, то $R_{p-1} \equiv 0\ (\mathrm{mod}\ p)$, и если $p \equiv \pm 2\ (\mathrm{mod}\ 5)$, тогда $R_{p+1} \equiv 0\ (\mathrm{mod}\ p)$. Как и в теореме Ферма, составные числа достаточно редко проходят данный тест. Будем называть составные числа, проходящие тест Люка, L-псевдопростыми, а составные числа, проходящие тест Ферма по основанию 2, F2-псевдопростыми. Объединим эти два теста. Назовем составные числа, проходящие комбинированный тест, FL-псевдопростыми. С помощью компьютерных вычислений были найдены несколько FL-псевдопростых чисел $n \equiv \pm 1\ (\mathrm{mod}\ 5)$. Однако FL-псевдопростых чисел вида $n \equiv \pm 2\ (\mathrm{mod}\ 5)$ найдено не было. Это породило Baillie-PSW гипотезу, сформулированную еще в 1980 году: не существует FL-псевдопростых

чисел вида $n \equiv \pm 2 \pmod 5$ (в самой гипотезе использовался не тест Ферма, а один раунд теста Миллера-Рабина с основанием 2). На сегодняшний день так и не было найдено ни одного Fl2-псевдопростого числа вида $n \equiv \pm 2 \pmod 5$. Если эта гипотеза верна, то простоту чисел вида $n \equiv \pm 2 \pmod 5$ можно было бы проверять с помощью двух проверок теорем Ферма и Люка, что является самым быстрым на текущий момент тестом простоты в мире. Используя свойства FL-псевдопростых чисел $n \equiv \pm 2 \pmod 5$ [4] и мультипроцессорный сервер Казанского федерального университета, мы проверили отсутствие таких чисел до границы $10^{21}$. Наша программа работала примерно 9 месяцев, используя 24 процессора. Отметим, что данный тест проверяет только числа вида $n \equiv \pm 2 \pmod 5$, то есть примерно половину от всех нечетных чисел (числа, кратные 5, легко отсекаются). Для проверки других чисел используем поля, построенные на других характеристических полиномах вида $f(x) = x^2 - ax - b$. Необходимым условием возможности использования полинома является требование того, чтобы его дискриминант не был полным квадратом или являлся отрицательным числом. Последнее дает нам знакопеременные ряды, что уменьшает рост слагаемых по абсолютной величине. С помощью компьютерных вычислений нами было найдено 5 нетривиальных полиномов, которые охватывают в совокупности 31/32 всех целых чисел (исключая числа, кратные модулю соответствующего дискриминанта).

| $N$ | $a$ | $b$ | $D = a^2 + 4b$ |
|---|---|---|---|
| 1 | 1 | 1 | 5 |
| 2 | 4 | $-2$ | 8 |
| 3 | 1 | $-2$ | $-7$ |
| 4 | 1 | $-3$ | $-11$ |
| 5 | 2 | $-3$ | $-8$ |

Справедливость Baillie-PSW гипотезы для ряда Фибоначчи не влечет автоматически ее справедливости при замене его другим рядом из нашей таблицы, однако имеются серьезные основания считать, что это верно. В этом случае большинство натуральных чисел могло бы быть проверено на простоту с помощью этого комбинированного теста.

## Список литературы

[1] Ш.Т. Ишмухаметов, Р.Г.Рубцова, Р.Р.Хуснутдинов, “Об одном комбинированном тесте простоты”, *Известия вузов.Математика*, **2**, 2022, 83–89. DOI: https://doi.org/10.3103/S1066369X22020049.

[2] Ш.Т.Ишмухаметов, Н.А.Антонов, Б.Г.Мубараков, Р.Г.Рубцова., “Об одном тесте простоты натуральных чисел”, *Известия вузов.Математика*, **12**, 2022, 123–129. DOI: 10.26907/0021-3446-2022-12-123-129.

[3] S.Ishmukhametov, N.Antonov, B. Mubarakov, “On a Modification of The Lucas Primality Test”, *Lobachevskii J.Math*, **7**, 2023, 1–8. DOI: 10.1134/S1995080223070193.

[4] Ш.Т.Ишмухаметов, Б.Г.Мубараков, Р.Г.Рубцова, Р.Г. Олейникова, “О BAILLIE-PSW гипотезе”, *Известия вузов.Математика*, **4**, 2024, 80–88. DOI: 10.26907/0021-3446-2024-4-80-88 .

Статья поступила 5 октября 2026 г.

## The use of Fermat’s Little Theorem and its analogues in cryptography

S. T. Ishmukhametov, A. A. Kurbangaleev, B. G. Mubarakov, R. G. Rubtsova

In this article, we will examine an important cryptographic problem: constructing efficient primality tests used to generate large prime numbers. We improve upon existing methods by using analogues of Fermat’s little theorem.

**Keywords:** primality test, finite fields, factorization, cryptographic protocols, elliptic curves, Lucas method, Williams’ method.

# References

[1] Sh.T. Ishmukhametov, R.G. Rubtsova, R.R. Khusnutdinov, “On a Combined Primality Test”, *Russian Mathematics (Izvestiya VUZ. Matematika), 2022, Volume 66, Issue 12, Pages 112–117*, **12**, 2022, 112–117. DOI: 10.3103/S1066369X22120088.

[2] Sh.T. Ishmukhametov, N.A. Antonov, B.G. Mubarakov, R.G. Rubtsova, “A New Primality Test for Natural Integers”, *Russian Mathematics (Izvestiya VUZ. Matematika)*, **66 (2)**, 2022, 70–73. DOI: 10.3103/S1066369X22020049.

[3] S.Ishmukhametov, N.Antonov, B. Mubarakov, “On a Modification of The Lucas Primality Test”, *Lobachevskii J.Math*, **7**, 2023, 1–8. DOI: 10.1134/S1995080223070193.

[4] Sh.T. Ishmukhametov, B.G. Mubarakov, R.G. Rubtsova, R.G. Oleinikova, “On the Baillie PSW Conjecture”, *Russian Mathematics (Izvestiya VUZ. Matematika)*, **68 (4)**, 2024, 72–78. DOI: https://doi.org/10.3103/S1066369X24700294.

Received on October 5, 2026