Evaluation of the Effectiveness of the Frobenius Primality Test

Sergei Khashin
http://math.ivanovo.ac.ru/dalgebra/Khashin/index.html
Ivanovo State University, Russia
July 20, 2018

Contents

1 Notations and preliminary information
  1.1 Pseudoprimes .................................................. 2
  1.2 Jacobi symbol .................................................. 3
  1.3 Frobenius index .............................................. 3
  1.4 Quadratic field .............................................. 4

2 Frobenius primality test
  2.1 Definition .................................................... 4
  2.2 Main theorem ............................................... 5
  2.3 Multiple factors ........................................... 5
  2.4 $\Phi$-positive factor ....................................... 6
  2.5 Agreed prime factors ....................................... 7

3 Results of calculations
  3.1 Direct computation ........................................ 7
  3.2 Large Frobenius index ...................................... 7
  3.3 Multiple factors ........................................... 8
  3.4 All factors except one ...................................... 8
  3.5 $\Phi$-positive prime factors ............................... 8
  3.6 $\Phi$-negative factors of intermediate size .......... 8
  3.7 Exactly two factors ........................................ 9
  3.8 Two agreed prime factors ................................ 10
  3.9 Exactly three factors ..................................... 11
  3.10 Three agreed prime factors .............................. 11
  3.11 Main result ................................................ 12

4 Conclusions .................................................... 12
Abstract

Frobenius method of primality test based on the properties of the Frobenius automorphism of the quadratic extension of the residue field. We prove several properties of this method. Though the method is probabilistic, but based on proved properties is checked he’s not wrong on the numbers that are less than $2^{64}$. There is reason to believe that the method is never wrong. The method can be recommended for wide use.

Key words: Primality test, MillerRabin test, Frobenius test

Introduction

The most popular methods for primality testing today are based on small Fermat theorem: MillerRabin and SolovayStrassen primality tests. The reliability of these methods is not high enough. For example, in [13], 24- and 25-valued numbers are found that will pass 12 and 13 of Miller-Rabin tests, respectively. Therefore, even a few dozen individual tests can not guarantee the primality of the number. In the Java language for numbers longer than 100 bits, an additional method is used: the Lucas test, [1]. This radically improves reliability, but a mathematical study of the combined use of these tests difficult.

The Frobenius method, that is, the method based on the Frobenius automorphism of the field $GF(p^2)$ for prime $p$, has been known for a long time ([3, 4, 5, 8, 7] etc.). In ([4, 12]), even some amplifications of this test are suggested. But for today, no single composite number is known to pass even the simplest version of the test. Although the book ([3], p.146), states that the number $5777 = 53 * 109$ will be the Frobenius pseudo-prime for $c = 5$. It is easy to verify that this is not the case. Apparently, at this point in the book, the term "Frobenius pseudo prime" is used in a slightly different sense.

In addition, in [4, 5] an upper bound on the error probability of the method ($\approx 1/1300$) is proved. This is much less than the estimate for the Miller-Rabin (1/4) method, but still the error probability looks very significant.

All this led to the fact that the Frobenius method has been greatly underestimated. In fact, to date there is no counterexample to this method and there is reason to believe that they do not exist at all.

Frobenius test is just to check some equality in quadratic extension of the integers modulo prime $p$.

The equality of the norms of the corresponding elements is equivalent to the Fermat test, and the equality of the irrational parts is a Lukas test. That is, the Frobenius test is a natural union of these two tests.

The complexity of the Frobenius test twice the complexity of the methods Fermat or Miller-Rabin, that is equal to the complexity of two such tests.

The Miller-Rabin test for the number $n$ begins with the choice of the base $a$, which is relatively prime to $n$.

As the base, take either the first prime numbers (2, 3, 5, . . .), or make a pseudo-random choice of the number $a$ that is relatively prime to $n$.

In the usual definition of the Frobenius test (see, for example, [4, 5]), it is also suggested to make a pseudo-random choice of the "base" $z = a + b\sqrt{c}$.

In this paper, we propose to fix this choice in the form $2 + \sqrt{c}$ or $1 + \sqrt{c}$ depending on $c$ (for details see the definition (2.1)). This is much more convenient and, most importantly, quite enough. Nevertheless, most of the proofs is given for arbitrary $a, b$.

At the beginning of the paper (section 1) we give the necessary information and fix the notation. The 2 section defines the Frobenius method (Definition 2.1) and proves its properties.

In this paper, statements that require only mathematical reasoning are called ”Theorems” (2.7...2.20), and statements that require computer calculations are called ”Propositions” (3.1...3.13).

The main result of the paper is the Proposition 3.13, claiming that the Frobenius method does not err on the numbers less $2^{64}$.

1 Notations and preliminary information

1.1 Pseudoprimes

Definition 1.1. ([11, 3]) A composite number $n$ is named pseudoprime to a base $a$ when

$$a^{n-1} \equiv 1 \mod n.$$
Pseudoprime numbers quite a lot. Among the numbers less than $2^{32}$ there are 10,043 pseudoprime base 2, among the numbers less than $2^{64}$ exactly 118,968,378 \(\text{(see [9])}\).

Several checking reduces the number of errors, but not very much.

For example, among 10,043 base 2 pseudoprimes less than $2^{32}$ there is 2,318.

The transition from pseudoprimality to more complex methods (Miller-Rabin or Solovey-Strassen, [11]) does not significantly improve reliability. The number of errors is reduced to three or four times.

### 1.2 Jacobi symbol

Let’s write out the basic properties of the Jacobi symbol \(\text{[11 2]}\), which we denote \(J(a/n)\). We denote by gcd\((a, b)\) the greatest common divisor.

- \(J(a + n/n) = J(a/n)\).
- If \(p\) is prime and gcd\((a, p) = 1\), then \(J(a/p) = a^{(p-1)/2} \mod p\).
- \(J(ab/n) = J(a/n)J(b/n)\).
- Let \(n\) is odd and \(n = n_1n_2\). Then \(J(a/n) = J(a/n_1)J(a/n_2)\).
- Let \(p, q\) are odd. Then \(J(p/q) = (-1)^{\frac{p+1}{2} \frac{q+1}{2}} J(q/p)\).

We write out the values of the \(J(a/n)\) for some \(a\):

\[
\begin{align*}
J(-1/n) &= \begin{cases} 
1, & n \equiv 1 \mod 4 \\
-1, & n \equiv 3 \mod 4
\end{cases} \\
J(2/n) &= \begin{cases} 
1, & n \equiv \pm 1 \mod 8 \\
-1, & n \equiv \pm 3 \mod 8
\end{cases} \\
J(3/n) &= \begin{cases} 
1, & n \equiv \pm 1 \mod 12 \\
-1, & n \equiv \pm 5 \mod 12
\end{cases} \quad (\gcd(6, n) = 1) \\
J(5/n) = J(n/5) &= \begin{cases} 
1, & n \equiv \pm 1 \mod 5 \\
-1, & n \equiv \pm 2 \mod 5
\end{cases}
\end{align*}
\]

### 1.3 Frobenius index

In the number theory the concept of ”least quadratic non-residue mod \(p^2\)" is widely used, that is, for the natural number \(n\) find the smallest positive \(c\) such that \(J(c/n) = -1\). In our case, a similar but slightly different value is required.

**Definition 1.2.** Let \(n\) be an odd number and not a perfect square. Its Frobenius index \(\text{Ind}_F(n)\) is the smallest \(c\) among the numbers \([-1, 2, 3, 4, 5, 6, \ldots]\) such that the Jacobi symbol \(J(c/n) \neq 1\).

From the multiplicativity of the Jacobi symbol it follows that if a Frobenius index is positive, then it is prime.

It is not difficult to find out when the Frobenius index \(c = \text{ind}_F(n)\) takes small values:

- If \(n \equiv 3 \mod 4\), then \(c = -1\).
- If \(n \equiv 5 \mod 8\), then \(c = 2\).

Now we assume that \(n\) is not divisible by 3.

- If \(n \equiv 17 \mod 24\), then \(c = 3\).
- If \(n \equiv 1 \mod 24\), then \(c \geq 5\).

Now we assume that \(n\) is not divisible by 3 and 5.

- If \(n \equiv 73\) or \(97 \mod 120\), then \(c = 5\).
- If \(n \equiv 1\) or \(49 \mod 120\), then \(c \geq 7\).
1.4 Quadratic field

Let $c$ is a square-free integer and $z = a + b\sqrt{c} \in \mathbb{Z}[\sqrt{c}]$. The number $a$ is called a rational part of $z$, $a = \text{Rat}(z)$, and $b$ is irrational part, $b = \text{Irr}(z)$. The number $N(z) = a^2 - b^2c$ is called a norm of $z$, $\overline{z} = a - b\sqrt{c}$ is a conjugated number. So $N(z_1z_2) = N(z_1)N(z_2)$, $N(z) = z \cdot \overline{z}$.

If $p$ is prime and $J(c/p) = -1$, then the ring $\mathbb{Z}_p[\sqrt{c}]$ is isomorphic to the Galois field $GF(p^2)$. The map

$$z \rightarrow z^p \mod p,$$

is a Frobenius automorphism and $z^p \equiv \overline{z}$.

If $J(c/p) = +1$, then exist $d \in \mathbb{Z}_p : d^2 = c \mod p$. The ring $\mathbb{Z}_p[\sqrt{c}]$ is isomorphic to the $\mathbb{Z}_p \times \mathbb{Z}_p$ is given by formula:

$$a + b\sqrt{c} \rightarrow (a + bd, a - bd).$$

In this case $z^p \equiv z \mod p$.

2 Frobenius primality test

2.1 Definition

Definition 2.1. Let $n$ is an odd number, not perfect square and $c = \text{Ind}_F(c)$ is a Frobenius index. Let

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

We call $n$ a Frobenius prime if

$$z^n \equiv \overline{z} \mod n. \tag{2}$$

Remark 2.2. If $J(c/n) = 0$ then $n$ is divided by $c$. This is a trivial case. So we shall assume that $J(c/n) = -1$.

The equality (2) holds for any prime $n$ with $J(c/n) = -1$.

If composite number $n$ if a Frobenius prime, then we call it a Frobenius pseudoprime(FPP). More precisely, if $z = a + b\sqrt{c}$ and $z^n \equiv \overline{z} \mod n$, then the number $n$ will be called Frobenius pseudoprime with parameters $(a, b, c)$, or $\text{FPP}(a, b, c)$.

In other words, the FPP numbers are those on which the Frobenius method is wrong.

Example 2.3. Let $n = 19$, so $c = -1$, $z = 2 + i$,

$$z^n = -3565918 + 2521451i \equiv 2 - i \mod n.$$

Example 2.4. Let $n = 33$, so $c = -1$, $z = 2 + i$,

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

Example 2.5. Let $n = 17$, so $c = 3$, $z = 1 + \sqrt{3}$,

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

Note that if $n$ is $\text{FPP}(a, b, c)$, then $n$ is pseudoprime to a base $N(z) = a^2 - b^2c$, that is, the Frobenius test includes the Fermat test.

A comparison of the irrational components is actually a Lucas test. Thus, the Frobenius test is a combination of the Fermat and Lucas tests.

**Hypothesis.** Frobenius pseudoprime numbers do not exist!

In other words, the Frobenius test is never wrong.

Do not try to find a counterexample by a straightforward search. It is proved that it is not among the numbers less than $2^{94}$. More likely to find it in the form of the product is simple.

Remark 2.6. Choice with the base $z = 2 + \sqrt{5}$ or $z = 1 + \sqrt{3}$ is not random. For some $n$ may exist "bad" bases, or in the terminology of the works [4, 5] "liars". The smallest example is $n = 7 \cdot 19 \cdot 43 = 5719$. In this case the base $z = 4689 + \sqrt{-1}$ is "liar" that is

$$z^n = \overline{z} \mod n.$$
2.2 Main theorem

The following statement (in slightly different formulations) is proved in ([4][12][8]).

**Theorem 2.7.** Let \( n \) be an FPP(a,b,c), \( n = pq \) where \( p \) is prime. Then

a) if \( J(c/p) = -1 \), then \( z^q \equiv z \mod p \).
b) if \( J(c/p) = +1 \), then \( z^q \equiv \bar{z} \mod p \).

**Proof.** Let \( J(c/p) = -1 \), then \( z^p \equiv \bar{z} \mod p \). The number \( n \) is FPP, that is \( z^{pq} \equiv \bar{z} \mod pq \), so

\[
z^{pq} \equiv (z^p)^q \equiv \bar{z}^q \equiv \bar{z} \mod p,
\]

and

\[
z^q \equiv \bar{z} \mod p.
\]

Let \( J(c/p) = +1 \), then \( z^p \equiv z \mod p \). The number \( n \) is FPP, so \( z^{pq} \equiv \bar{z} \mod pq \) and

\[
z^{pq} \equiv (z^p)^q \equiv z^q \equiv \bar{z} \mod p.
\]

\[
\square
\]

**Corollary 2.8.** Let \( z = a + b\sqrt{c} \in \mathbb{Z} \) \( z^q = a_q + b_q\sqrt{c} \in \mathbb{Z} \) and \( n \) is a FPP(a,b,c), \( n = pq \), where \( p \) is prime. Then

a) if \( J(c/q) = +1 \), then \( p \) is a prime factor of \( \gcd(a_q - a, b_q - b) \).
b) if \( J(c/q) = -1 \), then \( p \) is a prime factor of \( \gcd(a_q - a, b_q + b) \).

**Example 2.9.** Let \( q = 31 \), \( c = 5 \). Then \( J(c/q) = +1 \) and

\[
(1 + \sqrt{c})^q = a_q + b_q\sqrt{c} = 3232337626136576 + 1445545331654656\sqrt{c}
\]

and \( \gcd(a_q - a, b_q - b) = 104005 \), so \( p \) is one of the prime factors of \( 104005: 5, 11, 31, 61 \).

**Example 2.10.** Let \( q = 37 \), \( c = 5 \). Then \( J(c/q) = -1 \) and

\[
(1 + \sqrt{c})^q = 3712124497172627456 + 1660112543324045312\sqrt{c}
\]

and \( \gcd(a_q - a, b_q + b) = 37 \), so \( p \) can be only 37.

**Remark 2.11.** Although the numbers \( a_q, b_q \) grow rather quickly, the corresponding common divisor are not too large and can be factorized up to \( q \) equal to many millions.

2.3 Multiple factors

**Theorem 2.12.** Let \( p \) be a prime, \( n = p^2q \) for some \( q \) (\( q \) can be a multiple of \( p \)) and \( n \) be a FPP(a,b,c). Then

\[
z^p \equiv \bar{z} \mod p^2.
\]

**Proof.**

In the ring \( \mathbb{Z}_{p^2}[\sqrt{c}] \):

\[
(a + pb)^p \equiv a^p \mod p^2.
\]

So:

\[
z^{p^2q} \equiv \bar{z} \mod p^2q,
\]

therefore

\[
z^{p^2q} \equiv \bar{z} \mod p^2.
\]

As \( z^{p^2} \equiv z \mod p \), so \( z^q \equiv z^p \equiv \bar{z} \mod p \) and

\[
z^p \equiv \bar{z} + pu \mod p^2,
\]

\[
z^q \equiv \bar{z} + pv \mod p^2
\]

for some \( u, v \in \mathbb{Z}_{p}[\sqrt{c}] \). Then

\[
z^{pq} \equiv (z^p)^q \equiv (\bar{z} + pu)^q \equiv \bar{z}^q \equiv z + pu \mod p^2,
\]

\[
z^{p^2q} \equiv (z^{pq})^p \equiv (z^q + pu)^p \equiv \bar{z} + pu \mod p^2.
\]

On the other hand \( z^n \equiv \bar{z} \mod p^2 \), that is \( u = 0 \) therefore \( z^p \equiv \bar{z} \mod p^2 \).

\[
\square
\]

**Corollary 2.13.** If \( n = p^2q \) is a FPP(a,b,c), then \( N(z)^{p^{-1}} \equiv 1 \mod p^2 \), where \( N(z) \) is a norm of \( z \).
2.4 \( \Phi \)-positive factor

**Definition 2.14.** Let \( n \) be a Frobenius pseudoprime with parameters \((a, b, c)\). The prime factor \( p \) of \( n \) we call \( \Phi \)-positive, if \( J(c/p) = +1 \) and \( \Phi \)-negative, if \( J(c/p) = -1 \).

**Theorem 2.15.** Let \( n \) be a Frobenius pseudoprime, \( z = a + b\sqrt{c} \) and \( p \) is a \( \Phi \)-positive prime factor of \( n \), \( n = p \cdot q \), \( c \equiv d^2 \mod p \). We introduce the notation:

\[ z_1 = (a + b \cdot d) \mod p, \]
\[ z_2 = a - b \cdot d \mod p, \]
\[ z_1, z_2 \in \mathbb{Z}_p. \]

Then

\[ z_1^q \equiv z_2 \mod p, \]
\[ z_2^q \equiv z_1 \mod p, \]

**(3)** \( (4)\)

**Proof.** By definition:

\[ (a + b\sqrt{c})^p = a - b\sqrt{c} \mod p. \]

If \( J(c/p) = +1 \) then \( z^p = z \), so

\[ (a + b\sqrt{c})^q = a - b\sqrt{c} \mod p \]

Using isomorphism \( \mathbb{Z}_p[\sqrt{c}] \to \mathbb{Z}_p \times \mathbb{Z}_p \), we obtain the required.

**Corollary 2.16.** Let

\[ N = z_1 z_2 = a^2 - b^2 \cdot c \]

and

\[ w = z_1 / z_2 = \frac{(a + bd)^2}{N} \mod p. \]

Then

\[ N^{q-1} = 1, \]
\[ w^{q+1} = 1, \]

**Proof.** Multiplying equalities (3) and (4), we obtain

\[ (z_1 z_2)^q = z_1 z_2, \]

or \( N^{q-1} = 1 \), and dividing them into each other

\[ (z_1 / z_2)^q = z_2 / z_1. \]

or \( w^{q+1} = 1 \).

**Corollary 2.17.** Let \( \alpha = ord(N \mod p) \) and \( \beta = ord(w \mod p) \). Then

\[ gcd(\alpha, \beta) \leq 2. \]

**Proof.** We have:

\[ q - 1 = 0 \mod \alpha, \]
\[ q + 1 = 0 \mod \beta. \]

These two conditions can not be fulfilled simultaneously if \( \alpha \) and \( \beta \) have a common factor \( > 2 \).

**Corollary 2.18.** Let \( n \) be a Frobenius pseudoprime, \( z = a + b\sqrt{c} \), \( p \) is a \( \Phi \)-positive prime factor of \( n \) and \( q = n/p \). Then

\[ q \equiv A_p \mod M_p, \]

where

\[ M_p = \text{lcm}(ord(z_1 \mod p), ord(z_2 \mod p)). \]

**Proof.**

If \( q \) is increased by a multiple of \( ord(z_1 \mod p) \) and \( ord(z_2 \mod p) \), then both sides of the equalities (3) and (4) do not change.

Note that both \( ord(z_1 \mod p) \) and \( ord(z_2 \mod p) \) are divisors of \( p - 1 \), so their least common multiple is also a divisor of \( p - 1 \).
2.5 Agreed prime factors

Let \( n \) be FPP and \( p \) its \( \Phi \)-positive prime factors. Corollary (2.18) can be written in the form

\[
n \equiv D_p \mod M_p,
\]

for some \( D_p, M_p \).

If \( p \) is a \( \Phi \)-negative prime factor \( n \), according to the main theorem (2.7)

\[
q \equiv 1 \mod \ord(z \mod p)
\]
or

\[
n \equiv D_p \mod M_p,
\]

where \( D_p = p, M_p = \ord(z \mod p) \).

Let \( p_1, p_2 \) are two different prime factors of FPP \( n \), \( \Phi \)-positive of negative and \( n = p_1 p_2 q \). So:

\[
n \equiv D_{p_1} \mod M_{p_1},
\]

\[
n \equiv D_{p_2} \mod M_{p_2}.
\]

From this it follows that in this case it must be fulfilled

\[
D_{p_1} \equiv D_{p_2} \mod \gcd(M_{p_1}, M_{p_2}).
\] (5)

This relation does not depend on \( q \), only on \( p_1 \) and \( p_2 \).

**Definition 2.19.** Given \( z \in \mathbb{Z} \backslash \sqrt{c} \). Two primes will call \( z \)-consistent, or simply consistent, if the relation (5) holds for them.

**Theorem 2.20.** Let \( n \) be a Frobenius pseudoprime. Then all its prime factors are pairwise consistent.

3 Results of calculations

A hypothesis asserting that there are no Frobenius pseudoprime (FPP) can not yet be proved. Consider what we managed do in this direction.

3.1 Direct computation

We check all composite odd numbers that are not complete squares on FPP. On a usual computer (Intel(R) Pentium(R) CPU G4500 @3.50GHz) for a few days were all numbers checked up to \( 30 \cdot 10^9 \).

Check all composite odd numbers that are not complete squares on the FPP. On usual computer (Intel(R) Pentium(R) CPU G4500 @3.50GHz) in a few days was checked all numbers up to \( 30 \cdot 10^9 \).

So:

**Proposition 3.1.** There is no FPP less than \( 30 \) billions.

3.2 Large Frobenius index

It has already been said above that if \( n \equiv 1 \mod 24 \), then \( \ind_F(n) \geq 5 \). The Frobenius index can be arbitrarily large. Among the numbers \( < 2^{42} \), the largest value of the index (101) has the number 280544681.

In the paper [10] a complete list of 458069912 numbers less than \( 2^{64} \), whose index of Frobenius > 128 is constructed.

All these numbers are not FPP. In this way:

**Proposition 3.2.** There is no FPP less than \( 2^{64} \) with the Frobenius index > 128.
3.3 Multiple factors

The section (2.3) proves the properties that should satisfy multiple prime factors of FPP. A direct calculation of these properties showed that FPP does not have multiple factors less than $2^{32}$ with the Frobenius index $c < 128$ (without restriction on the value of FPP).

The total calculation time (3.50GHz) is about two days.

So:

**Proposition 3.3.** There are no FPPs smaller than $2^{64}$ having multiple prime factors.

3.4 All factors except one

Let $n$ be $FPP(a, b, c)$ and $p$ the prime factor of $n$, $q = n/p$. In this case $z = a + b\sqrt{c} \in \mathbb{Z}$ and $z^q = a_q + b_q\sqrt{c}$.

According to the Corollary (2.8) of the main theorem the number $p$ is a divisor of $D = \gcd(a_q - a, b_q \pm b)$, where the sign “+” or “−” is taken depending on the sign $a J(c/q)$.

Thus, for a fixed $z = a + b\sqrt{c}$, for each positive $q$ we perform the following steps:

1. calculate $z^q = a_q + b_q\sqrt{c}$,
2. calculate $D = \gcd(a_q - a, b_q \pm b)$,
3. prime factorization of $D$: $D = p_1 \cdots p_s$,
4. for each $p_i$ check whether the number of $n_i = q \cdot p_i$ FPP.

If $q$ is of the order of several million, then $a_q, b_q$ will have a length of up to tens of millions of bits. However, the number $D$ in all cases will not be so large and, most importantly, is decomposed into small prime factors.

Within a reasonable time (hours) the result is as follows:

**Proposition 3.4.** Let $n$ be an FPP (any size, not necessarily $< 2^{64}$) with an Frobenius index $c = \text{ind}_F(n) < 128$. Then $n$ has no prime factors $p$ such that $n/p < 2^{19}$.

3.5 Φ-positive prime factors

In the section (2.4) properties of the Φ-positive factors $p$ of FPP $n = pq$ are proved and an algorithm for finding numbers possessing these properties is proposed.

This algorithm gives us the possible Φ-positive prime factors $p$ and some comparison for $q$:

$$q \equiv q_p \mod A_p$$

for given $p$. An additional constraint will be of the comparison imposed by the Frobenius index:

$$
\begin{align*}
n &\equiv 3 \mod 4, \quad \text{if } \text{ind}_F(n) = -1, \\
&\equiv 5 \mod 8, \quad \text{if } \text{ind}_F(n) = 2, \\
&\equiv 17 \mod 24, \quad \text{if } \text{ind}_F(n) = 3, \\
&\equiv 1 \mod 24, \quad \text{if } \text{ind}_F(n) \geq 5,
\end{align*}
$$

and if $\text{ind}_F(n) \geq 5$ then $J(c/n) = +1$ for all $c < \text{ind}_F(n)$.

There are few such numbers $p$. For $c = \text{ind}_F(n) < 128$ and $p < 2^{32}$ we have only 26 numbers:
If we assume that \( n = pq < 2^{64} \), then most of these \( n \), can be directly check on FPP. After this, only following 8 numbers remain, for which a direct verification is too time-consuming:

| c  | p  | c  | p  | c  | p  | c  | p  |
|----|----|----|----|----|----|----|----|
| 2  | 8191 | 7  | 3923 | 29 | 12637 | 83 | 3278741 |
| 7  | 31  | 11 | 98641 | 61 | 271  | 101| 137   |

We see for FPP \( n < 2^{64} \) two \( \Phi \)-positive factors less than \( 2^{32} \) can be only for \( z = 1 + \sqrt{7} \), and this factors are 31 and 3923. By direct verification within a reasonable time (several hours), you can make sure that both factors can’t occur simultaneously. So:

**Proposition 3.5.** \( \Phi \)-positive prime factors less than \( 2^{32} \) for FPPs smaller than \( 2^{64} \) can be only 8 numbers mentioned above, and two such factors can not meet simultaneously.

### 3.6 \( \Phi \)-negative factors of intermediate size

In the previous subsection it was shown that the potential \( \Phi \)-positive prime factors occur very rarely. For \( \Phi \)-negative factors no such properties can be detected, that is, any prime number for which \( J(c/p) = -1 \) could, in principle, be a factor of the FPP. However, if we limit ourselves to only FPP less \( 2^{64} \), then we can impose some restrictions on such divisors.

**Proposition 3.6.** Let \( n < 2^{64} \) be an FPP with the Frobenius index \( c = \text{ind}_F(n) < 128 \). Then \( n \) does not have prime factors from the interval \( 2^{17} \ldots 2^{32} \).

**Proof.**

The absence of \( \Phi \)-positive factors of this size proved earlier. Therefore, we consider only \( \Phi \)-negative factors.

Let \( n < 2^{64} \) be a FPP with \( z = a + b\sqrt{c} \), \( c < 128 \) and \( p \) be a prime factor of \( n \), \( J(c/p) = -1 \). We denote \( n/p \) by \( q \). According to the main theorem (2.7):

\[ z^{q-1} \equiv 1 \mod p, \]

that is

\[ q \equiv 1 \mod \text{ord}(z \mod p). \]

or

\[ q = 1 + kQ_p \]

for some \( k \geq 1 \), where \( Q_p = \text{ord}(z \mod p) \). As \( n = pq < 2^{64} \), then \( q < 2^{64}/p \). Hence, we find the restriction on \( k \): \( k \leq k_{\text{max}} \). This means that the only valid candidates for the FPP will be in the numbers

\[ p(1 + Q_p), p(1 + 2Q_p), \ldots, p(1 + k_{\text{max}}Q_p). \]

As a result, in a reasonable time (a few hours for a fixed Frobenius index) you can check all \( \Phi \)-negative number in the interval \( 2^{17} \ldots 2^{32} \).  

**Example 3.7.** Let \( z = 2 + i, p = 10000019 \). Then \( Q_p = 1666730000060 = (p^2 - 1)/6 \) and for any \( k \geq 1 \): \( n = pq > 2^{64} \). That is, for this \( p \) there’s no acceptable \( q \).

Let \( p = 1000003 \). Then \( Q_p = 1000006000008 = p^2 - 1 \) and inequality \( n = pq < 2^{64} \) holds for \( k \leq 18 \). That is acceptable \( q \) is:

\[ 1 + Q_p, 1 + 2Q_p, \ldots, 1 + 18Q_p. \]

It is easy to check that for all this \( q \) the number \( n = pq \) is not FPP, i.e. that \( p \) cannot be a divisor FPP < \( 2^{64} \).

Let \( p = 1000003 \). Then \( Q_p = 434808696 = (p^2 - 1)/23 \) and inequality \( n = pq < 2^{64} \) holds for \( k \leq 424236 \). Verification of all such \( q \) will already take quite some time (several minutes), but still can be performed.

By a somewhat larger search, it is possible to construct for each index \( c < 128 \) a complete list of admissible simple \( \Phi \)-negative prime factors of FPP. For example, for \( c = -1 \) (\( z = 2 + i \)) the list will consist of 2424 prime numbers:

\[ 3, 7, 11, 19, 23, 31, 43, 47, \ldots, 108971, 109279, 110023. \]
| \(\text{ind}_F\) | The number of primes \(\max(p_i)\) | \(\text{ind}_F\) | The number of primes \(\max(p_i)\) |
|---|---|---|---|
| −1 | 2424 110023 | 53 | 427 7079 |
| 2 | 1026 49477 | 59 | 564 15271 |
| 3 | 2040 46817 | 61 | 593 17749 |
| 5 | 2031 65537 | 67 | 480 8821 |
| 7 | 1021 47791 | 71 | 520 10529 |
| 11 | 775 40237 | 73 | 577 14731 |
| 13 | 668 19141 | 79 | 596 21011 |
| 17 | 675 26321 | 83 | 288 10529 |
| 19 | 634 26713 | 89 | 321 15137 |
| 23 | 605 19801 | 97 | 318 17401 |
| 29 | 433 7039 | 101 | 316 21401 |
| 31 | 465 8009 | 103 | 301 8009 |
| 37 | 529 10429 | 107 | 298 11131 |
| 41 | 559 12517 | 109 | 312 15643 |
| 43 | 501 9203 | 113 | 330 15331 |
| 47 | 526 10093 | 127 | 312 20479 |

3.7 Exactly two factors

**Proposition 3.8.** Let \(n < 2^{64}\) is an FPP. Then \(n\) has more than two prime factors.

**Proof.** Let \(c = \text{ind}_F(n)\) be a Frobenius index of \(n\). Suppose that \(n = p_1p_2\). As \(J(c/n) = -1\), at one Jacobi symbol \(J(c/p_i)\) equals to \(-1\), another to \(+1\). We assume, for definiteness, that \(J(c/p_1) = -1, J(c/p_2) = +1\).

Suppose, that \(p_2 < 2^{32}\). Then, by Proposition 3.5, the number \(p_2\) must be one of 8 specified in this proposal. The largest of these numbers is 98,641. But according to the Proposition 3.4, \(p_2\) must be greater than \(2^{19}\).

The case \(p_2 > 2^{32}\) remains. This means that \(p_1 < 2^{32}\) and, by Proposition 3.5, it does not exceed \(2^{17}\). But then according to the Proposition 3.4, \(p_1\) should be greater than \(2^{19}\). Contradiction. \(\square\)

3.8 Two agreed prime factors

Suppose that FPP \(n\) has two factors of \(p_1\) and \(p_2\) smaller than \(2^{32}\). Then, firstly, both \(p_1\) and \(p_2\) should be contained in a relatively small list built in the previous paragraph.

Secondly, the factors need to be agreed and for \(q = n/(p_1p_2)\) the following relations must be fulfilled:

\[
q \equiv D_{p_12} \mod \gcd(M_{p_1}, M_{p_2}).
\]

for some \(D_{p_12}\).

Taking into account that \(n = p_1p_2q < 2^{64}\), it often turns out that for a given pair \((p_1, p_2)\) admissible \(q\) is a little and all of the corresponding \(n\) can be verified on the FPP. However, if \((p_1, p_2)\) are small, it is valid \(q\) is too much for direct examination.

**Proposition 3.9.** Let \(n < 2^{64}\) be an FPP with Frobenius index \(c = \text{ind}_F(n) < 128\) and \(p_1, p_2\) are its \(\Phi\)-negative factors, both less \(2^{32}\). Then \(p_1p_2 < 2^{18}\). Moreover, for each such \(c\), we get a complete list of valid pairs \((p_1, p_2)\):
\begin{tabular}{|c|c|c|c|c|c|}
\hline
$ind_F$ & The number of pairs & $max(p_i)$ & $ind_F$ & The number of pairs & $max(p_i)$ \\
\hline
$-1$ & 2438 & 108971 & 53 & 48 & 919 \\
2 & 230 & 10853 & 59 & 34 & 743 \\
3 & 150 & 46817 & 61 & 10 & 599 \\
5 & 187 & 28657 & 67 & 27 & 1871 \\
7 & 562 & 13451 & 71 & 32 & 4831 \\
11 & 456 & 9439 & 73 & 21 & 647 \\
13 & 128 & 16339 & 79 & 11 & 751 \\
17 & 74 & 2689 & 83 & 14 & 991 \\
19 & 88 & 1889 & 89 & 5 & 577 \\
23 & 73 & 881 & 97 & 13 & 433 \\
29 & 70 & 1429 & 101 & 4 & 349 \\
31 & 68 & 2089 & 103 & 4 & 181 \\
37 & 89 & 1297 & 107 & 8 & 439 \\
41 & 31 & 1223 & 109 & 12 & 379 \\
43 & 48 & 1291 & 113 & 3 & 683 \\
47 & 58 & 2771 & 127 & 5 & 463 \\
\hline
\end{tabular}

The numbers given in the table depend on the amount of time spent on computation and, if necessary, can be significantly reduced. But for our further goals this is enough.

In the Proposition (3.3) lists $\Phi$-positive integers that can be prime factors of FPP in this case. Checking them paired with the available list of valid $\Phi$-negative divisors, we get the following proposition.

**Proposition 3.10.** Let $n < 2^{64}$ be an FPP with Frobenius index $c = ind_F(n) < 128$. Then $n$ has no $\Phi$-positive factors, less then $2^{32}$.

### 3.9 Exactly three factors

**Proposition 3.11.** Let $n < 2^{64}$ is FPP. Then $n$ has more than three Prime factors

**Proof.** Let $c = ind_F(n)$ be the Frobenius index for $n$. Suppose that $n$ is decomposed into three prime factors: $n = p_1p_2p_3$. At least two of them must be less than $2^{32}$. According to the Proposition (3.9), $p_1p_2 < 2^{18}$. But according to the Proposition (3.3), $n/p_3$ must be greater than $2^{18}$. \qed

### 3.10 Three agreed prime factors

According to the Proposition (3.11) FPP $n$ must have at least four factors. At least three of them $p_1$, $p_2$ and $p_3$ should be less than $2^{32}$. Then the pair $(p_1, p_2)$, $(p_1, p_3)$ and $(p_2, p_3)$ must be contained in the list of Proposition (3.9). If $n = p_1p_2p_3q$ for some $q$, then

$$q \equiv D \mod gcd(M_{p_1}, M_{p_2}, M_{p_3}).$$

for some $D$. Taking into account that $n = p_1p_2p_3q < 2^{64}$, it often turns out that the triples $(p_1, p_2, p_3)$ of admissible $q$ is a little and all of the relevant $n$ can be verified on the FPP. However, if $(p_1, p_2, p_3)$ are small, then the admissible $q$ is too much for direct verification.

**Proposition 3.12.** a) There are no admissible triples $(p_1, p_2, p_3)$ with the Frobenius index $7 \leq c \leq 128$ and also with $c = 3$. In other words, possible value of the of the Frobenius index only $(-1, 2, 5)$.

b) For $c = 5$ admissible only triples $(13, 37, 433)$ and $(13, 37, 97)$.

c) For $c = 2$ there are 52 admissible triples:

$$(5, 53, 1613), (13, 109, 1549), (29, 37, 1549), (13, 37, 1549), (29, 109, 1429), (13, 37, 853), (5, 53, 677),$$

$$(13, 37, 613), (13, 37, 541), (13, 61, 397), (5, 53, 397), (13, 37, 397), (5, 197, 389), (29, 109, 373),$$

$$(13, 109, 373), (13, 37, 373), (13, 109, 349), (13, 37, 349), (13, 61, 293), (5, 53, 293), (13, 37, 293),$$

$$(11, 73, 1397), (11, 137, 1397), (11, 139, 1397), (11, 197, 1397), (11, 383, 1397), (11, 97, 1397).$$
(13, 61, 277), (5, 53, 277), (13, 37, 277), (29, 197, 269), (29, 149, 269), (29, 53, 269), (29, 197, 229), (5, 197, 229), (5, 157, 229), (29, 109, 229), (13, 109, 229), (13, 61, 229), (29, 53, 229), (5, 53, 229), (5, 173, 197), (53, 157, 197), (5, 157, 197), (29, 149, 197), (29, 53, 197), (5, 53, 197), (37, 61, 181), (5, 53, 173), (29, 109, 157), (29, 53, 157), (5, 53, 157), (29, 37, 157), (29, 53, 149), (29, 37, 109), (13, 37, 109), (13, 37, 61).

\[ d) \text{ For } c = -1 \text{ there are 323 admissible triples:} \]
\[ (19, 31, 12799), (7, 19, 8839), \ldots, (11, 47, 71). \]

### 3.11 Main result

**Proposition 3.13.** There are no Frobenius pseudoprime (FPP), smaller \( 2^{64} \).

**Proof.** Let the composite odd positive number \( n < 2^{64} \) not divisible by \( 3 \) pass the Frobenius test, that is, FPP. According to the Proposition 3.12 the Frobenius index \( c = \text{ind}_F(n) \) does not exceed 128. According to the Proposition 3.11 the number \( n \) has no multiple factors. According to the Proposition 3.10 the number \( n \) has no Φ-positive factors, less \( 2^{32} \). According to the Proposition 3.11 the number \( n \) has at least four prime factors. The Proposition 3.12 limits the possible values of the Frobenius index \( c \) by the \{−1, 2, 5\} and in each case there is a fixed list of valid factor triples \((p_1, p_2, p_3)\).

Let us consider the case \( c = 5 \), \( n = p_1p_2p_3q \). According to the Proposition 3.11 if \( q \) is prime then \( p_1p_2p_3 \) must be less than \( 2^{18} \), so \( q \) must be composite, hence \( n \) must have at least four factors smaller \( 2^{32} \), and these factors should be \( 13 \cdot 37 \cdot 97 \cdot 433 \). But all multiples of that number you can verify that they are not FPP.

Let us consider the case \( c = 2 \). Again, an FPP \( n \) must have at least four factors \( p_1p_2p_3p_4 \) smaller than \( 2^{32} \), and each of the triples
\[ p_1p_2p_3, \ p_1p_2p_4, \ p_1p_3p_4, \ p_2p_3p_4 \]
must be present in the above list. Such quadruples is two:
\[ (29 \cdot 53 \cdot 157 \cdot 197), \ (5 \cdot 53 \cdot 157 \cdot 197) \]
All multiples of this number are not FPP.

Now let \( c = -1 \). FPP \( n \) must have at least four factors \( p_1p_2p_3p_4 \), smaller than \( 2^{32} \), and each of the triples
\[ p_1p_2p_3, \ p_1p_2p_4, \ p_1p_3p_4, \ p_2p_3p_4 \]
must be present in the list (d) of Proposition 3.12. Such quadruples is 21:
\[ (7 \cdot 19 \cdot 79 \cdot 499), \ (7 \cdot 19 \cdot 79 \cdot 919), \ (7 \cdot 19 \cdot 79 \cdot 859), \ (7 \cdot 19 \cdot 79 \cdot 739), \ (7 \cdot 19 \cdot 79 \cdot 619), \ (7 \cdot 19 \cdot 79 \cdot 599), \ (7 \cdot 19 \cdot 79 \cdot 499), \ (7 \cdot 19 \cdot 79 \cdot 487), \ (7 \cdot 19 \cdot 79 \cdot 439), \ (7 \cdot 19 \cdot 79 \cdot 199), \ (7 \cdot 19 \cdot 199 \cdot 1999), \ (7 \cdot 19 \cdot 199 \cdot 859), \ (7 \cdot 19 \cdot 199 \cdot 599), \ (7 \cdot 19 \cdot 199 \cdot 499), \ (7 \cdot 19 \cdot 199 \cdot 487), \ (11 \cdot 47 \cdot 71 \cdot 691), \ (11 \cdot 47 \cdot 71 \cdot 431), \ (19 \cdot 31 \cdot 79 \cdot 1279), \ (31 \cdot 79 \cdot 139 \cdot 599). \]
All multiples of this number are not FPP.

\[ \square \]

### 4 Conclusions

- Frobenius test is one of the most efficient primality test.
- Its complexity is twice higher than that of methods based on Fermat’s theorem.
- How many times does reliability increase can not be estimated, because there is no example when the method is wrong.
- The development of the methods described in this paper may allow raising a “safe” border, for example, up to \( 2^{80} \).
- Another type of computational experiments could allow to prove statements like ”does not exist FPP, representable as a product of any number of primes less than \( N_0 \”).
References

[1] Robert Baillie; Samuel S. Wagstaff, Jr. *Lucas Pseudoprimes*. Mathematics of Computation. 35 (152): 1391-1417. doi:10.1090/S0025-5718-1980-0583518-6.

[2] Borevich, A. I.; Shafarevich, Igor R. *Number theory. Pure and Applied Mathematics..* 1966. 20. Boston, MA: Academic Press. ISBN 978-0-12-117850-5. MR 0195803.

[3] R.E. Crandall, C.Pomerance: *Prime Numbers: A Computational Perspective* (Second Edition), Springer-Verlag, 2005. - 597 Pages.

[4] I.B. Damgård and G.S.Frandsen, *An Extended Quadratic Frobenius Primality Test with Average Case Error Estimates*. Basic Research in Computer Science (BRICS), November 2001.

[5] I.B. Damgård and G.S.Frandsen, *An Extended Quadratic Frobenius Primality Test with Average- and Worst-Case Error Estimate*. Journal of Cryptology, Volume 19, Number 4 (2006), 489-520, DOI: 10.1007/s00145-006-0332-x

[6] Jan Feitsma *Tables of pseudoprimes and related data*. http://www.cecm.sfu.ca/Pseudoprimes/index-2-to-64.html Date: 2016-10-01.

[7] J. Grantham, Frobenius pseudoprimes *Math.of computation* Volume 70, Number 234, p.873-891 S 0025-5718(00)01197-2

[8] Khashin S.I., *Couterexamples for Frobenius primality test*. 2013. arxiv.org/abs/1307.7920.

[9] Khasin S.I., Khashina J.A., *Properties of Frobenius pseudoprime*. Vest.IvGU. 2014. V.2. p. 104-108.

[10] Khashin S.I., *Natural numbers with large Frobenius index*. Vest.IvGU. 2015. V.2. p. 75-78.

[11] Pomerance, C.; Rassias, M. Th. *Analytic Number Theory..*. 2015. Springer, New York. ISBN 978-3-319-22239-4. doi:10.1007/978-3-319-22240-0

[12] M. Seysen, *A Simplified Quadratic Frobenius Primality Test*. Cryptology ePrint Archive, 2005/462, http://eprint.iacr.org/2005/462.pdf

[13] Sorenson, Jonathan; Webster, Jonathan *Strong Pseudoprimes to Twelve Prime Bases*. 2015. arXiv.org:1509.00864 [math.NT].