

# Evaluation of the Effectiveness of the Frobenius Primality Test

Sergei Khashin

## Abstract

The Frobenius primality test is based on the properties of the Frobenius automorphism of the quadratic extension of the residue field. Although it is probabilistic, we show that is “very rarely wrong”. To date there are no counterexamples to this method and there are reasons to believe that they do not exist at all. In this paper, we suggest a version of the Frobenius test and prove that it does not fail for numbers less than  $2^{64}$ . We also show that a “Frobenius pseudoprime” will necessarily have a prime divisor greater than 3000.

Key words: Primality test, Miller-Rabin test, Frobenius test.

## Introduction

The most of popular nowadays methods for primality testing are based on small Fermat theorem: Miller-Rabin and Solovay-Strassen primality tests. However reliability of such methods is not high: for example in [10], 24- and 25-digit numbers are found that pass twelve and thirteen Miller-Rabin tests, respectively. Therefore, even a few dozen of positive tests applied to some particular number does not guarantee the primality of that number. This is important for applications and, for example, in the Java language another test for numbers longer than 100 bits is also used, the Lucas test, see [1]. That test has a significantly higher reliability, but a mathematical study of the combined use of these tests is difficult.

The Frobenius primality test method is based on the Frobenius automorphism of the finite field of order  $p^2$ ,  $GF(p^2)$  for some prime  $p$ . It has been known for a long time, see for example, [3, 4, 6]. In [4, 9], even stronger versions of this test were suggested. However over the years the Frobenius method was greatly underestimated.

The reason for this is twofold. First of all, it is a common belief that there are some small pseudo-primes for this test. For example, in the book [3, p.146] it is stated that the number  $5777 = 53 \cdot 109$  is a Frobenius pseudo-prime (FPP) for  $c = 5$ . However, it is easy to verify that this is not the case. Apparently, at this point in the book, the term “FPP” is used in a slightly different sense. Secondly, as it was established in [4], an upper bound on the error probability of the Frobenius method is  $\approx 1/1300$ . Although this is much less than the estimate for the Miller-Rabin (1/4) method, still the probability error looks very significant.

In the present paper, beside other results, we show that Frobenius method does not fail on numbers less  $2^{64}$ . In fact, to date no single composite number is known to pass even the simplest version of the test, and it is our hypothesis that FPP do not exist at all.

Frobenius test consists in checking 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 the Lukas test. That is, the Frobenius test is a natural union of these two tests.

The complexity of the Frobenius test is 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 a choice of the base  $a$ , which is relatively prime to  $n$ . As the base, one either takes the first prime numbers,  $2, 3, 5, \dots$ , or makes 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]), it is also suggested to make a pseudo-random choice of the “base”  $z = a + b\sqrt{c}$ .

In our approach, we propose to restrict this choice to the forms  $2 + \sqrt{c}$  or  $1 + \sqrt{c}$  depending on  $c$  (for details see Definition 2.1). This is much more convenient and, most importantly, sufficient. Nevertheless, most of the theorems is given for arbitrary  $a$  and  $b$ .

The paper is organized as follows. In Sec. 1 we give the necessary information and fix the notation. In Sec. 2 we introduce Frobenius method (Definition 2.1) and discover its properties. In Sec 3 we describe the non-trivial approach that lead to an algorithm that will allow to show that the Frobenius method does not fail on the numbers less  $2^{64}$ . In Sec. 4 we show that an FPP necessarily has a prime divisor  $> 3000$ .

The computational results of the paper were only possible due to our theoretical results on properties of FPPs. This significantly simplified the number of cases to consider and thus allowed to run the computations in some acceptable time. Statements that require only mathematical reasoning are called “Theorems”, and statements that in part require some computer calculations are called “Propositions”. The main results of the paper are Theorem 2.14, Theorem 2.17, Theorem 2.22, and Theorem 2.23, and also Proposition 3.14 and Proposition 4.1.

## 1 Notations and preliminary information

### 1.1 Jacobi symbol

We refer the reader to [2] or [8] for the definition and main properties of the Jacobi symbol, which we denote by  $J(a/n)$ . Here is a list of the properties that we shall use. (By  $\gcd(a, b)$  we denote the greatest common divisor.)

- $J(a + n/n) = J(a/n)$ .
- If  $p$  is prime and  $\gcd(a, p) = 1$ , then  $J(a/p) = a^{(p-1)/2} \pmod p$ .
- $J(ab/n) = J(a/n)J(b/n)$ .
- 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  $J(p/q) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} J(q/p)$ .

Below we give the values of the  $J(a/n)$  for some  $a$  that we shall need in what follows.

$$\begin{aligned}
 J(-1/n) &= \begin{cases} 1, & n \equiv 1 \pmod 4 \\ -1, & n \equiv 3 \pmod 4 \end{cases} \\
 J(2/n) &= \begin{cases} 1, & n \equiv \pm 1 \pmod 8 \\ -1, & n \equiv \pm 3 \pmod 8 \end{cases} \\
 J(3/n) &= \begin{cases} 1, & n \equiv \pm 1 \pmod{12} \\ -1, & n \equiv \pm 5 \pmod{12} \end{cases} \quad (\gcd(6, n) = 1) \\
 J(5/n) = J(n/5) &= \begin{cases} 1, & n \equiv \pm 1 \pmod 5 \\ -1, & n \equiv \pm 2 \pmod 5 \end{cases}
 \end{aligned}$$

### 1.2 Frobenius index

In number theory, the concept of the “least quadratic non-residue mod  $p$ ” 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 1.1.** 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  $[-1, 2, 3, 4, 5, 6, \dots]$  such that the Jacobi symbol  $J(c/n) \neq 1$ .

It follows from the multiplicativity of the Jacobi symbol 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  $n \equiv 3 \pmod 4$  then  $c = -1$ .

If  $n \equiv 5 \pmod 8$  then  $c = 2$ .

Now we assume that  $n$  is not divisible by 3.

If  $n \equiv 17 \pmod{24}$  then  $c = 3$ . If  $n \equiv 1 \pmod{24}$  then  $c \geq 5$ .

Now we assume that  $n$  is not divisible by 3 and 5.

If  $n \equiv 73$  or  $97 \pmod{120}$  then  $c = 5$ . If  $n \equiv 1$  or  $49 \pmod{120}$  then  $c \geq 7$ .

### 1.3 Quadratic field

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

If  $p$  is a 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

$$z \rightarrow z^p \pmod{p}$$

is the Frobenius automorphism and  $z^p \equiv \bar{z}$ .

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

$$a + b\sqrt{c} \rightarrow (a + bd, a - bd). \quad (1)$$

In this case  $z^p \equiv z \pmod{p}$ .

## 2 Frobenius primality test

### 2.1 Definition

**Definition 2.1.** Let  $n$  be an odd number and not a perfect square, and let  $c = \text{Ind}_F(c)$  be the 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

$$z^n \equiv \bar{z} \pmod{n}. \quad (2)$$

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

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

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

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

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

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

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

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

Note that if  $n$  is  $FPP(a, b, c)$ , 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 part 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. It is also useless to seek a counterexample by a straightforward search. For as it will be proved in Proposition 3.14 it is not among the numbers less than  $2^{64}$ . It is more likely to find a FPP in the form of the product of primes.

*Remark 2.6.* The choice with the base  $z = 2 + \sqrt{c}$  or  $z = 1 + \sqrt{c}$  is not random. For some  $n$  may exist “bad” bases, or in the terminology of the work [4] “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

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

**Definition 2.7.** 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  $J(c/p) = -1$ .

Each FPP has an odd number of  $\Phi$ -negative factors and arbitrary number of  $\Phi$ -positive.

## 2.2 First important theorem

The following statement (in slightly different formulations) is proved in [4, 9].

**Theorem 2.8.** Let  $n$  be an FPP( $a, b, c$ ),  $n = pq$  where  $p$  is prime. Then

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

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

$$z^{pq} \equiv (z^p)^q \equiv \bar{z}^q \equiv \bar{z} \pmod{p},$$

and

$$z^q \equiv z \pmod{p}.$$

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

$$z^{pq} \equiv (z^p)^q \equiv z^q \equiv \bar{z} \pmod{p}.$$

□

**Corollary 2.9.** Let  $n$  be an FPP( $a, b, c$ ) and  $p$  be a  $\Phi$ -negative prime divisor,  $Q = \text{ord}(z \pmod{p})$ . Then

$$n/p \equiv 1 \pmod{Q},$$

$$n \equiv p \pmod{Q}.$$

**Corollary 2.10.** Let  $z = a + b\sqrt{c} \in \mathbb{Z}$  and  $z^q = a_q + b_q\sqrt{c} \in \mathbb{Z}$  and  $n$  be 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 2.11.** 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 factor of 104005: 5, 11, 31, 61.

**Example 2.12.** 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 so  $p$  can be only 37.

*Remark 2.13.* 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 2.14.** *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*

$$z^p \equiv \bar{z} \pmod{p^2}.$$

*Proof.* In the ring  $\mathbb{Z}_{p^2}[\sqrt{c}]$ :

$$(a + pb)^p \equiv a^p \pmod{p^2}.$$

So

$$z^{p^2q} \equiv \bar{z} \pmod{p^2q},$$

and therefore

$$z^{p^2q} \equiv \bar{z} \pmod{p}.$$

As  $z^{p^2} \equiv z \pmod{p}$ , so  $z^q \equiv z^p \equiv \bar{z} \pmod{p}$  and

$$z^p \equiv \bar{z} + pu \pmod{p^2},$$

$$z^q \equiv \bar{z} + pv \pmod{p^2}$$

for some  $u, v \in \mathbb{Z}_p[\sqrt{c}]$ . Then

$$z^{p^q} \equiv (z^q)^p \equiv (\bar{z} + pv)^p \equiv \bar{z}^p \equiv z + p\bar{u} \pmod{p^2},$$

$$z^{p^2q} \equiv (z^{p^q})^p \equiv (z + p\bar{u})^p \equiv \bar{z} + pu \pmod{p^2}.$$

On the other hand  $z^n \equiv \bar{z} \pmod{p^2}$ , that is  $u = 0$  therefore  $z^p \equiv \bar{z} \pmod{p^2}$ . □

**Corollary 2.15.** *If  $n = p^2q$  is a FPP( $a, b, c$ ), then  $p^2$  is also FPP( $a, b, c$ ).*

**Corollary 2.16.** *If  $n = p^2q$  is a FPP( $a, b, c$ ), then  $N(z)^{p-1} \equiv 1 \pmod{p^2}$ , where  $N(z)$  is a norm of  $z$ .*

### 2.4 $\Phi$ -positive factor

There are very few such numbers (see section 3.5), but they still exist.

**Theorem 2.17.** *Let  $n$  be a Frobenius pseudoprime,  $z = a + b\sqrt{c}$  and  $p$  is a  $\Phi$ -positive prime factor of  $n$ ,  $n = p \cdot q$ ,  $c \equiv d^2 \pmod{p}$ . We introduce the notation:*

$$z_1 = a + b \cdot d \pmod{p},$$

$$z_2 = a - b \cdot d \pmod{p},$$

$z_1, z_2 \in \mathbb{Z}_p$ . Then

$$z_1^q \equiv z_2 \pmod{p}, \tag{3}$$

$$z_2^q \equiv z_1 \pmod{p}, \tag{4}$$

*Proof.* By definition:

$$(a + b\sqrt{c})^{p^q} = a - b\sqrt{c} \pmod{p}.$$

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

$$(a + b\sqrt{c})^q = a - b\sqrt{c} \pmod{p}$$

Using isomorphism  $\mathbb{Z}_p[\sqrt{c}] \rightarrow \mathbb{Z}_p \times \mathbb{Z}_p$ , we obtain the required. □

**Corollary 2.18.** *Let*

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

and

$$w = z_1/z_2 = \frac{(a + bd)^2}{N} \pmod{p}.$$

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 2.19.** *Let  $\alpha = \text{ord}(N \bmod p)$  and  $\beta = \text{ord}(w \bmod p)$ . Then*

$$\gcd(\alpha, \beta) \leq 2.$$

*Proof.* We have

$$q - 1 \equiv 0 \pmod{\alpha},$$

$$q + 1 \equiv 0 \pmod{\beta}.$$

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

**Corollary 2.20.** *Let  $n$  be a Frobenius pseudoprime,  $z = a + b\sqrt{c}$ ,  $p$  be a  $\Phi$ -positive prime factor of  $n$  and  $q = n/p$ . Then*

$$q \equiv A_p \pmod{M_p},$$

where

$$M_p = \text{lcm}(\text{ord}(z_1 \bmod p), \text{ord}(z_2 \bmod p)).$$

*Proof.* If  $q$  is increased by a multiple of  $\text{ord}(z_1 \bmod p)$  and  $\text{ord}(z_2 \bmod p)$ , then both sides of the equalities (3) and (4) do not change.

Note that both  $\text{ord}(z_1 \bmod p)$  and  $\text{ord}(z_2 \bmod p)$  are divisors of  $p - 1$ , so their least common multiple is also a divisor of  $p - 1$ . □

## 2.5 $\Phi$ -negative factor

**Theorem 2.21.** *Let  $p$  be a  $\Phi$ -negative prime divisor of FPP  $n$ , that is  $J(N(z), p) = -1$ . Denote  $Q = \text{ord}(z \bmod p)$ . Then co-order  $(p^2 - 1)/Q$  is odd. In particular, it follows that  $Q \equiv 0 \pmod{8}$ .*

*Proof.* As  $z^p \equiv \bar{z} \pmod{p}$ , then  $N(z) = z \cdot \bar{z} = z^{p+1}$ , so  $z^{(p^2-1)/2} = N(z)^{(p-1)/2} = J(N(z), p)$ . As  $z^{(p^2-1)/2} \neq 1$ , then co-order is odd. □

**Theorem 2.22.** *Let  $n$  be an FPP,  $c = \text{ind}_F(n)$  be its Frobenius index and  $p$  be an  $\Phi$ -negative prime divisor of  $n$ .*

- a) *If  $c = -1$ , then  $p \equiv 3 \pmod{4}$ .*
  - b) *If  $c = 2$ , then  $p \equiv 5 \pmod{8}$  and the product of all  $\Phi$ -negative prime divisors of  $n$  equals to  $1 \pmod{8}$ .*
  - c) *If  $c = 3$ , then  $p \equiv 17|19 \pmod{24}$ . In this case, there must be an odd number of divisors equals 17 modulo 24 (therefore, at least one is required). There must be an even number of divisors  $p_i$  which equals 19 modulo 24 and  $\gcd(24, \text{ord}(z \bmod p_i)) \leq 2$ .*
  - d) *If  $c = 5$ , then  $p \equiv 1 \pmod{4}$ .*
  - e) *If  $c = 7$ , then  $(p \bmod 24) < 12$  (that is  $1|5|7|11$ ).*
- Denote  $\text{ord}(z \bmod p)$  by  $Q$  and  $\gcd(Q, 24)$  by  $d$ .*
- f) *If  $c \geq 5$ , then  $p \equiv 1 \pmod{d}$ .*
  - g) *If  $c \geq 5$  and  $c'$  is a prime divisor of  $Q$ ,  $c' < c$ , then  $J(p, c') = 1$  (not  $J(c', p)$ , but  $J(p, c')$ ).*

*Proof.* Let  $n = pq$  and  $Q$  be an order of  $z$  modulo  $p$ .

a) by definition of  $\Phi$ -negative divisor.

b) as  $\text{ind}_F(n) = 2$ , then  $n \equiv 5 \pmod{8}$  and  $z = 2 + \sqrt{2}$ ,  $N(z) = z \cdot \bar{z} = 2$ .

By Thm. 2.8 we have  $q \equiv 1 \pmod{Q}$ . However according to Thm. 2.21 the number  $Q$  is divisible by 8 which means  $q \equiv 1 \pmod{8}$ . Therefore,  $n = pq \equiv p \pmod{8} = 5$ .

Thus, the product of all  $\Phi$ -negative prime divisors of  $n$  is 1 or 5 modulo 8. Each  $\Phi$ -positive prime divisor equals to  $\pm 1 \pmod{8}$ , therefore their product  $\equiv \pm 1 \pmod{8}$ . But  $-1$  is impossible, since in this case condition  $n \equiv 5 \pmod{8}$  fails.

c) In this case  $n \equiv 17 \pmod{24}$ . Since  $J(3/p) = -1$ ,  $p \equiv \pm 5 \pmod{12}$ , that is  $p \equiv 5|7|17|19 \pmod{24}$ . In this case  $N(z) = N(1 + \sqrt{3}) = -2$ . If  $p \equiv 5|7 \pmod{24}$ , then  $J(N(z), p) = -1$ . It follows from Thm. 2.21 that in this case  $Q$  is divided by 8, that is  $q \equiv 1 \pmod{8}$ . So  $n = pq \equiv p \pmod{8} = 5|7$ , which contradicts the fact that  $n \equiv 17 \pmod{24}$ .

Let  $p \equiv 19 \pmod{24}$ . Then

- $q \equiv 11 \pmod{24}$ .
- $q \equiv 1 \pmod{\text{ord}(z, p)}$ .

Let  $d = \gcd(\text{ord}(z, p), 24)$ . Therefore,  $10 \equiv 0 \pmod{d}$ , which is only possible if  $\gcd(\text{ord}(z, p), 24) = 2$  or  $1$ .

The statement about the number of multipliers follows from the fact that  $n \equiv 17 \pmod{24}$  and  $g^2 = 1$  for all  $g \in \mathbb{Z}_{24}^*$ .

d) If  $c = 5$ , then  $z = 1 + \sqrt{5}$ ,  $N(z) = 1 - 5 = -4$  and  $J(N(z), p) = J(-1, p)$ . Assume that  $p \equiv 3 \pmod{4}$ , then  $J(N(z), p) = -1$  and according to the theorem (2.21),  $Q = \text{ord}(z \pmod{p})$  is divided by 8. Since  $q \equiv 1 \pmod{Q}$ , then  $n = pq \equiv 3 \pmod{4}$ . But Frobenius index  $\geq 5$ , so  $n \equiv 1 \pmod{24}$ .

e) Since  $z = 1 + \sqrt{7}$ , then  $N(z) = 1 - 7 = -6$ . Therefore  $J(N(z), n) = 1$  if  $n \equiv 1, 5, 7, 11 \pmod{24}$  and  $J(N(z), n) = -1$  if  $n \equiv 13, 17, 19, 23 \pmod{24}$ .

In second case  $\text{ord}(z, p)$  is divided by 8 and congruence  $pq \equiv 1 \pmod{24}$  are impossible.

Thus, if  $c = 7$ , then all  $\Phi$ -negative prime divisors of an FPP must be congruenced 1, 5, 7 or 11 modulo 24.

f) All invertible residues  $k$  modulo 24 have a useful property:  $k^2 \equiv 1 \pmod{24}$ . So the congruence  $pq \equiv 1 \pmod{24}$  can be rewritten as  $q \equiv p \pmod{24}$ . With the congruence  $q \equiv 1 \pmod{Q}$  we get what we need.

g) By definition Frobenius index  $J(c', n)$  must be equals 1. Since  $n \equiv 1 \pmod{24}$  and  $J(q, c') = J(1 + \alpha c', c') = 1$ .

$$J(c', n) = J(n, c') = J(pq, c') = J(p, c')J(q, c') = J(p, c') = +1.$$

□

## 2.6 z-consistent prime factors

**Theorem 2.23.** *Let  $n$  be an FPP and  $p_1, p_2$  its two  $\Phi$ -negative divisors. If  $d = \text{GCD}(\text{ord}(z, p_1), \text{ord}(z, p_2)) > 1$  then*

$$p_1 \equiv p_2 \pmod{d}$$

*Proof.* From Corollary 2.9, it follows

$$n \equiv p_1 \pmod{\text{ord}(z, p_2)},$$

$$n \equiv p_2 \pmod{\text{ord}(z, p_1)}.$$

Therefore

$$n \equiv p_1 \equiv p_2 \pmod{d}.$$

□

**Theorem 2.24.** *Let  $n$  be an FPP( $a, b, c$ ),  $p$  is  $\Phi$ -negative prime divisor and  $Q = \text{ord}(z \pmod{p})$ . Then  $Q$  and  $n$  are coprime.*

*Proof.* We need to prove that  $Q$  is not divisible by any prime divisor of  $n$ , including  $p$ . The number  $Q$  is a divisor of  $p^2 - 1$  and, therefore, is not divisible by  $p$ .

According to Corollary 2.9  $n/p \equiv 1 \pmod{Q}$ , so  $Q$  is coprime with  $n/p$ , hence  $Q$  is coprime with each of its prime divisors. □

**Definition 2.25.** A pair of primes divisors  $(p_1, p_2)$  of FPP  $n$  is called  $z$ -consistent if:

$$\begin{aligned} J(c/p_1) &= -1 \\ J(c/p_2) &= -1 \\ \text{ord}(z, p_1) &\not\equiv 0 \pmod{p_2} \\ \text{ord}(z, p_2) &\not\equiv 0 \pmod{p_1} \\ p_1 &\equiv p_2 \pmod{\text{GCD}(\text{ord}(z, p_1), \text{ord}(z, p_2))}. \end{aligned}$$

Thus, all  $\Phi$ -negative FPP divisors are pairwise consistent.

Let  $n$  be FPP and  $p$  its  $\Phi$ -positive prime factors. Corollary 2.20 implies

$$n \equiv D_p \pmod{M_p},$$

for some  $D_p, M_p$ .

If  $p$  is a  $\Phi$ -negative prime factor  $n$ , according to the main Thm. 2.8

$$q \equiv 1 \pmod{\text{ord}(z \pmod{p})}$$

or

$$n \equiv D_p \pmod{M_p},$$

where  $D_p = p$ ,  $M_p = \text{ord}(z \pmod{p})$ .

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

$$n \equiv D_{p_1} \pmod{M_{p_1}},$$

$$n \equiv D_{p_2} \pmod{M_{p_2}}.$$

From this it follows that in this case we have

$$D_{p_1} \equiv D_{p_2} \pmod{\text{gcd}(M_{p_1}, M_{p_2})}. \tag{5}$$

This relation does not depend on  $q$ , only on  $p_1$  and  $p_2$ .

**Definition 2.26.** Given  $z \in \mathbb{Z}[\sqrt{c}]$ . Two primes will be called  $z$ -consistent or simply consistent if the relation (5) holds for them.

**Theorem 2.27.** *Let  $n$  be a Frobenius pseudoprime. Then all its prime factors are pairwise consistent.*

### 3 Results of calculations

The hypothesis asserting that there are no Frobenius pseudoprimes (FPP) can not yet be proved. Below are related results that we were able to establish.

#### 3.1 Search for small FPP

We considered all composite odd numbers that are not complete squares. All such numbers up to  $350 \cdot 10^9$  were checked on being a FPP. This computation took few days on a standard PC (Intel(R) Pentium(R) CPU G4500 @3.50GHz). As the result we have the following proposition.

**Proposition 3.1.** *There is no FPP less than 350 billions.*

#### 3.2 Search for large FPP with a large Frobenius index

As it was mentioned above, if  $n \equiv 1 \pmod{24}$  then  $\text{ind}_F(n) \geq 5$ . The Frobenius index can be arbitrarily large. Among the numbers  $< 2^{32}$ , the largest value of the index is 101 and it is for the number 2805 44 681. In [7] a complete list of 458 069 912 numbers less than  $2^{64}$ , whose index of Frobenius  $> 128$  is obtained. All these numbers are not FPP. As the result we have the following proposition.

**Proposition 3.2.** *[7] There is no FPP less than  $2^{64}$  with the Frobenius index larger than 128.*



### 3.3 Search for large FPP with multiple factors

Sec. 2.3 contains proofs of the properties that should be satisfied by 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 computation time (with 3.50GHz) is about two days. As the result we have the following proposition.

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

### 3.4 Estimation of the product of all factors except one (for FPP)

We propose the following idea to significantly simplify the search for FPP.

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  $z^q = a_q + b_q\sqrt{c}$ . Corollary 2.10 implies that for every  $q$  there is a small number of possible  $p$ , as  $p$  has to be a divisor of  $D = \gcd(a_q - a, b_q \pm b)$ , where the sign "+" or "-" is taken depending on the sign a  $J(c/q)$ .

*In practice it turned out that the number of possibilities for  $p$  is not just small but very small: about 1 to 3 different  $p$ .*

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  $D$ :  $D = p_1 \dots p_s$ ,
4. for each  $p_i$  check whether  $n_i = q \cdot p_i$  is 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  $n/p < 2^{21}$ .*

### 3.5 A complete list of $\Phi$ -positive prime factors less than $2^{32}$ for a FPP

In Sec. 2.4 properties of the  $\Phi$ -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  $\Phi$ -positive prime factors  $p$  and some congruence relation for  $q$ :

$$q \equiv q_p \pmod{A_p}$$

for a given  $p$ . An additional constraint comes from the congruence relation implied by the Frobenius index:

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

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:

$c$	$p$	$c$	$p$	$c$	$p$	$c$	$p$
-1	2276629	11	98641	61	271	89	109000877
-1	30906409	17	125597	67	75011	89	136973443
-1	806361541	23	5966803	67	25742443	101	137
2	8191	29	12637	83	1931	103	6863
2	2147483647	31	3596719249	83	3278741	103	3523679801
7	31	43	329947	83	806898559	107	219920461
7	3923					127	713342911

If we assume that  $n = pq < 2^{64}$  then most of these  $n$  can be directly checked whether they are a FPP or not. After this, only the following eight numbers remain, for which a direct verification is still difficult (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

Note that in the case of a large Frobenius index, the computation can be significantly reduced if you do not iterate over all numbers that are multiples of  $p$ , but only over those for which the Frobenius index is equal to the given  $c$  (as given in the table above). After that, only the following list of five  $\Phi$ -positive divisors remains unchecked:

$c$	$p$	$c$	$p$	$c$	$p$
2	8191	7	3923	101	137
7	31	61	271		

We see an FPP  $n$  such that  $n < 2^{64}$  has two  $\Phi$ -positive factors less than  $2^{32}$  only if its Frobenius index  $\text{ind}_F$  is 7. That is  $z = 1 + \sqrt{7}$ , and these factors are 31 and 3923. By direct verification within a reasonable time (several hours), one can make sure that both factors can't occur simultaneously. As the result we have the following statement.

**Proposition 3.5.**  *$\Phi$ -positive prime factors less than  $2^{32}$  for FPPs smaller than  $2^{64}$  can be only 5 numbers mentioned above, and two such factors can not meet simultaneously.*

### 3.6 The main proposition: there are no FPP less than $2^{64}$

Let  $n, n < 2^{64}$  be an FPP. Below it a summary of what we have discovered so far for such numbers:

- $n > 350 \cdot 10^9$  (Proposition (3.1)).
- Frobenius index  $c = \text{ind}_F(n) < 128$  (Proposition (3.2)).
- $n$  does not have multiple factors (Proposition (3.3)).
- The product of all prime factors except one is greater then  $2^{21}$  (Proposition (3.4)).
- $\Phi$ -positive factors  $p$  may be only for  $c = 2$  ( $p = 8191$ ),  $c = 7$  ( $p = 31, 3923$ ),  $c = 61$  ( $p = 271$ ),  $c = 101$  ( $p = 137$ )(Proposition (3.5)).

Later in this section, we assume that FPP  $n$  satisfies all these conditions.

**Proposition 3.6.** *Let  $n < 2^{64}$  be an FPP. Then  $n$  does not have prime factors from the interval  $(50159, 2^{32})$ .*

*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 Thm. 2.8

$$z^{q-1} \equiv 1 \pmod{p},$$

that is

$$q \equiv 1 \pmod{\text{ord}(z \pmod{p})}.$$

or

$$q = 1 + kQ_p$$

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

$$p(1 + Q_p), p(1 + 2Q_p), \dots, p(1 + k_{max}Q_p).$$

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  $(2^{17}, 2^{32})$ .  $\square$

**Example 3.7.** Let  $z = 2 + i$ ,  $p = 10\,000\,019$ . Then  $Q_p = 1\,666\,730\,000\,060 = (p^2 - 1)/6$  and for any  $k \geq 1$  we have  $n = pq > 2^{64}$ . That is for this  $p$  there is no suitable  $q$ .

Let  $p = 1\,000\,003$ . Then  $Q_p = 1\,000\,006\,000\,008 = p^2 - 1$  and inequality  $n = pq < 2^{64}$  holds for  $k \leq 18$ . That is the only suitable values for  $q$  are

$$1 + Q_p, 1 + 2Q_p, \dots, 1 + 18Q_p.$$

It is easy to check that for all these values of  $q$ , the number  $n = pq$  is not an FPP, that is  $p$  cannot be a divisor of an FPP that is less than  $2^{64}$ .

Let  $p = 100\,003$ . Then  $Q_p = 434\,808\,696 = (p^2 - 1)/23$  and inequality  $n = pq < 2^{64}$  holds for  $k \leq 424\,236$ . With the smaller  $p$  the computation time quickly increases. Verification of all eligible  $q$  in this case takes already several minutes.

By a somewhat larger search, it is possible to construct for each index  $c < 128$  a complete list of possible  $\Phi$ -negative prime factors of FPP. For example, for  $c = -1$  ( $z = 2 + i$ ) the list will consist of 350 prime numbers:

$$7, 11, 19, 23, 31, 43, 47, \dots, 39439, 50159.$$

$\text{ind}_F$	The number of primes	$\max(p_i)$	$\text{ind}_F$	The number of primes	$\max(p_i)$
-1	350	50159	53	39	21841
2	91	33461	59	40	5651
3	72	23057	61	39	17749
5	105	49477	67	31	5557
7	48	47791	71	30	34501
11	50	9437	73	34	6883
13	63	19141	79	32	9041
17	50	8681	83	33	38669
19	38	25939	89	26	7867
23	44	8069	97	32	6221
29	46	7687	101	46	9901
31	37	38917	103	30	14341
37	55	15289	107	21	8539
41	39	19447	109	38	13001
43	37	15277	113	37	13241
47	36	12109	127	22	4987

**Corollary 3.8.** Let  $n < 2^{64}$  be an FPP. Then  $n$  has more than two prime factors.

*Proof.* If  $n$  has exactly two prime factors, then the smallest of them by the Proposition 3.6 should not be more than 50159, which contradicts Proposition 3.5.  $\square$

**Proposition 3.9.** Let  $n < 2^{64}$  be an FPP and  $p_1, p_2$  be its prime factors, both less  $2^{32}$ . Then  $p_1 p_2 < 2^{17}$ .

Moreover, for each  $c < 128$ , we have a complete list of possible pairs  $(p_1, p_2)$ :

$\text{ind}_F$	The number of pairs	$\max(p_1 p_2)$	$\text{ind}_F$	The number of pairs	$\max(p_1 p_2)$
-1	184	128929	53	2	53947
2	64	28345	59	2	29857
3	36	40681	61	0	—
5	56	58669	67	1	66667
7	11	24641	71	0	—
11	8	42127	73	0	—
13	31	42199	79	0	—
17	22	77981	83	0	—
19	0	—	89	1	58277
23	1	24461	97	1	29651
29	1	53947	101	0	—
31	5	34103	103	0	—
37	7	58969	107	0	—
41	0	—	109	0	—
43	0	—	113	0	—
47	4	103351	127	0	—

*Proof.* Suppose that an FPP  $n$  has two factors of  $p_1$  and  $p_2$  less than  $2^{32}$ . Then both  $p_1$  and  $p_2$  should be contained in a relatively small list which is constructed using Proposition 3.6.

Factors need to be  $z$ -consistent and for  $q = n/(p_1 p_2)$  the following congruence relations should hold:

$$q \equiv D_{p_{12}} \pmod{\gcd(M_{p_1}, M_{p_2})}$$

for some  $D_{p_{12}}$ .

Taking into account that  $n = p_1 p_2 q < 2^{64}$ , it often turns out that for a given pair  $(p_1, p_2)$  all possible  $q$  are small and all corresponding  $n$  can be thus easily checked whether they are an FPP or not. However, if  $(p_1, p_2)$  are small in a sense then the number of possible  $q$ s is too large and we cannot check all of the corresponding  $n$  on being an FPP, and these are listed in the table above. (These remaining pairs will be addressed below).  $\square$

*Remark 3.10.* Among these pairs, there are none containing  $\Phi$ -positive numbers. In particular, an FPP  $n$  does not have  $\Phi$ -positive factors less than  $2^{32}$ .

**Corollary 3.11.** *Let  $n < 2^{64}$  be an FPP. Then  $n$  has more than three prime factors.*

*Proof.* If  $n$  has exactly three prime factors, at least two of them are less  $2^{32}$  and according Proposition 3.9 their product is less than 128929, which contradicts Proposition 3.5.  $\square$

**Proposition 3.12.** *Let  $n < 2^{64}$  be an FPP and  $p_1, p_2, p_3$  be its prime factors less than  $2^{32}$ . Then  $c = -1$  and triple  $(p_1, p_2, p_3)$  is one of the following:*

$p_1$	$p_2$	$p_3$
199	19	7
191	127	31
191	71	11
79	31	19
79	19	7
71	47	11

*Proof.* Pairs  $(p_1, p_2)$ ,  $(p_1, p_3)$ ,  $(p_2, p_3)$  must be present in the list of valid pairs given in Proposition 3.9. There are very few such triples. For almost all triples all their possible multiples  $n = p_1 p_2 p_3 q$  can be checked on being an FPP in a short time (hours). Only those triplets that are specified in the statement of Proposition 3.12 are remained as a possibility.  $\square$

We have already established in Corollaries 3.8 and 3.11 that an FPP  $n$ ,  $n < 2^{64}$  has more than two and than more than three prime factors.

**Corollary 3.13.** *Let  $n < 2^{64}$  be an FPP. Then  $n$  has more than four prime factors.*

*Proof.* If  $n$  has exactly four prime factors, at least three of them are less  $2^{32}$  and by Proposition 3.5 their product is greater than  $2^{21}$ . However, then for all triplets in Proposition 3.12 the product  $p_1p_2p_3$  is less than  $2^{21}$ .  $\square$

**Proposition 3.14.** *There are no FPP less than  $2^{64}$ .*

*Proof.* By Corollary 3.13, an FPP  $n$  has at least four prime factors  $< 2^{32}$ . Each triple of these four must be present in the list of Proposition 3.12. But they are not there.  $\square$

## 4 An FPP cannot be a product of small factors

**Proposition 4.1.** *Let  $n$  be an FPP. Then  $n$  has a prime divisor larger than 3000.*

To verify this statement, for each Frobenius index  $c < 3000$ , we iterate over all subsets of valid prime factors, and they must all be pairwise consistent.

*Remark 4.2.* In fact, the lower bound 3000 given in Proposition 4.1 can be improved for each  $c$ . Below is the list of obtained lower bounds.

$\text{ind}_F$	border	$\text{ind}_F$	border	$\text{ind}_F$	border	$\text{ind}_F$	border
-1	3067	53	4513	131	5897	223	6073
2	3109	59	4177	137	5209	227	5881
3	3089	61	4909	139	5881	229	5849
5	3793	67	5077	149	6217	233	5441
7	4177	71	5573	151	5113	239	6661
11	3637	73	4273	157	6829	241	5857
13	3049	79	5449	163	7057	251	6637
17	3361	83	5449	167	6449	...	...
19	4649	89	5189	173	4937	2971	7537
23	3251	97	6003	179	6361	2999	9293
29	3361	101	4253	181	5209		
31	3733	103	6217	191	6823		
37	3169	107	6037	193	3469		
41	3529	109	4657	197	5449		
43	3677	113	4789	199	6361		
47	4273	127	6569	211	6121		

*Remark 4.3.* These lower bounds depends only on our computational capabilities (within a few hours of processor time). Unfortunately, the volume of computations is growing exponentially, so it is not possible to significantly improve these bounds, even with the increase of the computation time.

## 5 Conclusions

The FPP numbers are those on which the Frobenius test is fail.

**Hypothesis.** *There are no Frobenius pseudoprime numbers.*

Below are the facts about FPP that are known to date along with some new facts established in the present paper.

- The complexity of the Frobenius test is about twice that of Fermat or Miller-Rabin.
- There are no examples of FPPs.
- There are no FPPs less than  $2^{64}$ .
- Each FPP has a prime factor larger than 3000.
- Frobenius test is one of the most efficient primality tests to date!

## References

- [1] R. Baillie, S.S. Wagstaff, Jr. *Lucas Pseudoprimes*, Math. Comp. 35 (1980), no. 152, 1391–1417.
- [2] A.I. Borevich, I.R. Shafarevich, *Number theory. Pure and Applied Mathematics.*, Translated from the Russian by Newcomb Greenleaf, vol. 20, Academic Press, New York-London, 1966.
- [3] R.E. Crandall, C.Pomerance: *Prime Numbers: A Computational Perspective*, Springer-Verlag, 2005.
- [4] I.B. Damgard, G.S. Frandsen, *An Extended Quadratic Frobenius Primality Test with Average- and Worst-Case Error Estimate*. Journal of Cryptology, vol. 19, n. 4 (2006), p. 489–520.
- [5] J. Feitsma *Tables of pseudoprimes and related data*.  
<http://www.cecm.sfu.ca/Pseudoprimes/index-2-to-64.html>
- [6] J. Grantham, *Frobenius pseudoprimes*, Math. Comp., 70 (2001), n. 234, p. 873–891.
- [7] S.I. Khashin, *Natural numbers with large Frobenius index*. Vest.IvGU. 2015. v.2. p. 75–78.
- [8] C. Pomerance, M. Th. Rassias, *Analytic Number Theory.*, 2015. Springer, New York.
- [9] M. Seysen, *A Simplified Quadratic Frobenius Primality Test*. IACR Cryptol. ePrint Arch., 2005, 462.
- [10] J. Sorenson, J. Webster, *Strong Pseudoprimes to Twelve Prime Bases*, Math. Comp. 86 (2017), 985-1003.