JSIAM Letters Vol.11 (2019) pp.53–55 ©2019 Japan Society for Industrial and Applied Mathematics JSIAM Letters

Quadratic Frobenius pseudoprimes with respect to $x^2 + 5x + 5$

Saki Nagashima[1], Naoyuki Shinohara[2] and Shigenori Uchiyama[1]

[1] Tokyo Metropolitan University, 1-1 Minamiosawa, Hachioji-shi, Tokyo 192-0397, Japan
[2] National Institute of Information and Communications Technology, 4-2-1 Nukuikita-machi, Koganei-shi, Tokyo 184-8795, Japan

E-mail *nagashima-saki@ed.tmu.ac.jp*

Received January 15, 2019, Accepted April 24, 2019

Abstract

The quadratic Frobenius test is a primality test. Some composite numbers may pass the test and such numbers are called quadratic Frobenius pseudoprimes. No quadratic Frobenius pseudoprimes with respect to $x^2 + 5x + 5$, which are congruent to 2 or 3 modulo 5, have been found. Shinohara studied a specific type of such a quadratic Frobenius pseudoprime, which is a product of distinct prime numbers p and q. He showed experimentally that p must be larger than 10^9, if such a quadratic Frobenius pseudoprime exists. The present paper extends the lower bound of p to 10^{11}.

Keywords quadratic Frobenius pseudoprime, primality test, primality-proving algorithm

Research Activity Group Algorithmic Number Theory and Its Applications

1. Introduction

Prime numbers are currently used in many cryptosystems. For example, RSA-2048 cryptosystem uses two 1024-bit prime numbers as its secret keys. To generate those prime numbers, we can select two kinds of algorithms to determine whether a positive integer is a prime. One kind comprises primality tests and the others are called primality-proving algorithms. A primality test is probabilistic; namely, some composite numbers may pass it. There are efficient primality tests such as the Miller-Rabin test and the quadratic Frobenius test whose time complexities are $O((\log n)^3)$ for a given integer n. On the other hand, primality-proving algorithms are deterministic algorithms, and thus no composite numbers pass their tests. However, the known primality-proving algorithms have high computational costs or require certain information to be able to apply them to a given integer n, for example, knowledge of the integer factorization of $n - 1$.

The AKS method is the only polynomial-time primality-proving algorithm not requiring any additional information. However, the AKS method is not as practical as the Miller-Rabin test and the quadratic Frobenius test, because its complexity is $\widetilde{O}((\log n)^6)$.

It is expected to construct an efficient primality-proving algorithm from some primality tests, by improving those tests.

We consider the quadratic Frobenius pseudoprimes with respect to $x^2 + 5x + 5$. No quadratic Frobenius pseudoprimes with respect to $x^2 + 5x + 5$, which are congruent to 2 or 3 modulo 5, have yet been found. Shinohara studied quadratic Frobenius pseudoprimes of the form pq with respect to $x^2 + 5x + 5$, where p and q are primes, p is congruent to 1 or 4 modulo 5, and q is congruent to 2 or 3 modulo 5. He proposed an algorithm for searching for them and experimentally showed that p must be larger than 10^9 if such a quadratic Frobenius pseudoprime exists. The present paper extends the lower bound of p to 10^{11}.

2. Preliminaries

Throughout this section, we assume that a, b are integers such that $\Delta = a^2 - 4b \neq 0$ unless otherwise indicated.

Theorem 1 ([1]). Let $f(x) = x^2 - ax + b$. If n is a prime number and $\gcd(n, 2b\Delta) = 1$, then

$$x^n \equiv \begin{cases} a - x \pmod{(f(x), n)}, & (\frac{\Delta}{n}) = -1, \\ x \pmod{(f(x), n)}, & (\frac{\Delta}{n}) = 1. \end{cases} \tag{1}$$

($(\frac{\cdot}{\cdot})$ is the Jacobi symbol.)

Definition 2 ([1]). We say that a composite number n such that $\gcd(n, 2b\Delta) = 1$ is a quadratic Frobenius pseudoprime with respect to $f(x) = x^2 - ax + b$ if (1) holds for n. Next, let $\mathrm{fpsp}(a, b)$ denote the set of all quadratic Frobenius pseudprimes with respect to $f(x) = x^2 - ax + b$.

Definition 3 ([1]). We refer to an element of $\mathrm{fpsp}(a, b)$ such that $(\frac{\Delta}{n}) = -1$ as a quadratic Frobenius pseudoprime of the second type with respect to $f(x) = x^2 - ax + b$. We denote the set of such numbers by $\mathrm{fpsp2}(a, b)$.

Here, we give the equivalence condition for an element being in $\mathrm{fpsp2}(a, b)$.

Definition 4 ([1]). For a positive integer n satisfying $\gcd(n, 2b\Delta) = 1$, we suppose the factorization $n = \prod_{i=1}^{k+l} p_i^{e_i}$, where k, l are positive integers, $(\frac{\Delta}{p_i}) = -1$

for $i \in [1,k]$ and $(\frac{\Delta}{p_i}) = 1$ for $i \in [k+1, k+l]$. Moreover, let $\Phi_m(x)$ be the m-th cyclotomic polynomial and $f(x) = x^2 - ax + b$. Then, we refer to the set of the following conditions on (n, a, b) as ICF2.
(ICF2-1) For each $i \in [1,k]$, there exists m_i such that $m_i \mid \gcd(\frac{n}{p_i} - 1, p_i^2 - 1)$, $m_i \nmid p_i - 1$, and $\Phi_{m_i}(x) \equiv 0 \pmod{(f(x), p_i^{e_i})}$.
(ICF2-2) $\sum_{i=1}^{k} e_i \equiv 1 \pmod 2$.
(ICF2-3) For each $i \in [k+1, k+l]$, there exists c_i such that $f(x) \equiv (x - c_i)(x - c_i^n) \pmod{p_i^{e_i}}$.
(ICF2-4) For each $i \in [k+1, k+l]$, there exists m_i such that $m_i \mid \gcd(\frac{n^2}{p_i^2} - 1, p_i - 1)$, $m_i \nmid n - 1$, and $\Phi_{m_i}(x) \equiv 0 \pmod{(x - c_i, p_i^{e_i})}$.

Theorem 5 ([1]). An odd composite number n is in fpsp2(a, b) if and only if ICF2 holds for n and (a, b).

3. Grantham's Problem

When considering the construction of a primality-proving algorithm from the quadratic Frobenius test, the following very interesting problem arises, in which we fix $f(x) = x^2 + 5x + 5$.

Problem 6 (Grantham's Problem [1–3]). Are there any composite numbers n such that

$$n \equiv \pm 2 \pmod 5, \quad x^{n+1} \equiv 5 \pmod{(f(x), n)}? \quad (2)$$

The discriminant Δ is equal to 5 and $n \equiv \pm 2 \pmod 5$, so $(\frac{\Delta}{n}) = -1$. Therefore, if there exists a composite number n satisfying (2), then n is in fpsp2$(-5, 5)$.

We assume that there exists an element of fpsp2$(-5, 5)$ which is a product of two distinct prime numbers. In other words, we assume that there exist prime numbers p, q such that $p \equiv \pm 1 \pmod 5$, $q \equiv \pm 2 \pmod 5$, and pq is in fpsp2$(-5, 5)$. We denote the set of such numbers by fpsp2_2$(-5, 5)$.

Lemma 7 ([1]). Let q be an odd prime number. Suppose that a, b are integers such that $(\frac{\Delta}{q}) = (\frac{b}{q}) = -1$, where $\Delta = a^2 - 4b$. Let m be the order of $x \in \mathbb{F}_q[x]/(f(x))$ and $q^2 - 1 = 2^s t$ where t is odd. Then 2^s divides m.

As $q^2 - 1 = (q+1)(q-1)$ is always divisible by 8, we have the following.

Corollary 8 ([1]). Let q be an odd prime number. Suppose that a, b are integers such that $(\frac{\Delta}{q}) = (\frac{b}{q}) = -1$, where $\Delta = a^2 - 4b$. Then 8 divides the order of $x \in \mathbb{F}_q[x]/(f(x))$.

From Theorem 5, Lemma 7 and Corollary 8, we have the following theorem.

Theorem 9 ([1]). Let p, q be prime numbers such that $(\frac{5}{p}) = 1$ and $(\frac{5}{q}) = -1$. Then there exist integers c_1, c_2 such that $f(x) \equiv (x - c_1)(x - c_2) \pmod p$. Let m_q be the order of $x \in \mathbb{F}_q[x]/(f(x))$. Then pq is in fpsp2$(-5, 5)$ if and only if the following conditions hold:

$$p \equiv 1, 9 \pmod{40}, \quad q \equiv \pm 2 \pmod 5,$$
$$m_q \mid p - 1,$$
$$c_1^q \equiv c_2 \pmod p, \quad c_2^q \equiv c_1 \pmod p.$$

4. Algorithm

From Theorem 9, we have an algorithm which computes a solution to Grantham's problem for $n = pq$.

Input: L (the list of all prime numbers $< B_1$), PL (the list of all prime numbers $p \equiv 1, 9 \pmod{40} < B_2$)
Output: PQL=$\{pq \in$ fpsp2_2$(-5, 5) \mid p, q$ prime, $p \equiv 1, 9 \pmod{40}$, $p < B_2, q < B_1\}$

```
for p ∈ PL do
    c_1, c_2 ← (the roots of f(x) ≡ 0 (mod p))
    m_p ← (the order of c_1 ∈ F_p^×)
    Compute t for c_1^t ≡ c_2 (mod p) and c_2^t ≡ c_1 (mod p)
    if t exists, then
        for q ∈ L do
            if q ≡ t (mod m_p) and q ≡ ±2 (mod 5) then
                QL ← QL ∪ {q}
        for q ∈ QL do
            m_q ← (the order of x ∈ F_q[x]/f(x))
            if m_q | p − 1 then
                PQL ← PQL ∪ {pq}
return PQL
```

5. Experimental Results

In our proposed algorithm, for one fixed p, the parameter t is used to find prime numbers q satisfying Theorem 9, namely, we try to compute t such that $c_1^t \equiv c_2 \pmod p$, $c_2^t \equiv c_1 \pmod p$, and $q \equiv t \pmod{m_p}$. Since $c_1^{t^2} \equiv c_1 \pmod p$, m_p is a factor of $t^2 - 1$. But, m_p does not divide $t-1$, because $f(x)$ does not have any multiple roots over $\mathbb{Z}/p\mathbb{Z}$, and so $c_1 \not\equiv c_2 \equiv c_1^t \pmod p$. Thus, the order of t in $(\mathbb{Z}/m_p\mathbb{Z})^\times$ is equal to 2. Therefore, by the approach explained in [1], which uses Chinese remainder theorem and elements of order 2 in $(\mathbb{Z}/r^{e_r}\mathbb{Z})^\times$ where r is a prime factor of m_p and e_r is the largest integer such that $r^{e_r} \mid m_p$, we can easily compute t if the prime factorization of m_p is known. To compute all prime factors of m_p for a given p in our experiments, we factorize $p-1$ by using the trial division algorithm. In a similar way, we try to compute m_q by factoring $q^2 - 1$, however, we need not to compute it in our experiments, due to the following reason.

We found that there exist three odd prime numbers $p \equiv 1, 9 \pmod{40}$ such that there exists t satisfying $c_1^t \equiv c_2$, $c_2^t \equiv c_1 \pmod p$ in the algorithm. The only prime numbers $p < 10^{11}$ that are potential candidates are $521, 221401$, and 1644512641. The corresponding triples of (p, t, m_p) are $(521, 181, 260)$, $(221401, 17549, 36900)$, and $(1644512641, 152977919, 822256320)$. In all cases, $t \equiv \pm 1 \pmod 5$ and $5 \mid m_p$, so $q \equiv t \equiv \pm 1 \pmod 5$. This contradicts $q \equiv \pm 2 \pmod 5$. Thus, prime numbers q such that $pq \in$ fpsp2_2$(-5, 5)$, with these three p's do not exist.

We implemented the proposed algorithm on Risa/Asir. The computer environment for our experiments is as follows:

- CPU: Intel(R)Xeon(R)CPU E5-2620 v4, 2.10GHz,
- Memory: 256GB,
- OS: Windows10 Pro.

The computation of the list of all prime numbers $< 10^{11}$ requires about 190 hours, and it takes about 707 hours to perform the proposed algorithm. The total running time is about 897 hours (37 days).

6. Conclusion

From our experiment, we found that there exist three odd prime numbers $p \equiv 1, 9 \pmod{40}$ such that there exists t satisfying $c_1^t \equiv c_2$, $c_2^t \equiv c_1 \pmod{p}$ in the algorithm, where $x^2 + 5x + 5 \equiv (x - c_1)(x - c_2) \pmod{p}$.

However, there is no element $n = pq \in \mathrm{fpsp2\_2}(-5, 5)$, such that p, q are prime numbers, $p \equiv 1, 9 \pmod{40}$, and $p < 10^{11}$.

The future tasks are to expand the search range and to narrow down the conditions for prime factors of elements of $\mathrm{fpsp2\_2}(-5, 5)$. If we can prove $t \equiv \pm 1 \pmod{5}$ and $5 \mid m_p$ for prime numbers that are candidates for p, then we can prove that no composite numbers exist in $\mathrm{fpsp2\_2}(-5, 5)$.

Acknowledgments

The authors would like to thank the anonymous reviewer for his/her valuable comments. This work was partially supported by consigned research fund from NTT Secure Platform Laboratories.

References

[1] N. Shinohara, Inefficacious conditions of the Frobenius primality test and Grantham's problem, IEICE Trans. Fundamentals, **E91-A** (2008), 3325–3334.

[2] R. Crandall and C. Pomerance, Prime Numbers: A Computational Perspective, Springer, New York, 2001.

[3] J. Grantham, Frobenius pseudoprimes, Math. Comp., **70** (2001), 873–891.