Notes on Number Theory and Discrete Mathematics
ISSN 1310–5132
Vol. 20, 2014, No. 4, 11–20

Frobenius pseudoprimes and a cubic primality test

Catherine A. Buell[1] **and Eric W. Kimball**[2]

[1] Department of Mathematics, Fitchburg State University
160 Pearl Street, Fitchburg, MA, 01420, USA
e-mail: cbuell1@fitchburgstate.edu

[2] Department of Mathematics, Bates College
3 Andrews Rd., Lewiston, ME, 04240, USA
e-mail: ericwkimball@gmail.com

Abstract: An integer, n, is called a Frobenius probable prime with respect to a polynomial when it passes the Frobenius probable prime test. Composite integers that are Frobenius probable primes are called Frobenius pseudoprimes. Jon Grantham developed and analyzed a Frobenius probable prime test with quadratic polynomials. Using the Chinese Remainder Theorem and Frobenius automorphisms, we were able to extend Grantham's results to some cubic polynomials. This case is computationally similar but more efficient than the quadratic case.

Keywords: Frobenius, Pseudoprimes, Cubic, Number fields, Primality.
AMS Classification: 11Y11.

1 Introduction

Fermat's Little Theorem is a beloved theorem found in numerous abstract algebra and number theory textbooks. It states, for p an odd prime and (a, p)= 1, $a^{p-1} \equiv 1 \bmod p$.

Fermat's Little Theorem holds for all primes; however, there are some composites that pass this test with a particular base, a. These are called Fermat pseudoprimes.

Definition 1.1. A Fermat pseudoprime is a composite n for which $a^{n-1} \equiv 1 \bmod n$ for some base a and (a, n) = 1.

The term pseudoprime is typically used to refer to Fermat pseudoprime.

Example 1.2. Consider $n = 341$ and $a = 2$.

$$(341, 2) = 1 \text{ and } 2^{340} \equiv 1 \bmod 341$$

Since $341 = 11 \cdot 31$, 341 is clearly composite, then 341 is a Fermat pseudoprime to the base 2.

Passing Fermat's "Test" declared a number a probable prime. We will discuss a different primality test, where integers that pass this test are called Frobenius probable primes. This test, done with respect to polynomials, relies on distinct degree factorization and other properties of rings and fields. Any integer that passes this test with respect to a polynomial is a Frobenius probable prime with respect to that polynomial.

In Section 2, we discuss distinct degree factorization and the Frobenius probable prime test. Section 3 introduces a quadratic test for Frobenius probable primes, as well as the cubic extension of the test. Finally, in Section 4 we discuss the application of these tests to the Gaussian integers, as well as rings of integers over other number fields.

We will be using $\mathbb{Z}_p$ to denote $\mathbb{Z}$ mod $p\mathbb{Z}$ and $\mathbb{Z}_p[x]$ to denote polynomials with coefficients in $\mathbb{Z}$ mod $p\mathbb{Z}$.

2 Introduction to Frobenius pseudoprimes

The foundation of the Frobenius probable prime test is distinct degree factorization. A polynomial in $\mathbb{Z}_p[x]$ for some prime p can be factored using distinct degree factorization, where we can easily count the number of irreducible polynomials of a particular degree.

2.1 Distinct degree factorization

We can factor a polynomial $f(x)$ of degree d in $\mathbb{Z}_p[x]$ as the product of $F_i(x)$ where each $F_i(x)$ is the product of the irreducible polynomials of degree i dividing $f(x)$.

Let $f_0(x) = f(x)$. For $1 \leq i \leq d$,

$$F_i(x) = \text{gcd}(x^{p^i} - x, f_{i-1}(x)) \text{ in } \mathbb{Z}_p[x]$$

$$f_i(x) = \frac{f_{i-1}(x)}{F_i(x)}.$$

So, $f(x) = F_1(x)F_2(x)\ldots F_d(x)$.

This technique factors polynomials into irreducible polynomials of different degrees. For example, $F_1(x)$ is the product of irreducible factors of degree 1. The construction of $F_i(x)$ uses $x^{p^i} - x$ because this polynomial product of all irreducible polynomials of degree dividing i in $\mathbb{Z}_p[x]$. For example,

$$x^{3^1} - x = x(x + 1)(x + 2) \text{ in } \mathbb{Z}_3[x].$$

Also,

$$x^{3^2} - x = x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2) \text{ in } \mathbb{Z}_3[x].$$

Finally, $f_i(x)$ removes the irreducible factors of lesser degree before proceeding on to $F_{i+1}(x)$.

Example 2.1. Let $f(x) = x^4 + 3x^3 + 3x^2 + 3x + 2$ and $p = 3$.

Since we are in $\mathbb{Z}_3[x]$, $x^4 + 3x^3 + 3x^2 + 3x + 2 \equiv x^4 + 2$.

$$\begin{aligned}
\text{Step 1}: (i=1): \quad & F_1(x) = \gcd(x^3 - x, x^4+2) = (x+1)(x+2) \\
& f_1(x) = \tfrac{x^4+2}{(x+1)(x+2)} = x^2+1 \\
\text{Step 2}: (i=2): \quad & F_2(x) = \gcd(x^{3^2} - x, x^2+1) = x^2+1 \\
& f_2(x) = \tfrac{(x^2+1)}{(x^2+1)} = 1 \\
\text{Step 3}: (i=3): \quad & F_3(x) = \gcd(x^{3^3} - x, 1) = 1 \\
& f_3(x) = \tfrac{1}{1} = 1 \\
\text{Step 4}: (i=4): \quad & F_4(x) = \gcd(x^{3^4} - x, 1) = 1 \\
& f_4(x) = \tfrac{1}{1} = 1
\end{aligned}$$

For $f(x) = x^4 + 2$ in $\mathbb{Z}_3[x]$ and $p = 3$,

$$\begin{aligned}
F_1(x) &= (x+1)(x+2) & f_1(x) &= (x^2+1) \\
F_2(x) &= (x^2+1) & f_2(x) &= 1 \\
F_3(x) &= 1 & f_3(x) &= 1 \\
F_4(x) &= 1 & f_4(x) &= 1
\end{aligned}$$

In summary,

$$\begin{aligned}
f(x) &= F_1(x)F_2(x)F_3(x)F_4(x) \\
&= (x+1)(x+2)(x^2+1).
\end{aligned}$$

From distinct degree factorization, we get three statements that hold for all suitable polynomials and p.

Theorem 2.2. *[1] Let p be an odd prime, and let $f(x)$ be a monic polynomial in $\mathbb{Z}_p[x]$ of degree d with discriminant Δ. Assume $p \nmid f(0)\Delta$.*

1. *We have $f_d(x) = 1$, and for each i, $1 \le i \le d, i \mid \deg(F_i(x))$.*
2. *For $2 \le i \le d$, $F_i(x) \mid F_i(x^p)$.*
3. *Let $S = \Sigma_{2|i} \dfrac{\deg(F_i(x))}{i}$. Then $(-1)^S = \left(\frac{\Delta}{p}\right)$.*

Like Fermat's Little Theorem, this theorem will hold for all primes. The first statement holds because we are in $\mathbb{Z}_p[x]$, which is a Euclidean domain so all the $F_i(x)$ exist. The second statement holds because the coefficients are in the field $\mathbb{Z}_p$ which has characteristic p. The third statement defines S where S counts the number of even degree irreducible factors. This statement holds because of the Frobenius automorphism on $\mathbb{Z}_p$.

We expect this theorem to hold for our example of distinct degree factorization because $p = 3$, a prime.

Example 2.3. $f(x) = x^4 + 2, p = 3$

$$\begin{aligned} F_1(x) &= (x+1)(x+2) & \qquad f_1(x) &= (x^2+1) \\ F_2(x) &= (x^2+1) & f_2(x) &= 1 \\ F_3(x) &= 1 & f_3(x) &= 1 \\ F_4(x) &= 1 & f_4(x) &= 1 \end{aligned}$$

1. We have $f_4(x) = 1$, and for each i, $1 \leq i \leq 4, i \mid$ deg$(F_i(x))$.
2. For $2 \leq i \leq 4$, $F_i(x) \mid F_i(x^3)$.
3. $S = \Sigma_{2|i} \dfrac{\text{deg}(F_i(x))}{i} = (-1)^1 = -1$, and $\left(\frac{2048}{3}\right) = -1$.

2.2 Frobenius probable prime test

We shall now introduce Grantham's three-step test called the Frobenius probable prime test. This test is a generalization of Theorem 2.2 for any integer n. The test is passed by all primes and some composites too. These that pass are called Frobenius probable primes. If at any point a step is failed in this test, then we can call n a composite.

1. **Factorization Step:** First, if $f_d(x) \neq 1$, then n is composite. Next, let $f_0(x) = f(x)$ mod n. For $1 \leq i \leq d$, let $F_i(x) =$ gcmd$(x^{n^i} - x, f_{i-1}(x))$ and $f_i(x) = \dfrac{f_{i-1}(x)}{F_i(x)}$. If any of the gcmds do not exist, then n is composite.
2. **Frobenius Step:** Determine whether or not $F_i(x^n)$ is divisible by $F_i(x)$ for $2 \leq i \leq d$. If $F_i(x)$ does not divide $F_i(x^n)$ for some i, then n is composite.
3. **Jacobi Step:** Let $S = \Sigma_{2|i} \dfrac{\text{deg}(F_i(x))}{i}$. If $(-1)^S \neq \left(\frac{\Delta}{n}\right)$, then n is composite.

Since we are now in $\mathbb{Z}_n[x]$ where n is not necessarily prime, then any of these steps could be failed. The Factorization step, which is essentially distinct degree factorization, requires the Euclidean algorithm to determine $F_i(x)$ and $f_i(x)$. Since we are not necessarily in a Euclidean domain, then the Euclidean algorithm could fail. The Frobenius step is the same as the second step of Theorem 2.2 and it could be failed because we may not be in a field with characteristic n. Finally, the Jacobi step will be failed if $(-1)^S \neq \left(\frac{\Delta}{n}\right)$.

Every odd prime, p, is a Frobenius probable prime with respect to any suitable monic, square-free polynomial, $f(x)$.

Definition 2.4. A *Frobenius pseudoprime* with respect to a monic polynomial $f(x)$ is a composite which is a Frobenius probable prime with respect to $f(x)$.

It is interesting to note that when $f(x)$ is linear, then this is equivalent to Fermat's Little Theorem. When n is a Frobenius pseudoprime with respect to $f(x)$ where $f(x) = x - a$, then n is a Fermat pseudoprime to the base a. Therefore, since 341 is a Fermat pseudoprime to the base 2, then 341 is a Frobenius pseudoprime with respect to $x - 2$.

3 Theory of Frobenius pseudoprimes

The Frobenius probable prime test is computationally heavy. So, Grantham created other tests that determine Frobenius probable primes with respect to quadratic polynomials, one of which is discussed and another can be found in [2].

3.1 Quadratic and cubic test

Theorem 3.1. *[1] Let $f(x) = x^2 - bx - c$. Let $\Delta = b^2 + 4c$. Let n be an integer with $(n, 2f(0)\Delta) = 1$.*

1. *If $\left(\frac{\Delta}{n}\right) = 1$ and $x^n \equiv x \bmod (n, f(x))$, then n is a Frobenius probable prime with respect to $f(x)$.*
2. *If $\left(\frac{\Delta}{n}\right) = -1$ and $x^n \equiv b - x \bmod (n, f(x))$, then n is a Frobenius probable prime with respect to $f(x)$.*

We decided to expand on these tests by turning the quadratic polynomial into a cubic polynomial by multiplying the quadratic by some $(x - a)$. The resulting test adds no real computational cost to the original quadratic test; however, there are fewer composites that will be deemed probable primes in the cubic test.

Theorem 3.2. *Let $g(x) = (x - a)(x^2 - bx - c)$, $\Delta = (a^2 - ab - c)(b^2 + 4c)$, $2a = b$, and let n be an integer with $(n, 2g(0)\Delta) = 1$.*

1. *If $\left(\frac{\Delta}{n}\right) = 1$ and $x^n \equiv x \bmod (n, g(x))$, then n is a Frobenius probable prime with respect to $g(x)$.*
2. *If $\left(\frac{\Delta}{n}\right) = -1$ and $x^n \equiv b - x \bmod (n, g(x))$, then n is a Frobenius probable prime with respect to $g(x)$.*

In the first case, where $\left(\frac{\Delta}{n}\right) = 1$, it turns out that any appropriate a will hold. However, in the second case where $\left(\frac{\Delta}{n}\right) = -1$, $2a = b$ is required.

We have the stipulation that $2a = b$ in the case where $\left(\frac{\Delta}{n}\right) = -1$ because this simplifies to $x^n \equiv b - x \bmod (x - a)(x^2 - bx - c)$. It is not necessary to make this choice; however, as seen in Lemma 3.4, the alternate equivalent expression is complicated for general a.

Before we can examine this proof, we must show that the Jacobi symbol of the discriminant of the cubic and n is equal to the Jacobi symbol of the discriminant of the quadratic and n. We will let Δ_c (Δ_q) be the discriminant of the cubic (quadratic).

Lemma 3.3. *For the cubic polynomial $(x - a)(x^2 - bx - c)$ and the quadratic polynomial $(x^2 - bx - c)$, $\left(\dfrac{\Delta_c}{n}\right) = \left(\dfrac{\Delta_q}{n}\right)$.*

Proof. The discriminant of $(x-a)(x^2-bx-c)$ is $(a^2-ab-c)^2(b^2+4c)$ while the discriminant of x^2-bx-c is b^2+4c. Thus, the addition of the $x-a$ term changes the discriminant by a factor of $(a^2-ab-c)^2$. By the properties of the Jacobi symbol,

$$\begin{aligned}\left(\frac{\Delta_c}{n}\right) &= \left(\frac{(a^2-ab-c)^2}{n}\right)\left(\frac{b^2+4c}{n}\right)\\ &= \left(\frac{a^2-ab-c}{n}\right)\left(\frac{a^2-ab-c}{n}\right)\left(\frac{b^2+4c}{n}\right)\\ &= \left(\frac{a^2-ab-c}{n}\right)^2\left(\frac{b^2+4c}{n}\right).\end{aligned}$$

Suppose $\left(\frac{a^2-ab-c}{n}\right) = \pm 1$, then $\left(\frac{a^2-ab-c}{n}\right)^2 = 1$. So,

$$\begin{aligned}\left(\frac{\Delta_c}{n}\right) &= \left(\frac{(a^2-ab-c)^2}{n}\right)\left(\frac{b^2+4c}{n}\right)\\ &= \left(\frac{b^2+4c}{n}\right)\\ &= \left(\frac{\Delta_q}{n}\right).\end{aligned}$$

Note $\left(\frac{a^2-ab-c}{n}\right) \neq 0$. By the definition of the Jacobi symbol, $\left(\frac{a^2-ab-c}{n}\right) \neq 0$ when $\gcd(n, a^2-ab-c) = 1$. Since we require that $\gcd(n, 2g(0)\Delta_c) = 1$, then

$$\gcd(n, 2g(0)(a^2-ab-c)^2(b^2+4c)) = 1.$$

So $\gcd(n, a^2-ab-c) = 1$ as required. □

Lemma 3.4. *For $g(x) = (x-a)(x^2-bx-c), n \in \mathbb{Z}$ and Δ the discriminant of $g(x)$, if $\left(\frac{\Delta}{n}\right) = -1$ and $2a = b$, then $x^n \equiv b - x$ mod $(n, g(x))$*

Proof. First, we want $x^n \equiv x \bmod (x-a)$ and $x^n \equiv b - x \bmod (x^2-bx-c)$. This will give us the required roots to build our equivalence.

Then, by the Chinese Remainder Theorem, we determine $f(x)$ and $g(x)$ such that

$$f(x)(x^2-bx-c) \equiv x \bmod (x-a)$$

and

$$g(x)(x-a) \equiv b - x \bmod (x^2-bx-c).$$

Then,

$$x^n \equiv f(x)(x^2-bx-c) + g(x)(x-a) \bmod (x-a)(x^2-bx-c).$$

Through some algebra, we find that

$$f(x) = \frac{a}{a^2-ab-c}$$

and

$$g(x) = \frac{x(-b+a)}{a^2-ab-c} + \frac{(-b+a)c}{(a^2-ab-c)a} - \frac{b}{a}.$$

By substitution,

$$\begin{aligned} x^n &\equiv f(x)(x^2-bx-c) + g(x)(x-a) \text{ mod } (x-a)(x^2-bx-c) \\ &\equiv \frac{2ax^2 - abx - 2ac - bx^2 - xa^2 + cx + a^2b + b^2x - b^2a}{a^2-ab-c} \qquad (1) \end{aligned}$$

Let $2a = b$.

$$\begin{aligned} x^n &\equiv \left(\frac{1}{-a^2-c}\right)\left(2a(-a^2-c) - (-a^2-c)x - (0)x^2\right) \\ &\equiv 2a - x = b - x \text{ mod } (x-a)(x^2-bx-c) \end{aligned}$$

□

Without the $2a = b$ stipulation, then x^n must be equivalent to the fraction from line (1) when $\left(\frac{\Delta}{n}\right) = -1$.

To prove Theorem 3.2, we need to prove both when $\left(\frac{\Delta}{n}\right) = 1$ and when $\left(\frac{\Delta}{n}\right) = -1$. Note that when implementing the Frobenius probable prime test for a quadratic, we use $F_i(x)$ and $f_i(x)$ whereas when implementing the test for a cubic, we use $G_i(x)$ and $g_i(x)$.

Proof. Case 1: $\left(\frac{\Delta}{n}\right) = 1$.

Assume for n with $(n, 2g(0)\Delta) = 1$ that $\left(\frac{\Delta}{n}\right) = 1$ and $x^n \equiv x \text{ mod } (n, g(x))$. We want to show that n is a Frobenius probable prime with respect to $g(x)$.

1. **Factorization Step:** Since $x^n \equiv x \text{ mod } (n, g(x))$, then $x^n - x \equiv 0 \text{ mod } (n, g(x))$. Thus, $G_1(x) = g(x)$ since $G_1(x) = \text{gcmd}(x^n - x, g(x))$ in $\mathbb{Z}_n[x]$. This means that $g_1(x) = G_2(x) = g_2(x) = G_3(x) = g_3(x) = 1$. So, we have passed the Factorization step.

2. **Frobenius Step:** Since $G_2(x) = G_3(x) = 1$, then we have passed the Frobenius step.

3. **Jacobi Step:** Also, since $G_2(x) = 1$, then the degree of $G_2(x) = 0$. Therefore, $S = 0$. Thus, $(-1)^S = 1 = \left(\frac{\Delta}{n}\right)$. So, we have passed the Jacobi step.

Therefore, n, is a Frobenius probable prime with respect to $g(x)$ if $\left(\frac{\Delta}{n}\right) = 1$ and $x^n \equiv x \text{ mod } (n, g(x))$.

Case 2: $\left(\frac{\Delta}{n}\right) = -1$ and $2a = b$.

Assume for n with $(n, 2g(0)\Delta) = 1$ that $\left(\dfrac{\Delta}{n}\right) = -1$, $2a = b$, and $x^n \equiv b - x \bmod (n, g(x))$. We want to show that n is a Frobenius probable prime with respect to $g(x)$.

1. **Factorization Step:** Since $x^n \equiv b - x \bmod (n, g(x))$, then $x^n - x \equiv b - 2x \bmod (n, g(x))$. Let $b = 2a$, then

   $$x^n - x \equiv b - 2x \equiv 2a - 2x \equiv 2(a - x) \bmod (n, g(x)).$$

   This means that $x^n - x \equiv 2(a - x) \bmod (n, g(x))$. Thus,

   $$G_1(x) = \text{gcmd}(2(a - x), (x - a)(x^2 - bx - c)) = x - a.$$

   Therefore, $G_1(x) = x - a$, which means that $g_1(x) = x^2 - bx - c$. So,

   $$G_2(x) = \text{gcmd}(x^{n^2} - x, x^2 - bx - c).$$

   Since $x^n \equiv b - x \bmod (n, g(x))$, then $x^2 - bx - c \mid x^{n^2} - x$. Thus, $G_2(x) = x^2 - bx - c$, which means that $g_2(x) = G_3(x) = g_3(x) = 1$. Therefore, we have passed the Factorization step.

2. **Frobenius Step:** To pass the Frobenius step, $G_2(x)$ must divide $G_2(x^n)$. Since $G_2(x) = x^2 - bx - c = f(x)$, then we just need to show that $f(x) \mid f(x^n)$. We know that $x^n \equiv b - x \bmod (n, g(x))$, so $f(x^n) \equiv f(b - x) \bmod (n, f(x))$. Also,

   $$f(b - x) = (b - x)^2 - b(b - x) - c = x^2 - bx - c = f(x).$$

   Thus, $f(x) \mid f(x^n)$ which means that $G_2(x) \mid G_2(x^n)$. So, we have passed the Frobenius step.

3. **Jacobi Step:** Since the degree of $G_2(x)$ is 2, then $S = 1$. Thus, the Jacobi step is passed since $(-1)^S = \left(\dfrac{\Delta}{n}\right) = -1$.

Therefore, n, is a Frobenius probable prime with respect to $g(x)$ if $\left(\dfrac{\Delta}{n}\right) = -1$, $2a = b$, and $x^n \equiv b - x \bmod (n, g(x))$. □

3.2 Strength of cubic test

The cubic theorem relates to the quadratic theorem in two ways;

1. If n is a Frobenius probable prime with respect to $(x - a)(x^2 - bx - c)$, then it is a Frobenius probable prime with respect to $x^2 - bx - c$.

2. A Frobenius probable prime with respect to $x^2 - bx - c$ is not always a Frobenius probable prime with respect to $(x - a)(x^2 - bx - c)$.

This means that the cubic test does not add any more Frobenius pseudoprimes to the quadratic test for the related polynomial. Also, the cubic test removes some Frobenius pseudoprimes from the quadratic test for the related polynomial.

Example 3.5. Let $n = 5777$ and $f(x) = x^2 - x - 1$. Since, $\Delta_q = 5$, then we have $\left(\dfrac{5}{5777}\right) = -1$. So, we want $x^n \equiv b - x \bmod (n, f(x))$. In fact,

$$x^{5777} \equiv 1 - x \text{ mod } (5777, f(x)).$$

So, 5777 is a Frobenius probable prime with respect to $f(x)$. Since 5777 is composite, then it is a Frobenius pseudoprime with respect to $f(x)$.

To test this with the cubic test, let $a = 2889$ because $2 \cdot 2889 \equiv 1 \bmod 5777$. Thus, we have $g(x) = (x - 2889)(x^2 - x - 1)$ where $\Delta_c = 348064204258805$. So, we do indeed get $\left(\dfrac{348064204258805}{5777}\right) = -1$. However,

$$x^{5777} \not\equiv 1 - x \text{ mod } (5777, g(x)).$$

So, 5777 is not a Frobenius probable prime with respect to $g(x)$.

4 Gaussian integers and Further work

We considered the idea of a Frobenius pseudoprime in rings of integers over number fields. In particular, we developed a Frobenius probable prime test in the Gaussian integers.

4.1 Gaussian Frobenius probable primes

The Gaussian integers are a Euclidean domain, which means we are again working in a principal ideal domain. Let $\alpha \in \mathbb{Z}[i]$ and $N = |\alpha|$. If α is prime, then $\mathbb{Z}[i]/(\alpha)$ is a field and isomorphic to $\mathbb{F}_N$. Since α is prime, N is either a prime p or a square of some prime p. First, let $\alpha \in \mathbb{Z}[i]$ and $f(x)$ a monic polynomial in $(\mathbb{Z}[i]/(\alpha))[x]$ of degree d with discriminant Δ. Assume $\alpha \nmid f(0)\Delta$. Since $\mathbb{Z}[i]/(\alpha)$ is a field, $(\mathbb{Z}[i]/(\alpha))[x]$ is a Euclidean domain, which is required in the implementation of the algorithm.

1. **Factorization Step:** First, if $f_d(x) \neq 1$, then α is composite. Next, let $f_0(x) = f(x) \bmod \alpha$. For $1 \leq i \leq d$, let $F_i(x) = \text{gcmd}(x^{N^i} - x, f_{i-1}(x))$ and $f_i(x) = \dfrac{f_{i-1}(x)}{F_i(x)}$. If any of the gcmds do not exist, then α is composite.

2. **Frobenius Step:** Determine whether or not $F_i(x^N)$ is divisible by $F_i(x)$ for $2 \leq i \leq d$. If $F_i(x)$ does not divide $F_i(x^N)$ for some i, then α is composite.

3. **Jacobi Step:** Let $S = \Sigma_{2|i} \dfrac{\deg(F_i(x))}{i}$. If $(-1)^S \neq \left[\frac{\Delta}{\alpha}\right]_2$, then α is composite.

If α is prime, then the Factorization step holds because $(\mathbb{Z}[i]/(\alpha))$ is a field, so $(\mathbb{Z}[i]/(\alpha))[x]$ is a Euclidean domain. The Frobenius step holds from the prime characteristic of the field. Finally, the Jacobi step holds from the Frobenius automorphism on such a field. Note the notation $\left[\frac{a}{b}\right]_2$ is the symbol for the quadratic reciprocity on the Gaussian integers which is analogous to the Jacobi symbol in the integers.

4.2 Open questions

The accuracy of the Frobenius probable prime test for the Gaussian integers remains to be determined, as is the best programming tools to implement it.

The Gaussian integers are not the only ring that we can extend these results too. These results could be extended to rings of integers over other number fields, in particularly $\mathbb{Z}[\sqrt{d}]$, when $\mathbb{Z}[\sqrt{d}]$ is a principal ideal domain.

Acknowledgements

Thank you to Ben Weiss and Jon Grantham for their input, comments, and support.

References

[1] Grantham, J. Frobenius Pseudoprimes, *Mathematics of Computation*, Vol. 234, 2000, 873–891.

[2] Grantham, J. A Probable Prime Test With High Confidence, *Journal of Number Theory*, Vol. 72, 1998, 32–47.