STUDYING THE EFFICIENCY OF THE FROBENIUS PRIMALITY TEST

HIVA GHEISARI
Master of Science, University of Tehran, Iran, 2020

A thesis submitted
in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in

MATHEMATICS

Department of Mathematics and Computer Science
University of Lethbridge
LETHBRIDGE, ALBERTA, CANADA

© Hiva Gheisari, 2024

STUDYING THE EFFICIENCY OF THE FROBENIUS PRIMALITY TEST

HIVA GHEISARI

Date of Defence: April 26, 2024

Dr. Andrew Fiori	Associate Professor	Ph.D.
Dr. Habiba Kadiri	Associate Professor	Ph.D.
Thesis Supervisors		
Dr. Joy Morris	Professor	Ph.D.
Thesis Examination Committee Member		
Dr. Nathan Ng	Professor	Ph.D.
Thesis Examination Committee Member		
Dr. Wendy Osborn	Associate Professor	Ph.D.
Chair, Thesis Examination Committee		

Dedication

To my beloved husband, Saeed,

Your unwavering love, patience, and encouragement have been my greatest source of strength throughout this journey. Thank you for standing by my side, for believing in me even when I doubted myself, and for the countless sacrifices you made to support me. This achievement is as much yours as it is mine. I am forever grateful for your presence in my life.

Acknowledgments

I extend my deepest gratitude to my supervisors, Professor Andrew Fiori and Professor Habiba Kadiri, for their unwavering support and insightful critiques throughout my research journey. In particular, I am profoundly thankful to Andrew, whose deep commitment to academic excellence and meticulous attention to detail left an indelible mark on this dissertation. His generous investment of time, thoughtful mentorship, and steadfast mental support sustained me throughout my academic journey. His ability to consistently challenge me to think more deeply and critically has been instrumental in shaping my development as a scholar.

I am also deeply appreciative of the members of my thesis committee, Dr. Joy Morris and Dr. Nathan Ng, for their invaluable constructive feedback and essential suggestions. Their expertise and thoughtful perspectives greatly enhanced the quality of my work, pushing me to achieve a higher standard of scholarship.

Moreover, I would like to express my sincere appreciation to the chair of my committee, Dr. Wendy Osborn, as well as the faculty and staff of the Department of Mathematics at the University of Lethbridge. Their combined expertise, unwavering support, and invaluable resources have been instrumental in shaping my academic experience. The supportive environment they fostered not only enabled me to concentrate on my research but also contributed to my personal and professional growth in profound ways.

Finally, I am grateful for the encouragement and sense of community fostered within the department, which created a space for growth, collaboration, and discovery.

Abstract

In mathematics, especially number theory, prime numbers are essential concepts. Prime numbers are used in cryptography as one application.

Finding large prime numbers is crucial for cryptographic protocols; to do this, we must be able to tell whether a given number is prime or not. To test whether a number is a prime number, we require a computationally efficient primality testing algorithm. The primary objective of my research is to evaluate how well the tests work. Especially, in my research our main focus is on Grantham's primality test. Grantham's test is probabilistic and fast, but it comes with the risk of false positives. To determine how 'good' a test is, one must be aware of the possibility of false positives because in our development, deterministic tests are slower than false positive ones.

In this thesis, we will explain the definitions of 'probable prime numbers', such as 'Frobenius pseudoprime', as given by Jon Grantham. Our research goal is to find upper and lower bounds for the number of probable prime numbers by generalizing the work of Paul Erdős and Carl Pomerance on Fermat pseudoprimes, and Jon Grantham on Frobenius pseudoprimes.

Contents

Chapter 1

Introduction And Motivation

One of the modern applications of prime numbers is in the context of cryptography. In several important cryptography protocols, it is important to find large prime numbers; to do this, we must be able to determine whether a provided number is prime or not. For further information on the role of prime numbers in cryptography, see [Dent and Mitchell, 2005, Chapter 16.2]. For this approach, we use a primality test which will determine whether or not a given number is prime. These tests do not generally give prime factorization, only stating whether the input number is prime or not. Factorization is considered a computationally difficult problem, whereas primality testing is comparatively easier, with a running time that is polynomial in the size of the input, specifically $\log(n)^k$ for some positive constant k. On the other hand, the running time for the best-known factorization algorithms is $\exp(\log(n)^{1/3}\log\log(n)^{2/3})$.

Primality tests come in two types, deterministic and probabilistic. Deterministic tests determine with absolute certainty whether a number is prime. These tests in general are much slower than probabilistic tests.

Hence, the key advantage of probabilistic tests is that they are faster, the drawback is the uncertainty of having identified a prime. Many probabilistic tests have running time of $O(\log(n))$ to determine the primality of a number of size n. In contrast, the running time of the deterministic tests conjecturally is $O((\log n)^3)$. In order to understand the time

and accuracy trade-offs, it remains to better evaluate the risk of false positives and identify probabilistic tests with lower rates of false positives. The number of false positives depends on the definitions of the probable prime.

In my thesis, the main goal is to study the efficiency of the Frobenius test as a probabilistic test. There are various types of primality test. For example, the Lucas-Lehmer test [Lehmer, 1930] and elliptic curve primality test [Morain, 1998] are deterministic primality tests. On the other hand, Rabin-Miller test [Rabin, 1980], Fermat primality test [Erdős and Pomerance, 1986], Frobenius primality test [Grantham, 2001], Miller–Rabin and Solovay–Strassen primality test [Gallier and Quaintance, 2017], and Baillie–PSW primality test [Baillie et al., 2021] are probabilistic tests.

One important definition we need here is that of **probable prime** numbers. These are numbers that satisfy certain theorems or properties typically associated with prime numbers, but they are not necessarily prime. When a composite number satisfies specific properties characteristic of prime numbers, it is called a **pseudoprime**. Different types of pseudoprimes are classified based on which properties of prime numbers they satisfy. A partial classification of pseudoprimes includes Euler pseudoprime [Pomerance et al., 1980], Lucas pseudoprime ([Baillie and Wagstaff, 1980] and [Baillie et al., 2021]), Lehmer pseudoprime [Rotkiewicz, 1982], Fermat pseudoprime [Erdős and Pomerance, 1986], Elliptic pseudoprime [Gordon and Pomerance, 1991], Frobenius pseudoprime [Grantham, 2001], Catalan pseudoprime [Aebi and Cairns, 2008], and Perrin pseudoprime [Grantham, 2010].

In [Grantham, 2001], Grantham introduced a new primality test that simultaneously refines many existing primality tests. One of the tests that Grantham generalized is Fermat primality test, which tries to identify if a given number n is prime by checking if $a^n \equiv 1 \pmod{n}$ for some pre-chosen a.

It is worth mentioning here that Erdős and Pomerance in [Erdős and Pomerance, 1986], studied the number of Fermat pseudoprimes and provided upper and lower bounds for the

number of Fermat pseudoprimes which are less than x. They proved

$$x^{-8/23} \leq \frac{1}{x^2} \sum_{\substack{n \leq x \\ n \text{ is composite}}} \left| \{a \in (\mathbb{Z}/n\mathbb{Z})^\times : a^{n-1} \equiv 1 \pmod{n}\} \right| \leq \mathcal{L}^{-1+o(1)}(x), \tag{1.1}$$

where $\mathcal{L}(x) = \exp\left(\frac{(\log x)(\log\log\log x)}{(\log\log x)}\right)$.

Roughly speaking, for a chosen at random, the probability that a composite number n, that is coprime to a, is misidentified by the base a test is between $x^{-8/23}$ and $x^{-\frac{\log\log\log x}{\log\log x}}$.

Most primality tests use auxiliary parameters, for example Fermat's test uses an integer number a and checks if $a^{n-1} \equiv 1 \pmod{n}$. In Grantham's test the auxiliary parameter is a polynomial $P(x)$ with integer coefficients. Grantham's test is alternatively called the **Frobenius primality test**. Correspondingly, composite numbers which Grantham's test misidentifies as primes will be called Frobenius pseudoprimes. We will explain the Frobenius primality test in Theorem 2.18, and we shall study the likelihood of false positives for the Grantham's test in Chapter 4.

The case of base-a Fermat pseudoprimes corresponds to Frobenius pseudoprimes for the degree one polynomial $x - a$ (see Theorem 2.28 for details). Consequently, the work of Erdős and Pomerance [Erdős and Pomerance, 1986] covers the Fermat case which in Grantham generalization would correspond to degree one Frobenius pseudoprimes where the associated polynomial has degree one. We would call it a degree one Frobenius pseudoprime.

Fiori and Shallue [Fiori and Shallue, 2020] generalized Erdős and Pomerance's work to quadratic polynomials, in which they counted the pairs $(P(x), n)$, where $P(x)$ is a quadratic polynomial with integer coefficients and n is Frobenius pseudoprime with respect to $P(x)$. We can call $P(x)$ a **liar to the integer** n. They denoted the number of quadratic liars respect with n by $L_2(n)$, and found the following upper and lower bounds for the number of quadratic liars, which is analogous to the Erdős and Pomerance bounds given in equation

(1.1).

$$x^{-\alpha^{-1}-o(1)} \leq \frac{1}{x^3} \sum_{\substack{n\leq x \\ n \text{ is composite}}} L_2(n) \leq \mathcal{L}^{-1+o(1)}(x). \tag{1.2}$$

This motivates us to consider the next case, which is **cubic Frobenius pseudoprimes**, where the polynomial $P(x)$ is of degree three. In Sections 4.3 and 4.4, we will generalize these tactics and definitions to find upper and lower bounds for the number of cubic Frobenius pseudoprimes. So if we denote the number of cubic polynomials which are liars to n by $L_3(n)$, we can prove

$$x^{-\alpha^{-1}-o(1)} \leq \frac{1}{x^4} \sum_{\substack{n\leq x \\ n \text{ is composite}}} L_3(n) \leq \mathcal{L}^{-1+o(1)}(x). \tag{1.3}$$

As with the work of Fiori-Shallue, who split liars into two types and bounded both types separately, in the cubic case there are three types of liars, and we will bound each case separately. For details see Theorem 4.36, 4.47, and 4.50 for lower bounds and Theorem 4.54, 4.57, and 4.59 for upper bounds.

Our thesis is organized as follows.

Chapter 2 presents necessary background material. In Section 2.1, the discussion centers around Erdős and Pomerance results for the Fermat primality test and in Section 2.2, we introduce Grantham's test. In Subsection 2.2.1, we will introduce the quadratic Frobenius pseudoprimes that are formulaized by [Fiori and Shallue, 2020].

In Chapter 3, we provide an alternative description of Frobenius pseudoprimes that will allow us to count them. In this description, we make a connection between the conditions in Granthams definition and a conditions on the map $x \mapsto x^n$ acting as a permutation on the roots of a polynomial $P(x)$.

Finally, in Chapter 4, we use the reinterpretation of Frobenius pseudoprimes which we found in Chapter 3 to give our main results in terms of the cycles and factorization structures

of cubic Frobenius pseudoprimes. In Section 4.1, we give formulas for the number of cubic liars for a fixed n. In Section 4.2, we provide some number theory materials as background, and in Section 4.3 and Section 4.4, we will present the lower and upper bounds for the number of cubic Frobenius pseudoprimes, respectively.

1.1 Notations

For the rest of the thesis, p denotes a prime number and both r and d are positive integers.

Definition 1.1. When we say $p^r \,||\, n$ that means $p^r \mid n$ and $p^{r+1} \nmid n$.

Theorem 1.2. *[Cox, 2011a, Theorem 11.1.4] Given any prime number p and any positive integer d, there is a finite field with p^d elements and denoted by $\mathbb{F}_{p^d}$.*

Theorem 1.3. *[Cox, 2011a, Chapter 11] Two finite fields with the same number of elements are isomorphic.*

Definition 1.4. Let $f(x)$ and $g(x)$ be real-valued functions. Then we have the following definitions

1. We write $f(x) = O(g(x))$ to mean that there exists a constant $C > 0$ such that $|\, f(x) \,| \leq Cg(x)$ for x is sufficiently large. Alternatively, we write $f(x) \ll g(x)$. Also, we write $f(x) \gg g(x)$ to mean $g(x) = O(f(x))$. This notation is known as the Vinogradov notation.

2. We write $f(x) = o(g(x))$ to mean $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$ where $g(x) \neq 0$ for x is sufficiently large.

3. We write $f(x) \asymp g(x)$ to mean $g(x) \ll f(x) \ll g(x)$. It is called the order of magnitude estimate.

Definition 1.5. Let $f(x)$ be a real valued function. Then we write $f(x) = o(1)$ to mean $\lim_{x\to\infty} f(x) = 0$ for x sufficiently large.

Remark 1. $f(x) \asymp g(x)$ means that there exists constants $C_1, C_2 > 0$ s.t. for x sufficiently large,

$$C_1 g(x) <\mid f(x) \mid< C_2 g(x).$$

Definition 1.6. Let n be an positive integer. Then $\pi(n)$ is the prime counting function that computes the number of primes less than n.

Theorem 1.7. *Let n be positive integer and $\pi(n)$ be the prime counting function, then we have*

$$\pi(n) \asymp \frac{n}{\log n}.$$

Remark 2. When we say $f(x) = x^{1-o(1)}$ it means

$$\log(f(x)) = (1-o(1))\log x, \text{ or equivalently } \frac{\log(f(x)) - \log x}{\log x} = o(1).$$

So when x goes to infinity, then $\frac{\log(f(x))-\log x}{\log x}$ goes to zero.

Definition 1.8. Given fields F and L with $F \subseteq L$, we say an element a of L is an **algebraic element over** F, or just **algebraic over** F, if there exists some nonzero polynomial $f(x) \in F[x]$ with coefficients in F such that $f(a) = 0$.

Definition 1.9. A field $\overline{F}$ is called an **algebraic closure of** F if $F \subset \overline{F}$ and $\overline{F}$ contains all the elements that are algebraic over F.

Definition 1.10. [Cox, 2011b] Let $f(x)$ be a monic polynomial of degree d over a field F with no repeated roots. Let $\alpha_1, \ldots, \alpha_d \in \overline{F}$ be the roots of $f(x)$. Then the **discriminant of**

the polynomial $f(x)$ is

$$\Delta_f = \prod_{1 \le i < j \le d} (\alpha_i - \alpha_j)^2.$$

Definition 1.11. [Stein, 2005] Let p be an odd prime and let a be an integer. Set

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } \gcd(a,p) \neq 1, \\ +1 & \text{if } a \text{ is a quadratic residue, and} \\ -1 & \text{if } a \text{ is a quadratic non-residue.} \end{cases}$$

Definition 1.12. [Stein, 2005] The **Jacobi symbol** is an extension of the Legendre symbol. More precisely for any integer a and any positive odd integer n, the Jacobi symbol $\left(\frac{a}{n}\right)$ is defined to be the product of the Legendre symbols corresponding to the prime factors of n :

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k},$$

where

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

is the prime factorization of n.

Definition 1.13. Given $x > 0$ we shall define

$$\mathcal{L}(x) = \exp\left(\frac{\log x \log_3 x}{\log_2 x}\right)$$

where $\log_2 x = \log\log x, \log_3 x = \log\log\log x$. Here, and throughout the thesis, log is the natural logarithm.

Chapter 2

Background

We break down this Chapter into two Sections. The first part is about Fermat pseudoprimes and some results about counting them. Also, we will introduce Carmichael numbers as an example of false positive for Fermat primality test [Erdős and Pomerance, 1986], [Erdős and Renyi, 1956].

The second Section centers on Grantham's Primality test and Frobenius pseudoprimes [Grantham, 2001]. We will explain there several lemmas and theorems from Fiori and Shallue's article [Fiori and Shallue, 2020] on quadratic Frobenius pseudoprimes. These are the results our thesis ultimately generalizes.

2.1 Fermat pseudoprime

As we mentioned in Chapter 1, there are plenty of probabilistic primality tests. Here we introduce the Fermat primality test that was established by Erdős. Also, we will discuss the result of Erdős and Pomerance which showed that there exist infinitely many composite numbers that are false positives for the Fermat primality test [Erdős and Pomerance, 1986]. The Fermat primality test will be based on Fermat's Little Theorem.

Theorem 2.1 (Fermat's Little Theorem)**.** *If p is a prime and a is any integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.*

Fermat pseudoprimes are discussed in many references. The definitions in this sec-

tion can be found in many sources, for example see [Erdős and Pomerance, 1986, p. 259], [Grantham, 2001, p. 875], and [Stein, 2005, Theorem 2.4.1].

Definition 2.2. A **Fermat pseudoprime** to the pre-chosen base integer $a > 1$ is a composite number n with $(a,n) = 1$ such that $a^{n-1} \equiv 1 \pmod{n}$. When this happens we call a a **liar** or **false witness** for n, or equivalently, say that n is a pseudomprime to the base a.

Remark 3. By Theorem 2.1 and Definition 2.2, when we say an integer number n 'passes the Fermat test', we mean n satisfies $a^{(n-1)} \equiv 1 \pmod{n}$.

Definition 2.2 is historically the notion of a pseudoprime. Fermat pseudoprimes are counterexamples to the converse of Fermat's little Theorem.

Example 2.3. Consider $n = 341$ and $a = 2$. The integer 341 satisfies Fermat's little theorem but it is not a prime number (as $341 = 11 \times 31$). So 341 is an example of Fermat pseudoprime.

The Fermat primality test is not foolproof; indeed, there are composite numbers that pass the Fermat primality test for all bases. We put the definition here.

Definition 2.4. A Carmichael number is a composite integer n such that $a^n \equiv a \pmod{n}$ for all integers a relatively prime to n.

An alternative and equivalent definition of Carmichael numbers is given by Korselt's criterion.

Theorem 2.5. *[Korselt, 1899] A composite integer n is a Carmichael number if and only if n is square-free, and for all primes $p \mid n$ we have $p-1 \mid n-1$.*

Example 2.6. The smallest example of Carmichael number is $n = 561 = 3 \cdot 11 \cdot 17$, for which $a^{560} \equiv 1 \pmod{561}$ for all integers a co-prime to 561.

Remark 4. We know there are infinitely many Carmichael numbers due to the work of [Alford et al., 1994]. Despite this the Carmichael numbers are relatively scarce compared to the prime numbers according to the bound [Erdős and Renyi, 1956]. Denoting the number of Carmichael numbers by $C(x)$ and the number of 2-pseudoprimes by $P(x)$ that are not exceeding x. Also, denote the number of primes not greater than x by $\pi(x)$, then we have

$$C(x) < x\exp\left(-c_2\frac{(\log x)(\log\log\log x)}{(\log\log x)}\right), \tag{2.1}$$

$$P(x) < x\exp\left(-c_1\sqrt{(\log x)(\log\log x)}\right), \tag{2.2}$$

for some positive constants c_1 and c_2, and by the 'Prime Number Theorem' we have

$$\pi(x) \sim \frac{x}{\log(x)} = x\exp(-\log\log x). \tag{2.3}$$

By definition, we know $C(x) < P(x)$, and by comparing (2.1) and (2.2), we expect $C(x) = o(P(x))$. Moreover, from (2.1), (2.2), and (2.3) we have $C(x) = o(\pi(x))$ and $P(x) = o(\pi(x))$. This means if a number passes the Fermat test, it is more likely to be prime than a false positive.

Understanding the likelihood that numbers are false positives motivates the following definition. The following definition is based on [Erdős and Pomerance, 1986, p. 875].

Definition 2.7. For a composite number n such that $(a,n) = 1$, the set of all residues modulo n that are false witnesses are denoted by

$$F(n) = \{a \pmod n : a^{n-1} \equiv 1 \pmod n\},$$

and the size of set is denoted by $\ell(n) = |F(n)|$.

Note that if $\ell(n)$ is large, then it would be hard to detect that n is composite using the Fermat primality test.

Definition 2.8. We denote the average size of $\ell(n)$ by $\frac{1}{x}\sum_{n\leqslant x}{}'\ell(n)$ where $\sum_{n\leqslant x}{}'$ defines a sum over composite numbers n up to x.

In the following theorem, Erdős and Pomerance (see [Erdős and Pomerance, 1986, p. 875]) investigated the average behavior of the function $\ell(n)$.

Theorem 2.9. *For x sufficiently large, we have*

$$x^{15/23} < \frac{1}{x}\sum_{n\leqslant x}{}'\ell(n) \leqslant x\mathcal{L}(x)^{-1+o(1)}, \tag{2.4}$$

where $\mathcal{L}(x) = \exp\left(\frac{(\log x)(\log\log\log x)}{\log\log x}\right)$.

This shows that the average size of $F(n)$ lies between $x^{15/23}$ and $x^{1-(1+o(1))(\frac{\log\log\log x}{\log\log x})}$,we see that on average there are a lot of false witnesses but not too many.

The lack of accuracy of the Fermat test because of the existence of false positives and Carmichael numbers was what motivated Grantham to introduce another primality test, which we will define in Section 2.2.

2.2 Frobenius pseudoprime

In this section, we use the theorem due to Grantham to define the Frobenius test, which experimentally has a much lower false positive rate, see [Baillie et al., 2021] and [Jacobsen, 2020].

We provide the following lemmas without proof and mention the definition of the splitting field here, which all come from [Cox, 2011b].

Lemma 2.10. *For all $n, m \in \mathbb{N}$, $m \mid n$ if and only if $x^{p^m} - x \mid x^{p^n} - x$.*

Lemma 2.11 (Fermat–Euler Theorem)**.** *If n and a are co-prime positive integers then $a^{\varphi(n)} \equiv 1 \pmod{n}$, where φ denotes Euler's totient function.*

Lemma 2.12. *let $d, n \in \mathbb{N}$. Then $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if $d \mid n$.*

Definition 2.13. [Cox, 2011a, Definition 5.1.1] Let $f(x) \in F[x]$ be a polynomial of degree $n \geq 1$. Then an extension $F \subset L$ is the **splitting field of** $f(x)$ **over** F if

$$f(x) = c\prod_{i=1}^{n}(x-\alpha_i),$$

where $c \in F$, $\alpha_i \in L$, for all i, and $L = F(\alpha_1, \ldots, \alpha_n)$ is the field extension obtained by adjoining the roots $\alpha_1, \ldots, \alpha_n$ to F.

In the next Lemma, we describe how the polynomial $x^{p^i} - x$ factors into irreducible polynomials modulo a prime number p. It is one of the well known lemmas from algebra.

Lemma 2.14. *If p is a prime number then*

$$x^{p^i} - x \equiv \prod_{d|i} G_d(x) \pmod{p},$$

where $G_d(x)$ is the product of all irreducible polynomials of degree d over $\mathbb{F}_p$.

Proof. The proof has three steps:

- First step: We show that $x^{p^i} - x$ has no repeated factors.
- Second step: We show that every irreducible polynomial of degree dividing i divides $x^{p^i} - x$.
- Third step: We show that if there exists an irreducible polynomial that divides $x^{p^i} - x$ then its degree has to divide i.

For the first step, it suffices to find the gcd of $x^{p^i} - x$ and its derivative. Its derivative is equal

to $p^i x^{p^i-1}-1$. Thus

$$\gcd(x^{p^i}-x, p^i x^{p^i-1}-1) \equiv \gcd(x^{p^i}-x,-1) \equiv 1 \pmod{p},$$

and $x^{p^i}-x$ does not have a multiple order root and thus no repeated factor.

For the second step, assume $g(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree d such that $d \mid i$. To show that $g(x)$ divides $x^{p^i}-x$, we are going to show that every root of $g(x)$ is a root of $x^{p^i}-x$. Since $g(x)$ is an irreducible polynomial with degree d then $\left(\frac{\mathbb{F}_p[x]}{<g(x)>}\right)^{\times}$ is a quotient ring with p^d-1 invertible elements. So by Lemma 2.11, for $x \in \left(\frac{\mathbb{F}_p[x]}{<g(x)>}\right)^{\times}$ we have $x^{p^d-1}=1$, or $x^{p^d}-x=0$. Hence, $x^{p^d}-x \in < g(x) >$ and $g(x) \mid x^{p^d}-x$. By Lemma 2.10, since d divides i then $x^{p^d}-x$ divides $x^{p^i}-x$. Therefore, $g(x) \mid x^{p^i}-x$.

For the last part, consider $g(x) \in \mathbb{F}_p[x]$ is an irreducible degree-d polynomial and that $g(x)$ divides $x^{p^i}-x$. Because $\mathbb{F}_{p^d} = \frac{\mathbb{F}_p[x]}{<g(x)>}$ and $\mathbb{F}_{p^d}$ is Galois, we see that the roots of $g(x)$ generate $\mathbb{F}_{p^d}$. Now, by our assumption, we know $g(x) | x^{p^i}-x = \prod_{\alpha \in \mathbb{F}_{p^i}} (x-\alpha)$, so the roots of $g(x)$ are in $\mathbb{F}_{p^i}$. This gives us $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^i}$. Hence by Lemma 2.12, we find $d \mid i$. □

The following claim follows immediately from the fact that the ring of polynomials over any field is a unique factorization domain.

Proposition 2.15. *[Grantham, 2001, p. 878] A polynomial $f(x)$ of degree d with no repeated roots can be written as $\prod_{i=1}^{d} H_i(x)$, where each $H_i(x)$ is the product of irreducible polynomials of degree i.*

The following definition comes from [Grantham, 2001, p. 878] with a few changes.

Definition 2.16. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree d with no repeated roots and p be a prime number. We recursively define $f_i(x)$ and $F_i(x)$ to be polynomials modulo p by

- $f_0(x) = f(x) \pmod{p}$,

- For $1 \leq i \leq d$, define $F_i(x) = \gcd(x^{p^i} - x, f_{i-1}(x)) \pmod{p}$ and $f_i(x) = \frac{f_{i-1}(x)}{F_i(x)}$.

The following claim can be extracted from the Grantham proof of [Grantham, 2001, Theorem 3.1]. Here we provide more details.

Lemma 2.17. *Let p be a prime. Suppose that $f(x) \in \mathbb{F}_p[x]$ is a degree-d polynomial with no repeated roots. Then the polynomial $F_i(x)$ in Definition 2.16 satisfies*

$$\textit{For all } 1 \leq i \leq d, F_i(x) = \gcd(G_i(x), f(x)),$$

with $H_i(x) = F_i(x)$, where $G_i(x)$ is as in Lemma 2.14 and $H_i(x)$ is as in Proposition 2.15.

Proof. First we will show that $H_i(x) = \gcd(G_i(x), f(x))$ and then we will use this to show that the polynomial $H_i(x)$ is exactly the polynomial $F_i(x)$ from Definition 2.16.
We know that $H_i(x)$ is the product of the irreducible polynomials of degree i that divide $f(x)$, and since $G_i(x)$ is the product of all irreducible polynomials of degree i, it follows that $H_i(x) \mid G_i(x)$. Thus,

$$\gcd(G_i(x), f(x)) = \gcd(G_i(x), \prod_{i=1}^{d} H_i(x)) = H_i(x).$$

Now we prove by induction on i that $F_i(x) = H_i(x)$ and $f_i(x) = \prod_{t=i+1}^{d} H_t(x)$.

For $i = 1$, Definition 2.16 gives $F_1(x) = \gcd(x^p - x, f(x))$, and by the definition of $G_i(x)$, we have $G_1(x) = x^p - x$. Therefore, $F_1(x) = \gcd(G_1(x), f(x))$. This proves the first part of the base step of the induction, showing that $H_1(x) = F_1(x)$. By Definition 2.16, we know that $f_1(x) = \frac{f(x)}{F_1(x)}$. Since we have established that $H_1(x) = F_1(x)$, substituting this into our expression gives us

$$f_1(x) = \frac{f(x)}{F_1(x)} = \frac{f(x)}{H_1(x)}.$$

The polynomial $H_1(x)$ is the product of linear irreducible polynomials that divide $f(x)$, and

since $f(x)$ has no repeated roots, dividing by $H_1(x)$ removes all the degree 1 factors. Thus, $f_1(x)$ is equal to the product of irreducible polynomials of degrees greater than 1. We can also express this as follows, using Proposition 2.15

$$f_1(x) = \prod_{t=2}^{d} H_t(x).$$

Now, for the purpose of induction, assume $H_{i-1}(x) = F_{i-1}(x)$ and $f_{i-1}(x) = \prod_{t=i}^{d} H_t(x)$. We will show that $H_i(x) = F_i(x)$ and that $f_i(x) = \prod_{t=i+1}^{d} H_t(x)$. By Definition 2.16, we know that

$$F_i(x) = \gcd(f_{i-1}(x), x^{p^i} - x).$$

Additionally, by Lemma 2.14, we know that $x^{p^i} - x \equiv \prod_{j|i} G_j(x)$ modulo p. Substituting this into the expression, we get

$$F_i(x) = \gcd(f_{i-1}(x), \prod_{j|i} G_j(x)).$$

By the induction hypothesis for $f_{i-1}(x)$, we have

$$F_i(x) = \gcd(\prod_{t=i}^{d} H_t(x), \prod_{j|i} G_j(x)).$$

Since we know that $H_i(x) \mid G_i(x)$ and $j \leq i$, it follows that

$$F_i(x) = \gcd(H_i(x), G_i(x)) = H_i(x).$$

Now by the definition of $f_i = \frac{f_{i-1}(x)}{F_i(x)}$ and by the induction hypothesis, we have

$$f_i(x) = \frac{f_{i-1}(x)}{F_i(x)} = \frac{\prod_{t=i}^{d} H_t(x)}{F_i(x)} = \frac{\prod_{t=i}^{d} H_t(x)}{H_i(x)} = \prod_{t=i+1}^{d} H_t(x).$$

The result now follows by induction. □

Remark 5. The fact that p does not divide the discriminant and that $f(x) \in \mathbb{F}_p[x]$ does not have repeated roots are equivalent. If $f(x)$ has repeated roots then, by Definition 1.10, the discriminant is equal to 0, that is, p divides the discriminant.

The following theorem, which we refer to as Grantham's Theorem, is a fundamental theorem that leads us to the definition of Frobenius pseudoprime. [Grantham, 2001, Theorem 3.1]

Theorem 2.18. *Let p be an odd prime, and let $f(x)$ be a monic polynomial in $\mathbb{F}_p[x]$ of degree d with discriminant Δ. Assume $p \nmid f(0)\Delta$ with $F_i(x)$ and $f_i(x)$ defined in Definition 2.16.*

1. *We have $f_d(x) = 1$ and for $i = 1, \cdots, d$ we have $i \mid \deg(F_i)$.*
2. *For $2 \leq i \leq d$, we have $F_i(x) \mid F_i(x^p)$.*
3. *Let $S = \sum_{2|i} \frac{\deg(F_i(x))}{i}$. Then $(-1)^S = \left(\frac{\Delta}{p}\right)$. That is, if $\left(\frac{\Delta}{p}\right) = 1$, then S is an even integer, and if $\left(\frac{\Delta}{p}\right) = -1$, then S is an odd integer.*

Proof. For the first claim we use Definition 2.16.

$$
\begin{aligned}
f_1(x) &= \frac{f_0(x)}{F_1(x)}, \\
f_2(x) &= \frac{f_1(x)}{F_2}(x) = \frac{\frac{f_0(x)}{F_1(x)}}{F_2(x)} = \frac{f_0(x)}{F_1(x)F_2(x)}, \\
f_3(x) &= \frac{f_2(x)}{F_3(x)} = \frac{f_0(x)}{F_1(x)F_2(x)F_3(x)}, \\
&\vdots \\
f_d(x) &= \frac{f_{d-1}(x)}{F_d(x)} = \frac{f_0(x)}{F_1(x)F_2(x)\cdots F_d(x)} = \frac{f_0(x)}{f(x)} = \frac{f(x)}{f(x)} = 1.
\end{aligned}
$$

To prove $i \mid \deg(F_i)$ for $1 \leq i \leq d$, by Definition 2.15 and Lemma 2.17, we have

$$F_i(x) = \prod_{\substack{\deg(g(x))=i \\ g(x) \text{ is irr poly}}} g(x).$$

Thus $\deg(F_i(x))$ is equal to the product of the number of irreducible polynomials $g(x)$ and i as the degree of polynomial $g(x)$, namely $i \mid \deg(F_i)$.

Let $2 \leq i \leq d$, we now prove $F_i(x) \mid F_i(x^p)$. we recall that $(x+y)^p = x^p + y^p$ in $\mathbb{F}_p[x]$, so $F_i(x^p) = (F_i(x))^p$ in $\mathbb{F}_p[x]$. Hence, $F_i(x) \mid F_i(x^p)$.

For convenience, we delay the proof of third part until in Chapter 3, Lemma 3.19. □

We take the following definition precisely from [Grantham, 2001, p. 880].

Definition 2.19. Let $f(x), g_1(x), g_2(x)$ be monic polynomials over a commutative ring (with identity). We say that $f(x)$ is the greatest common monic divisor (gcmd) of $g_1(x)$ and $g_2(x)$ if the ideal generated by $g_1(x)$ and $g_2(x)$ is equal to the ideal generated by $f(x)$. We write $f(x) = \text{gcmd}(g_1(x), g_2(x))$. Note that $\text{gcmd}(g_1(x), g_2(x))$ does not necessarily exist

The following theorem and Remark 6 come from [Cox, 2011b, p. 516] with a little modifications.

Theorem 2.20. *Division Algorithm. Let $f(x), g(x) \in F[x]$ where F is an integral domain, and assume that $g(x)$ is nonzero. Then there are polynomials $q(x), r(x) \in F[x]$ such that*

$$f(x) = q(x)g(x) + r(x), \text{ where } r(x) = 0 \text{ or } \deg(r(x)) < \deg(g(x)).$$

Furthermore, $q(x)$ and $r(x)$ are unique.

Remark 6. The application of Theorem 2.20 is the Euclidean algorithm for computing the greatest common divisor (or gcd) of two polynomials $f(x), g(x) \in F[x]$, at least one of

which is nonzero. Recall that $\gcd(f(x),g(x))$ is the polynomial of maximum degree in $F[x]$, which divides both $f(x)$ and $g(x)$. If $g(x) \neq 0$, we compute $\gcd(f(x),g(x))$ by repeatedly applying the division algorithm until we get a zero remainder:

$$\begin{aligned}
f(x) &= q_0(x)g(x) + r_0(x), \quad \deg(r_0(x)) < \deg(g(x)),\\
g(x) &= q_1(x)r_0(x) + r_1(x), \quad \deg(r_1(x)) < \deg(r_0(x)),\\
r_0(x) &= q_2(x)r_1(x) + r_2(x), \quad \deg(r_2(x)) < \deg(r_1(x)),\\
&\vdots\\
r_n(x) &= q_{n+2}(x)r_{n+1}(x) + r_{n+2}(x), \quad \deg(r_{n+2}(x)) < \deg(r_{n+1}(x)),\\
r_{n+1}(x) &= q_{n+3}(x)r_{n+2}(x) + 0.
\end{aligned}$$

Then $\gcd(f(x),g(x))$ is equal to $r_{n+2}(x)$.

Lemma 2.21. *[Stein, 2005] Let $f(x),g(x) \in F[x]$. By Theorem 2.20 and Remark 6, we have $f(x) = g(x)q(x) + r(x)$ for some $q(x),r(x) \in F[x]$ such that $\deg(r(x)) < \deg(g(x))$. Then we have*

$$\gcd(f(x),g(x)) = \gcd(r(x),g(x)).$$

The next proposition explains that although the Euclidean algorithm can't always find a GCMD, it will have identified that n is not prime.

Proposition 2.22. *[Grantham, 2001, Proposition 3.5] The Euclidean algorithm will either find the GCMD of two monic polynomials in $(\mathbb{Z}/n\mathbb{Z})[x]$ or find a proper factor of n.*

Proof. We know that $(\mathbb{Z}/n\mathbb{Z})$ is not a principal ideal domain when n is composite; that is, some of the numbers in $(\mathbb{Z}/n\mathbb{Z})$ are not invertible. By Remark 6, we see that the long division needs to be done as part of the Euclidean algorithm over $(\mathbb{Z}/n\mathbb{Z})$ and it is possible if the leading coefficients of each non-zero remainder is invertible. So, the Euclidean algorithm can only fail to complete if one of the divisions fails because the non-zero leading

coefficient of a remainder is not invertible in $(\mathbb{Z}/n\mathbb{Z})$. In such cases, this coefficient will share a nontrivial factor of n.

When the Euclidean algorithm terminates (meaning one of the remainders becomes zero), the last non-zero remainder is a divisor of the two polynomials and can be expressed as a linear combination of the two. This proof follows the same identical as the proof of the correctness of the Euclidean algorithm over polynomials. When the leading coefficient of the last non-zero remainder is invertible, we can make this remainder monic through division, ultimately leading to the determination of the greatest common monic divisor (gcmd). □

Note that even if gcmd exists, the Euclidean algorithm might detect a factor of n while computing it. In the following example we will demonstrate this fact.

Example 2.23. Let $n = 20$. We want to find $\text{gcmd}(x^{20} - x, x^2 + x + 1)$ over $(\mathbb{Z}/20\mathbb{Z})$. By Theorem 2.20, we have

$$(x^{20} - x) = (x^2 + x + 1)T(x) + (-2x - 1), \tag{2.5}$$

where $T(x) = x^{18} - x^{17} + x^{15} - x^{14} + x^{12} - x^{11} + x^9 - x^8 + x^6 - x^5 + x^3 - x^2 + 1$. Now by Lemma 2.21 we have

$$\text{gcmd}(x^{20} - x, x^2 + x + 1) = \text{gcmd}(-2x - 1, x^2 + x + 1).$$

Since -2 does not have multiplicative inverse in $(\mathbb{Z}/20\mathbb{Z})[x]$, the Euclidean Algorithm does not terminate. Then, as predicted by Proposition 2.22, we find 2 as the proper factor of 20.

On the other hand, we have the linear combination of $x^2 + x + 1$ and $-2x - 1$, that is

$$(28)(x^2 + x + 1) + (14x + 7)(-2x - 1) \equiv 1 \pmod{20}. \tag{2.6}$$

So, by combining (2.5) and (2.6) we have

$$(x^2+x+1)(28-(14x+7)T(x))+(x^{20}-x)(14x+7)\equiv 1. \pmod{20}$$

That means we find gcmd of x^2+x+1 and $x^{20}-x$ is equal to 1.

Now we define the Frobenius probable prime numbers and then the Frobenius pseudoprime numbers definition. Definition 2.24 is based on [Grantham, 2001, p. 881].

Definition 2.24. Let $f(x)\in\mathbb{Z}[x]$ be a monic polynomial of degree d with discriminant Δ and consider the odd integer $n>1$. We say n is the Frobenius probable prime number respect to $f(x)$, if $(n,f(0)\Delta)=1$ and it passes the following algorithm. Note that all computations are done in $(\mathbb{Z}/n\mathbb{Z})[x]$.

1. **Factorization Step**.

   - Let $f_0(x)=f(x)$.
   - For $1\le i\le d$, let $F_i(x)=\text{gcmd}(x^{n^i}-x, f_{i-1}(x))$ and $f_i(x)=\frac{f_{i-1}(x)}{F_i(x)}$.

   If any of the gcmds do not exist, declare that n to be composite and stop, similarly, if $f_d(x)\neq 1$, declare n to be composite and stop.
   If n passes the Factorization step then we move to the next step of the algorithm.

2. **Frobenius Step**. For $2\le i\le d$, compute $F_i(x^n) \pmod{F_i(x)}$. If it is nonzero for some i, declare n to be composite and stop.
   If n passes the Factorization step and Frobenius step then we move to the last step of the algorithm.

3. **Jacobi Step**. Let $S=\sum_{2|i}\frac{\deg(F_i(x))}{i}$. If $(-1)^S\neq\left(\frac{\Delta}{n}\right)$, declare n to be composite and stop.

If n passes all these three steps, declare n to be a Frobenius probable prime respect to the monic polynomial $f(x)$.

Remark 7. We call the algorithm in Definition 2.24 Grantham's algorithm.

Remark 8. [Grantham, 2020, Grantham, 1998] All of these calculations can be done in time $O(\log(n))$.

The following definition is the definition of Frobenius pseudoprime numbers which is based on [Grantham, 2001, p. 882].

Definition 2.25. Let $f(x) \in \mathbb{Z}[x]$. We call n is a Frobenius pseudoprime with respect to a monic polynomial $f(x)$ if it is a composite and a Frobenius probable prime as in Definition 2.24.

Definition 2.26. When n is a Frobenius pseudoprime with respect to the polynomial $f(x)$ we shall call $f(x)$ a liar, or false witness, for n.

Remark 9. In general, we will say that (f,n) is a Frobenius pseudoprime or a liar pair whenever n is a Frobenius pseudoprime with respect to the polynomial $f(x)$.

Definition 2.27. If (f,n) gives a Frobenius pseudoprime, we shall refer to the sequence of numbers $\frac{\deg F_i(x)}{i}$ as the cycle structure of the Frobenius pseudoprime, when $F_i(x)$ is the product of disjoint $i-$cycles. This terminology will be motivated by Lemma 3.19.

Remark 10. By Definition 2.24, if (f,n) is a Frobenius pseudoprime, then $f_d(x) = 1$ is equivalent to $f(x) = F_1(x)\cdots F_d(x)$.

By the Frobenius definition, we will see that the Fermat pseudoprime numbers are degree-1 Frobenius pseudoprimes. Also, in the following theorem we will see that the converse statement is also true.

Theorem 2.28. *[Grantham, 2001, Theorem 4.1] An odd integer n is a Fermat pseudoprime to the base a if and only if it is a Frobenius pseudoprime with respect to the polynomial* $f(x) = x - a$.

Proof. First, assume n is a Fermat pseudoprime number to the base a. This means is $a^{n-1} \equiv 1 \pmod{n}$. Since n is a Fermat pseudoprime so $a^n \equiv a \pmod{n}$ that is $x - a \mid x^n - x$. Now we apply the steps of Grantham's algorithm to $f(x) = x - a$.

The first thing is that, we have $(n, f(0)\Delta) = (n, a) = 1$ since $\Delta = 1$. For the factorization step, since $d = 1$ then $f_1(x) = 1$ and $f_0 = f(x)$ so we have to show that $F_1(x) = f(x)$. Then we have

$$F_1(x) = \operatorname{gcmd}(x^n - x, x - a) = x - a \pmod{n}$$

Since $d = 1$, the Frobenius Step is vacuous. Note that $S = 0$ and $\left(\frac{\Delta}{n}\right) = \left(\frac{1}{n}\right) = 1$, so n passes the Jacobi Step. Therefore n is a Frobenius pseudoprime.

Now, assume n is a Frobenius pseudoprime with respect to $x - a$. Since n is a Frobenius pseudoprime by the factorization step we must have $f_1(x) = 1$ and $F_1(x) = x - a$. So by the Factorization Step, we know $(x - a) \mid (x^n - x)$ means that a is a root of $x^n - x$ so that $a^n - a = 0$. Since $(n, f(0)\Delta) = (n, a) = 1$, then we have $a^{n-1} \equiv 1 \pmod{n}$. Thus n is a Fermat pseudoprime to the base a. □

Remark 11. Frobenius pseudoprimes can be categorized based on the degree of the associated polynomial $f(x)$. Specifically, we distinguish the following cases:

1. For a linear polynomial $f(x)$, we obtain degree-1 Frobenius pseudoprimes, these are Fermat pseudoprimes. The number of these was studied by Erdős and Pomerance.

2. For a quadratic polynomial $f(x)$, we obtain degree-2 Frobenius pseudoprimes. The number of these was studied by Fiori and Shallue.

3. For a cubic polynomial $f(x)$, we define degree-3 Frobenius pseudoprimes. The aim of my thesis is to generalize the existing results on counting these from degree-1 and degree-2 pseudoprimes to the case of cubic polynomials.

Now, we want to provide some examples that illustrate the algorithm's performance and how we can use it to identify if a number is a Frobenius probable prime or is definitely composite.

All calculations in these examples have been solved by Sage. We have attached the code in Appendix A.

Example 2.29. Consider the number $n = 89$ and the irreducible polynomial $f(x) = x^4 + 12x + 1$ over $\mathbb{Z}$. Now we implement the algorithm steps.

1 **Factorization Step**.

- Initiate with $i = 1$ and applying Lemma 2.21 we find

$$\begin{aligned} F_1(x) &= \gcmd\left(x^{89} - x, x^4 + 12x + 1\right) \\ &= \gcmd\left(59x^3 + 51x^2 + 20x + 86, x^4 + 12x + 1\right) \\ &= x + 78, \end{aligned}$$

in $(\mathbb{Z}/89\mathbb{Z})[x]$. So, $f_1(x) = \frac{f(x)}{F_1(x)} = \frac{x^4+12x+1}{x+78} = x^3 + 11x^2 + 32x + 8$. By the above arithmetic we have $F_1(x) = x + 78$. That means, $1 \mid \deg(F_1(x))$.

- For $i = 2$,

$$\begin{aligned} F_2(x) = \gcmd\left(x^{89^2} - x, f_1(x)\right) &= \gcmd\left(x^{89^2} - x, x^3 + 11x^2 + 32x + 8\right) \\ &= \gcmd\left(64x^2 + 86x + 19, x^3 + 11x^2 + 32x + 8\right) \\ &= 1, \end{aligned}$$

in $(\mathbb{Z}/89\mathbb{Z})[x]$. Thus, $f_2(x) = \frac{f_1(x)}{F_2(x)} = f_1(x) = x^3 + 11x^2 + 32x + 8$, and we have that $\deg(F_2(x)) = 0$, so that $0 \mid \deg F_2(x)$.

– For $i = 3$,

$$\begin{aligned} F_3(x) = \text{gcmd}\left(x^{89^3} - x, f_2(x)\right) &= \text{gcmd}\left(x^{89^3} - x, x^3 + 11x^2 + 32x + 8\right) \\ &= \text{gcmd}\left(0, x^3 + 11x^2 + 32x + 8\right) \\ &= x^3 + 11x^2 + 32x + 8, \end{aligned}$$

in $(\mathbb{Z}/89\mathbb{Z})[x]$. Thus, $f_3(x) = \frac{f_2(x)}{F_3(x)} = 1$, and $\deg F_3(x) = 3$ then $3 \mid \deg(F_3(x))$.

– For $i = 4$,

$$\begin{aligned} F_4(x) &= \text{gcmd}\left(x^{89^4} - x, f_3(x)\right) \\ &= \text{gcmd}\left(x^{89^4} - x, 1\right) \\ &= \text{gcmd}\,(0, 1) \\ &= 1, \end{aligned}$$

in $(\mathbb{Z}/89\mathbb{Z})[x]$. Thus, $f_4(x) = 1$, $\deg F_4(x) = 0$ so $4 \mid \deg F_4(x) = 0$.

Thus 89 passes the first step.

2 **Frobenius Step**.

– For $i = 2, F_2(x) = 1$ and $F_2(x^{89}) = 1$. So, $F_2(x^{89}) \equiv 0 \pmod{F_2(x)}$. Thus $F_2(x) | F_2(x^{89})$

– For $i = 3, F_3(x) = f_2(x) = x^3 + 11x^2 + 32x + 8$, then

$$F_3(x^{89}) \equiv f_2(25x^2 + x + 59) \equiv 0 \pmod{F_3(x)}.$$

Thus, $F_3(x) | F_3(x^{89})$.

– For $i = 4, F_4(x) = 1$ then $F_4(x^{89}) = 1$. So, $F_4(x) | F_4(x^{89})$.

Thus, we conclude that 89 passes the second step.

3 **Jacobi Step**.

$S = \frac{\deg F_2(x)}{2} + \frac{\deg F_4(x)}{4} = 0 + 0 = 0$. Then $(-1)^S = (-1)^0 = 1$. On the other hand, $(\frac{\Delta}{n}) = (\frac{16}{89}) = 1$. So, $(\frac{\Delta}{n}) = (-1)^S$, making 89 passing the third step.

We conclude that 89 is a Frobenius probable prime number!

The following example shows how the choice of polynomials changes the outcome of the test. We will illustrate this with $n = 1763$ and the irreducible polynomials $f(x) = x^2 - 3x - 1$ and $f(x) = x^2 + x + 1$.

(a) We consider $n = 1763 = 41 \times 43$ and the irreducible polynomial $f(x) = x^2 - 3x - 1$ over $\mathbb{Z}$. Now we implement the algorithm steps.

1 **Factorization Step**.

– For $i = 1$,

$$F_1(x) = \text{gcmd}\left(x^{1763} - x, x^2 - 3x - 1\right) = \text{gcmd}\left(1760, x^2 - 3x - 1\right) = 1,$$

in $(\mathbb{Z}/1763\mathbb{Z})[x]$. Thus, $f_1(x) = \frac{f(x)}{F_1(x)} = f(x) = x^2 - 3x - 1$ and $\deg F_1(x) = 0$ so that we have $1 \mid \deg F_1(x)$.

– For $i = 2$,

$$\begin{aligned} F_2(x) &= \text{gcmd}\left(x^{1763^2} - x, x^2 - 3x - 1\right) \\ &= \text{gcmd}\left(0, x^2 - 3x - 1\right) \\ &= x^2 - 3x - 1 \end{aligned}$$

in $(\mathbb{Z}/1763\mathbb{Z})[x]$. Thus, $f_2(x) = \frac{f_1(x)}{F_2(x)} = 1$ and we have $\deg F_2(x) = 2$ and so $2 \mid \deg F_2(x)$.

So, 1763 passes the first step.

2 **Frobenius Step**.

– For $i = 2, F_2(x) = f_1(x) = f(x) = x^2 - 3x - 1$. So,

$$F_2(x^{1763}) \equiv F_2(x+1760) \equiv f(x+1760) = 1757x + 18 \not\equiv 0 \pmod{F_2(x)},$$

in $(\mathbb{Z}/1763\mathbb{Z})[x]$. Therefore $F_2(x) \nmid F_2(x^{1763})$. So, 1763 could not pass the Frobenius step. That means 1763 is a composite number.

(b) For $n = 1763$ still, we now use the irreducible polynomial $f(x) = x^2 + x + 1$ over $\mathbb{Z}$ instead of $f(x) = x^2 - 3x - 1$.

1 **Factorization Step**.

– For $i = 1$,

$$\begin{aligned} F_1(x) = \gcmd\left(x^{1763} - x, x^2 + x + 1\right) &= \gcmd\left(1761x + 1762, x^2 + x + 1\right) \\ &= 1 \end{aligned}$$

in $(\mathbb{Z}/1763\mathbb{Z})[x]$. Thus, $f_1(x) = \frac{f(x)}{F_1(x)} = f(x) = x^2 + x + 1$, so $\deg F_1(x) = 0$, and $1 \mid \deg F_1(x)$.

– For $i = 2$,

$$F_2(x) = \gcmd\left(x^{1763^2} - x, x^2 + x + 1\right) = \gcmd\left(0, x^2 + x + 1\right) = x^2 + x + 1,$$

in $(\mathbb{Z}/1763\mathbb{Z})[x]$. Thus $f_2(x) = \frac{f_(1)}{F_1(x)} = 1$, $\deg F_2(x) = 2$. So, $2 \mid \deg F_2(x)$.
So, 1763 passed the first step.

2 **Frobenius Step**.

For $i = 2, F_2(x) = f(x) = x^2 + x + 1$ we have

$$F_2(x^{1763}) \equiv F_2(1762x + 17620) \equiv f(1762x + 17620) \equiv 0 \pmod{F_2(x)},$$

Therefore 1763 passed the Frobenius step.

3 **Jacobi Step**.

$S = \frac{\deg F_2(x)}{2} = 1$, then $(-1)^S = (-1)^1 = -1$. The Jacobi symbol is equal to $(\frac{\Delta}{n}) = (\frac{1760}{1763}) = -1$. Therefore, $(-1)^S = (\frac{\Delta}{n})$, making 1763 passing the last step.

Hence, we also conclude that 1763 is a probable prime number. If we consider part (a) or that $1763 = 41 \cdot 43$ then we see that it is composite and so 1763 is a Frobenius pseudoprime number.

Due to the last example, we find that choosing the irreducible polynomial has a direct effect on the algorithm's determination of whether the number is composite or Frobenius probable prime.

One of the questions is how to choose a better irreducible polynomial. To understand how 'good' an irreducible polynomial is, we need to be able to determine how likely it is to identify composite numbers. One way to determine the accuracy of the Frobenius primality test is to estimate a count for the number of Frobenius pseudoprimes.

2.2.1 Quadratic Frobenius pseudoprimes

In this section, we introduce the key theorems and lemmas of [Fiori and Shallue, 2020]. It is these results, that we will generalize to cubic Frobenius pseudoprimes. We will provide the generalization in Chapter 3 and 4.

Fiori and Shallue utilized Grantham's algorithm and Definition 2.25 to study quadratic Frobenius pseudoprimes. Before applying Grantham's algorithm to outline key theorems and lemmas, we will restate the terminology used in [Fiori and Shallue, 2020], with minor

modifications.

Fiori and Shallue refined the counting quadratic Frobenius liars with respect to the value of the Jacobi symbol. We are going to explain it more in the following definition.

Definition 2.30. For each fixed value of n, denote by $L_2^+(n)$ the total number of quadratic polynomials $f(x)$ modulo n such that $(f(x),n)$ is a liar pair and $(\frac{\Delta_f}{n}) = +1$. Likewise, denote by $L_2^-(n)$ the total number of quadratic polynomials $f(x)$ modulo n such that $(f(x),n)$ is a liar pair and $(\frac{\Delta_f}{n}) = -1$.

Note 2.31. Instead of working over $(\mathbb{Z}/n\mathbb{Z})$, they worked over $(\mathbb{Z}/p^r\mathbb{Z})$ and finalized the result by using the Chinese Reminder Theorem. So by splitting the calculation over $p^r \mid n$ then we can rewrite Jacobi symbol $\left(\frac{\Delta_f}{n}\right) = \prod_{i=1}^{t}\left(\frac{\Delta_f}{p_i}\right)^{r_i}$, where $n = \prod_{i=1}^{t} p_i^{r_i}$.

Definition 2.32. For all primes p such that $p^r \mid n$, they defined that n is a Frobenius pseudoprime at p^r if each of the first two steps of Grantham's test are satisfied modulo p^r.

Briefly we have the definition of $L_2^{++}(n,p_i)$, $L_2^{+-}(n,p_i)$, $L_2^{--}(n,p_i)$, and $L_2^{-+}(n,p_i)$ in the following definition.

Definition 2.33. Suppose $p^r \| n$ then we have one of four following cases

1. The number of quadratic polynomials over $\mathbb{Z}/p^r\mathbb{Z}$ with $\left(\frac{\Delta}{n}\right) = +1$ and $\left(\frac{\Delta}{p}\right) = +1$ for which n is a quadratic Frobenius pseudoprime at p is denoted by $L_2^{++}(n,p)$.

2. The number of quadratic polynomials over $\mathbb{Z}/p^r\mathbb{Z}$ with $\left(\frac{\Delta}{n}\right) = +1$ and $\left(\frac{\Delta}{p}\right) = -1$ for which n is a quadratic Frobenius pseudoprime at p is denoted by $L_2^{+-}(n,p)$.

3. The number of quadratic polynomials over $\mathbb{Z}/p^r\mathbb{Z}$ with $\left(\frac{\Delta}{n}\right) = -1$ and $\left(\frac{\Delta}{p}\right) = -1$ for which n is a quadratic Frobenius pseudoprime at p is denoted by $L_2^{--}(n,p)$.

4. The number of quadratic polynomials over $\mathbb{Z}/p^r\mathbb{Z}$ with $\left(\frac{\Delta}{n}\right) = -1$ and $\left(\frac{\Delta}{p}\right) = +1$ for

which n is a quadratic Frobenius pseudoprime at p is denoted by $L_2^{-+}(n,p)$.

Remark 12. When Jacobi symbol $\left(\frac{\Delta_f}{n}\right) = +1$ then we have $\left(\frac{\Delta_f}{p_i}\right) = -1$ for an even number of the $p^{r_i}|n$ for which r_i is odd, or $\left(\frac{\Delta_f}{p_i}\right) = +1$. In this case we show the number of Frobenius liars by $L_2^{+-}(n,p_i)$ and $L_2^{++}(n,p_i)$ respectively.
Also, if Jacobi symbol $\left(\frac{\Delta_f}{n}\right) = -1$ then we have $\left(\frac{\Delta_f}{p_i}\right) = -1$ for an odd number of the $p^{r_i}|n$ for which r_i is odd, or $\left(\frac{\Delta_f}{p_i}\right) = +1$. In this case we show the number of Frobenius liars by $L_2^{--}(n,p_i)$ and $L_2^{-+}(n,p_i)$ respectively.

Theorem 2.34. *[Fiori and Shallue, 2020, Theorem 12] For $p^r||n$ we have*

$$\begin{aligned} L_2^+(n) = &\frac{1}{2}\prod_i \left(L_2^{++}(n,p_i) + L_2^{+-}(n,p_i)\right) \\ &+ \frac{1}{2}\prod_{2|r_i} \left(L_2^{++}(n,p_i) + L_2^{+-}(n,p_i)\right) \prod_{2\nmid r_i} \left(L_2^{++}(n,p_i) - L_2^{+-}(n,p_i)\right). \end{aligned} \tag{2.7}$$

Theorem 2.35. *[Fiori and Shallue, 2020, Theorem 16] For $p^r||n$ we have*

$$\begin{aligned} L_2^-(n) = &\frac{1}{2}\prod_i \left(L_2^{-+}(n,p_i) + L_2^{--}(n,p_i)\right) \\ &- \frac{1}{2}\prod_{2|r_i} \left(L_2^{-+}(n,p_i) + L_2^{--}(n,p_i)\right) \prod_{2\nmid r_i} \left(L_2^{-+}(n,p_i) - L_2^{--}(n,p_i)\right). \end{aligned} \tag{2.8}$$

In equation (2.7) and (2.8) respectively, they have ensured that only terms with the correct number of $\left(\frac{\Delta_f}{p_i}\right) = -1$ will remain. In Chapter 4, we will present Theorem 4.15 with detailed proof, which is analogous of Theorems 2.34 and 2.35, and demonstrate how to prove this type of result in general.

The next few lemmas show the formulas for finding the number of quadratic Frobenius liars in the cases of $L_2^{++}(n,p), L_2^{+-}(n,p), L_2^{-+}(n,p)$, and $L_2^{--}(n,p)$.

By knowing these formulas we can establish the inequalities (2.13) and (2.14). Us-

ing equations (2.9) and (2.10) in Lemma 2.36, we deduce a formula for $L_2^+(n)$, and using equations (2.11) and (2.12) in Lemma 2.36, we deduce a formula for $L_2^-(n)$.

Lemma 2.36. *[Fiori and Shallue, 2020, Lemma 10, 11, 14, 15] Suppose $p^r \| n$. Then*

$$L_2^{++}(n,p) = \frac{1}{2}\left(\gcd(n-1,p-1)^2 - \gcd(n-1,p-1)\right), \tag{2.9}$$

$$L_2^{+-}(n,p) = \frac{1}{2}\left(\gcd(n-1,p^2-1) - \gcd(n-1,p-1)\right), \tag{2.10}$$

$$L_2^{-+}(n,p) = \frac{1}{2}\left(\gcd(n^2-1,p-1) - \gcd(n-1,p-1)\right), \tag{2.11}$$

and

$$L_2^{--}(n,p) = \frac{1}{2}\left(\gcd(p^2-1,n^2-1,n-p) - \gcd(n-1,p-1)\right). \tag{2.12}$$

In Chapter 4, we will present Lemmas 4.7-4.14 with proofs, which are analogous to Lemma 2.36, and demonstrate how to prove this type of result in general.

In the following theorems, they provided the upper and lower bounds for the number of quadratic Frobenius pseudoprimes.

Theorem 2.37. *[Fiori and Shallue, 2020, Theorem 2] For all $\alpha \leq 10/3$ and all x sufficiently large,*

$$x^{3-\alpha^{-1}-o(1)} \leq \sum_{n\leq x}{}' L_2^+(n) \leq x^3 \mathcal{L}(x)^{-1+o(1)}. \tag{2.13}$$

Moreover, the same bounds hold if we replace $L_2^+(n)$ by $L_2(n)$.

Theorem 2.38. *[Fiori and Shallue, 2020, Theorem 3] For all $\alpha \leq 4/3$ and all x sufficiently large,*

$$x^{3-\alpha^{-1}-o(1)} \leq \sum_{n\leq x}{}' L_2^-(n) \leq x^3 \mathcal{L}(x)^{-1+o(1)}. \tag{2.14}$$

We will provide Theorems 4.36 and 4.54 corresponding to Theorems 2.37 and 2.38,

along with detailed proofs.

Chapter 3

Reinterpretation Of Frobenius Pseudoprimes

In this chapter, we reinterpret the definition of Grantham's test in terms of permutations of roots of polynomials. The purpose of this chapter is to allow us to count Frobenius pseudoprimes in the next chapter. Since the conditions in Grantham's test 2.24 are hard to use directly to count cubic Frobenius liars, here we give a reinterpretation of Grantham's test as a condition on the map $x \mapsto x^m$ being a permutation of the roots of a polynomial. Before delving into the proofs, we briefly present the philosophy of lemmas and theorems in this chapter.

In Lemmas 3.13–3.17, our focus is to explain how the factorization step in Grantham's algorithm relates to the map $x \mapsto x^m$, which induces a permutation on the set of roots of the polynomial $P(x)$.

In Lemmas 3.18–3.19, we establish how the Jacobi step in Grantham's algorithm has a reinterpretation in terms of the permutation's cycle structure.
Finally, our understanding of Grantham's ideas is wrapped up in Theorem 3.28, which neatly summarizes what we've learned.

Here, we mention some notations that are used frequently during this section.

Terminology. We denote a monic polynomial $P(x)$ of degree d over a field F with no

repeated roots, and the set of its distinct roots by $M = \{\alpha_1, \cdots, \alpha_n\}$. We denote the permutations of the set M by σ, and write $\sigma^d(\alpha_i) = \underbrace{\sigma(\sigma(\cdots(\sigma}_{\text{d times}}(\alpha_i))))$ for a d times composition of permutation σ.

Definition 3.1. We define the map $\phi : \overline{F} \to \overline{F}$ by $\phi(x) = x^m$.

The following definitions are given in [Knapp, 2006], with some modifications.

Definition 3.2. Let $\sigma \in S_n$ and $a \in \{1, \cdots, n\}$. let i be the smallest positive integer such that $\sigma^i(a) = a$. Then $(a, \sigma(a), \cdots, \sigma^{i-1}(a))$ is called a cycle of σ of length i, or an i-cycle generated by a. In this case we say that a belongs to an i-cycle of σ and i is an order of a that is indicated by $\text{ord}(a) = i$.

Definition 3.3. A cyclic permutation of length 2 (i.e. a permutation that only exchanges two elements) is called a transposition.

Definition 3.4. A permutation is called even if it can be expressed as a product of an even number of transpositions. It is called odd otherwise

Remark 13. A cycle is an even permutation if and only if its length is odd, and a cycle is an odd permutation if and only if its length is even.

Definition 3.5. The sign of a permutation σ is denoted $\text{sgn}(\sigma)$ and defined as $+1$ if σ is even and -1 if σ is odd. Alternatively, the sign of a permutation σ can be defined from its decomposition into the product of transpositions as

$$\text{sgn}(\sigma) = (-1)^m,$$

where m is the number of transpositions in the decomposition.

Definition 3.6. [Barwick, 2016] Let $\sigma \in S_n$. We can express a permutation very compactly,

by writing down the $n \times n$ matrix

$$P_\sigma = (\hat{e}_{\sigma(1)}, \cdots, \hat{e}_{\sigma(n)})$$

called the permutation matrix corresponding to σ and the vector $\hat{e}_i$ is standard unit vector.

Remark 14. [Barwick, 2016] The determinant of a permutation matrix P_σ is called the sign of the permutation σ

$$\operatorname{sgn}(\sigma) = \det(P_\sigma).$$

Lemma 3.7. *(Vandermonde determinant)[Smith, 2021] For any non-negative integer n, we have*

$$\det(\mathbf{V}_n) = \prod_{j=1}^{n-1} \left(\prod_{k=j+1}^{n} (x_k - x_j) \right) = \prod_{1 \leqslant j < k \leqslant n} (x_k - x_j),$$

where

$$\mathbf{V}_n := \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{bmatrix}.$$

The next proposition expresses the determinant of a square matrix in terms of permutations of the matrix entries.

Proposition 3.8. *Let P_σ be a permutation matrix, $\sigma \in S_n$ and V_n be a Vandermonde determinant then we have*

$$\operatorname{sgn}(\sigma) \prod_{1 \leqslant j < k \leqslant n} (x_{\sigma(k)} - x_{\sigma(j)}) = \prod_{1 \leqslant j < k \leqslant n} (x_k - x_j).$$

Proof. We know that the determinant of the product of square matrices is equal to the

product of their determinants. Therefore by Remark 14 and Lemma 3.7, we have:

$$\det(\mathbf{V}_n \cdot P_\sigma) = \det \mathbf{V}_n \cdot \det P_\sigma = \prod_{1 \leqslant j < k \leqslant n} \left(x_k - x_j\right) \operatorname{sgn}(\sigma).$$

On the other hand $\mathbf{V}_n \cdot P_\sigma$ is represented by $\mathbf{V}_n \cdot P_\sigma(I_n)$ where I_n is the identity matrix. It means that $P_\sigma(I_n)$ just reorders the columns of matrix $\mathbf{V}_n$. We denote the columns of matrix $\mathbf{V}_n$ by $\vec{X}_i$ where i is the number of column, so $\mathbf{V}_n$ is represented by $[\vec{X}_1 \vec{X}_2 \cdots \vec{X}_n]$ and we have

$$\mathbf{V}_n \cdot P_\sigma = [\vec{X}_1 \vec{X}_2 \cdots \vec{X}_n] \begin{bmatrix} \hat{e}_{\sigma(1)} \\ \hat{e}_{\sigma(2)} \\ \vdots \\ \hat{e}_{\sigma(n)} \end{bmatrix} = [\vec{X_{\sigma(1)}} \vec{X_{\sigma(2)}} \cdots \vec{X_{\sigma(n)}}] = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_{\sigma(1)} & x_{\sigma(2)} & \cdots & x_{\sigma(n)} \\ x_{\sigma(1)}^2 & x_{\sigma(2)}^2 & \cdots & x_{\sigma(n)}^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_{\sigma(1)}^{n-1} & x_{\sigma(2)}^{n-1} & \cdots & x_{\sigma(n)}^{n-1} \end{bmatrix}.$$

Therefore, $\det(\mathbf{V}_n \cdot P_\sigma) = \prod_{1 \leqslant j < k \leqslant n} \left(x_{\sigma(k)} - x_{\sigma(j)}\right)$ and we get the result. □

The following definitions are given in [Cox, 2011b], with some modifications.

Definition 3.9. Let $F \subset L$ be a finite extension. Then $Gal(L/F)$ is the set

$$\{\sigma : L \to L \mid \sigma \text{ is an automorphism }, \sigma(a) = a \text{ for all } a \in F\}.$$

In other words, $Gal(L/F)$ consists of all automorphisms of L that are the identity on F.

Fact. There exists a root α of polynomial $f(x)$ that is also a root of polynomial $g(x)$ if and only if $(x-\alpha) \mid f(x)$ and $(x-\alpha) \mid g(x)$. In the other words, $\gcd(f(x), g(x)) > 1$.

The following Lemma and Lemma 3.11 are standard and well-known results in number theory.

Lemma 3.10. *If p is prime, and $P(x) \in \mathbb{F}_p[x]$ then $P(x) \mid P(x^p)$.*

Proof. Define $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where $a_i \in \mathbb{F}_p$. We know that the equation $x^p \equiv x$ has p roots in $\mathbb{F}_p$ by theorem 2.1.

Let $P(x^p) = (x^p)^n + a_{n-1}(x^p)^{n-1} + \cdots + a_0$. Since $P(x^p) \in \mathbb{F}_p[x]$, we have

$$P(x^p) = (x^n + a_{n-1}x^{n-1} + \cdots + a_0)^p.$$

Using that $(x+y)^p = x^p + y^p$ in $\mathbb{F}_p$ because of $p \mid \binom{k}{p}$ for $k = 1, \cdots, p-1$. Thus, $P(x^p) = (P(x))^p$ and we get the result that $P(x) \mid P(x^p)$. □

Lemma 3.11. *If p is prime, and $P(x) \in \mathbb{F}_p[x]$ then $P(x) \mid (x^{p^{d!}} - x)$.*

Proof. By Lemma 2.14, we can rewrite the polynomial $x^{p^{d!}} - x$ over $\mathbb{F}_p$ as

$$x^{p^{d!}} - x = \prod_{\substack{\deg(g(x))=i \\ i \mid d! \\ g(x) \text{ is irr poly}}} g(x) \qquad (\text{mod } p).$$

Since, $P(x) \mid \prod_{\substack{\deg(g(x))=i \\ i \mid d! \\ g(x) \text{ is irr poly}}} g(x) \mid x^{p^{d!}} - x$ modulo p, then $P(x) \mid x^{p^{d!}} - x$. □

Lemma 3.12. *Let $P(x) \in F[x]$ and $m \in \mathbb{N}$, then $P(x) \mid P(x^m)$ if and only if $\phi(M) \subseteq M$.*

Proof. ($\Longleftarrow$) Let $m \in \mathbb{N}$ and a polynomial $P(x) \in F[x]$. Thus

$$P(x) = \prod_{i=1}^{d}(x - \alpha_i), \text{ and } P(x^m) = \prod_{i=1}^{d}(x^m - \alpha_i),$$

where $\alpha_i \in F$. Assuming $\phi(M) \subseteq M$ then

$$\forall i \in \{1,\cdots,n\}, \exists j \in \{1,\cdots,n\} \text{ s.t } \alpha_i^m = \alpha_j. \tag{3.1}$$

Consider $\alpha_t \in M$ so

$$P(\alpha_t^m) = \prod_{i=1}^{d} (\alpha_t^m - \alpha_i).$$

By equation (3.1), there exists at least one $\alpha_i \in M$ such that $\alpha_t^m = \alpha_i$. Hence, we have $\alpha_t^m - \alpha_i = 0$, and $P(\alpha_t^m) = 0$. Since $P(x)$ has no repeated roots we conclude that all roots of $P(x)$ are roots of $P(x^m)$. Thus, $P(x) \mid P(x^m)$.

($\Longrightarrow$) Assuming $P(x) \mid P(x^m)$. Thus we have

$$\exists h(x) \in F[x] \text{ s.t } P(x) \cdot h(x) = P(x^m).$$

Means that for all $\alpha_i \in M$ we have $P(\alpha_i^m) = P(\alpha_i)h(\alpha_i) = 0$. Thus there is at least one $\alpha_t \in M$ such that $\alpha_i^m - \alpha_t = 0$, or $\alpha_i^m = \alpha_t$. Thus $\phi(M) \subseteq M$. □

Lemma 3.13. *Assume $\phi(M) \subset M$ then the map $\phi : M \to M$ is bijective if and only if for some $i \in \mathbb{N}$, $P(x) \mid (x^{m^i} - x)$.*

Proof. ($\Longleftarrow$) Assuming for some $i \in \mathbb{N}$, $P(x)$ divides $(x^{m^i} - x)$, thus for all $\alpha_j \in M$, we have

$$\alpha_j^{m^i} - \alpha_j = 0 \text{ or } \phi^i(\alpha_j) = \alpha_j^{m^i} = \alpha_j.$$

Means that for all $\alpha_j \in M$ we have $\phi^i = \text{Id}$. Hence, ϕ has an inverse ϕ^{i-1}. So the map ϕ is bijective.

($\Longrightarrow$) In this part, we want to show that if map ϕ is bijective then there exists at least one $i > 0$ such that $P(x) \mid x^{m^i} - x$. Since the map ϕ is bijective then it is also a permutation map. So it can be written in terms of cycles, and each root of polynomial $P(x)$ is in one cycle.

Consider the following cycles of roots of a polynomial $P(x)$, where $s_1, \cdots, s_d$ are the

order of $\phi(\alpha_1), \cdots, \phi(\alpha_d)$ respectively.

$$\alpha_1 \xrightarrow{\phi} \alpha_1^m \xrightarrow{\phi} \alpha_1^{m^2} \xrightarrow{\phi} \alpha_1^{m^3} \cdots \xrightarrow{\phi} \alpha_1^{m^{s_1}} = \alpha_1,$$

$$\alpha_2 \xrightarrow{\phi} \alpha_2^m \xrightarrow{\phi} \alpha_2^{m^2} \xrightarrow{\phi} \alpha_2^{m^3} \cdots \xrightarrow{\phi} \alpha_2^{m^{s_2}} = \alpha_2,$$

$$\vdots$$

$$\alpha_d \xrightarrow{\phi} \alpha_d^m \xrightarrow{\phi} \alpha_d^{m^2} \xrightarrow{\phi} \alpha_d^{m^3} \cdots \xrightarrow{\phi} \alpha_d^{m^{s_d}} = \alpha_d.$$

So for each cycle we have

$$\forall \alpha_j \in M, \phi^{s_j}(\alpha_j) = \alpha_j.$$

Consider the integer $S = \text{lcm}(s_1, \ldots, s_n)$. We will show that S is the desired integer such that $P(x) \mid (x^{m^S} - x)$. We know $s_j \mid S$ means that there exists $k_j \in \mathbb{N}$ such that $s_j k_j = S$. By the following k_j-cycle of α_j

$$\underbrace{\alpha_j \xrightarrow{\phi^{s_j}} \alpha_j \xrightarrow{\phi^{s_j}} \alpha_j \xrightarrow{\phi^{s_j}} \cdots \xrightarrow{\phi^{s_j}} \alpha_j}_{k_j \text{ times}},$$

we find that $\phi^{s_j k_j}(\alpha_j) = \phi^S(\alpha_j) = \alpha_j$, or $\alpha_j^{m^S} - \alpha_j = 0$. Since these expression are true for all roots of polynomial $P(x)$ then we have $P(x) \mid x^{m^S} - x$. □

Corollary 3.14. *The map ϕ acts as a permutation of the roots of $P(x)$ if and only if $P(x) | P(x^m)$ and $P(x) | x^{m^{d!}} - x$.*

Lemma 3.15. *Assume ϕ permutes the roots of $P(x)$. If $d \in \mathbb{N}$ and the permutation ϕ has a d-cycle, then* $\gcd(P(x), x^{m^d} - x) > 1$.

Proof. The assumption that ϕ has a d-cycle implies that there exists $\alpha_j \in M$ such that

$\phi^d(\alpha_j) = \alpha_j$ i.e $\alpha_j^{m^d} = \alpha_j$. So $x - \alpha_j \mid x^{m^d} - x$. As $\alpha_j \in M$ implies that $x - \alpha_j \mid P(x)$. Therefore $\gcd(P(x), x^{m^d} - x) > 1$. □

Lemma 3.16. *Assume ϕ permutes the roots of $P(x)$. If $\gcd(P(x), x^{m^d} - x) > 1$ then the permutation ϕ has an i-cycle with $i \mid d$.*

Proof. The assumption $\gcd(P(x), x^{m^d} - x) > 1$ gives that there exists a root α_j of $P(x)$ such that $x - \alpha_j \mid x^{m^d} - x$. So $\alpha_j^{m^d} = \alpha_j$. On the other hand, $(\alpha_j)^{\mathrm{ord}(\alpha_j)} = \alpha_j$ means that, we have $\mathrm{ord}(\alpha_j)$-cycle; $(\alpha_j, \phi(\alpha_j), \cdots, \phi^{\mathrm{ord}(\alpha_j)-1})$. Thus $\mathrm{ord}(\alpha_j) \mid d$ by Lagrange's theorem. □

Lemma 3.17. *Assume ϕ permutes the roots of $P(x)$ and let $d \in \mathbb{N}$. Suppose $P(x) \mid x^{m^d} - x$ and for all $i \mid d$ with $i \neq d$ we have $gcd(P(x), x^{m^i} - x) = 1$ then the permutation ϕ is a product of disjoint d-cycles.*

Proof. By the assumption, for $i = d$ we know $P(x) \mid x^{m^d} - x$ which implies that for all $\alpha_j \in M$, $\alpha_j^{m^d} = \alpha_j$, i.e $\phi^d(\alpha_j) = \alpha_j$. So, all of the cycles in σ have orders dividing d.

We know that, for all $i \mid d$ and $i \neq d$, $\gcd(P(x), x^{m^i} - x) = 1$. It follows that if α_j is a root of $P(x)$ then it is not a root of $x^{m^d} - x$, i.e $\alpha_j^{m^i} \neq \alpha_j$, thus $\phi^i(\alpha_j) \neq \alpha_j$. Hence, the cycles must all have a length of exactly d. □

Lemma 3.18. *If $F_i(x)$ is defined and satisfies the Factorization and Frobenius steps as in Definition 2.24 then the map ϕ permutes the roots of $F_i(x)$ modulo p for each $p|n$ as a product of $\frac{\deg F_i(x)}{i}$ disjoint i-cycles.*

Proof. From our hypothesis we have

$$F_i(x) | x^{m^i} - x \pmod{n} \quad \text{and} \quad \gcd(F_i(x), x^{m^j} - x) = 1 \pmod{n} \quad j < i.$$

Thus this also holds for each $p|n$. So by Lemma 3.17 the permutation is a product of disjoint i-cycles. We conclude the number of $i-$cycles is equal to $\frac{\deg F_i(x)}{i}$. □

Lemma 3.19. *Suppose as in Definition 2.24, we have* $f_d(x) = 1 \pmod n$ *and* $f(x)|f(x^n) \pmod n$, *that is the Factorization and Frobenius conditions are satisfied. Then* ϕ *permutes the roots of* $f(x)$ *modulo* p *for each* $p|n$ *and the sign of the permutation* ϕ *is* $(-1)^S$, *where* S *is as defined by Grantham in Definition 2.24.*

Proof. For each $1 \leq i \leq d$, we replace $f_{i-1}(x)$ in Factorization step of Definition 2.24 with $P_{i-1}(x)$ and define $F_i(x) = \gcd\left(x^{m^i} - x, P_{i-1}(x)\right)$. By Lemma 3.18 we know that the number of $i-$cycles is equal to $\frac{\deg F_i(x)}{i}$. So referring to Definition 3.5, we find that the sign of the permutation is determined by its odd cycles which by Remark 13 means we we need to count the even length permutations. Then we have

$$| \{i-\text{cycles}, 2 \mid i\} | = \sum_{2|i} \frac{\deg F_i(x)}{i}.$$

Note that in Jacobi step of Definition 2.24 we have $S = \sum_{2|i} \frac{\deg F_i(x)}{i}$. Thus

$$| \{i-\text{cycles}, 2 \mid i\} | = S.$$ □

Proposition 3.20. *[Cox, 2011b, Proposition 2.4.1] If* $\sigma \in S_n$, *then*

$$\sigma \cdot \sqrt{\Delta} = \text{sgn}(\sigma)\sqrt{\Delta},$$

where $\text{sgn}(\sigma)$ *is the sign of* σ *defined in Definition 3.5, and* $\sigma \cdot \sqrt{\Delta}$ *is the polynomial obtained from* $\sqrt{\Delta}$ *by permuting the variables* $x_1, \cdots, x_n$ *according to* σ.

Lemma 3.21. *Let* $\alpha_1, ..., \alpha_d$ *be the roots of polynomial* $P(x)$ *(in any order). Consider the*

Vandermonde determinants

$$M_1 = (-1)^{d(d-1)/2} \prod_{1\le i<j\le d} (\alpha_i - \alpha_j), \text{ and } M_2 = (-1)^{d(d-1)/2} \prod_{1\le i<j\le d} (\alpha_i^m - \alpha_j^m).$$

Then the sign of the permutation ϕ *is* M_1/M_2, *and* $M_1^2 = M_2^2 = \Delta_{P(x)}$.

Proof. We rewrite M_2 using the permutation ϕ and Proposition 3.8 then we have

$$\begin{aligned} M_2 &= (-1)^{d(d-1)/2} \prod_{1\le i<j\le d} (\alpha_i^m - \alpha_j^m) \\ &= (-1)^{d(d-1)/2} \prod_{1\le i<j\le d} (\phi(\alpha_i) - \phi(\alpha_j)) \\ &= (-1)^{d(d-1)/2} \mathrm{sgn}(\phi) \prod_{1\le i<j\le d} (\alpha_i - \alpha_j) \\ &= \mathrm{sgn}(\phi) M_1. \end{aligned}$$

Thus the sign of permutation σ is obtained by

$$\frac{M_1}{M_2} = \mathrm{sgn}(\phi).$$

In addition, as σ is a bijection map on the roots of polynomial $P(x)$, thus we have that $M_1 = (-1)^{\frac{d(d-1)}{2}}\sqrt{\Delta}$. Then $M_1^2 = M_2^2 = \Delta$. □

The following lemma comes from the second part of [Cox, 2011b, Proposition 7.4.1] with a few changes.

Lemma 3.22. *Let* $\Delta_{P(x)}$ *and* $\left(\frac{\Delta_{P(x)}}{p}\right)$ *are not equal to zero. If* σ *is in* $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$, *and* M_1 *is in* $\mathbb{F}_p$ *then* $\mathrm{sgn}(\sigma) = 1$.

Proof. The permutation $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$, where $\sigma(\mathbb{F}_p) = \mathbb{F}_p$. By assumption $M_1 \in \mathbb{F}_p$ and referring to Lemma 3.21 we have $M_1 = \sqrt{\Delta_{P(x)}} \in \mathbb{F}_p$. So by Proposition 3.20, for all

$\sigma \in Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ we have

$$\begin{aligned}\sqrt{\Delta_{P(x)}} \in \mathbb{F}_p &\iff \sigma \cdot \sqrt{\Delta_{P(x)}} = \sqrt{\Delta_{P(x)}} \\ &\iff \operatorname{sgn}(\sigma)\sqrt{\Delta_{P(x)}} = \sqrt{\Delta_{P(x)}},\end{aligned}$$

since $\Delta_{P(x)} \neq 0$ then $\operatorname{sgn}(\sigma) = 1$. □

Corollary 3.23. *If $M_1 \notin \mathbb{F}_p$ then there exists σ in $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ such that* $\operatorname{sgn}(\sigma) = -1$.

Proof. By Proposition 3.20 and Lemma 3.22, there exists $\sigma \in Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ such that

$$\sigma \cdot \sqrt{\Delta_{P(x)}} = \operatorname{sgn}(\sigma)\sqrt{\Delta_{P(x)}} \neq \sqrt{\Delta_{P(x)}},$$

so $\operatorname{sgn}(\sigma) = -1$. □

Lemma 3.24. *Let p be prime and $\left(\frac{\Delta_{P(x)}}{p}\right) \neq 0$. Referring to Lemma 3.19 then we have* $(-1)^S = \left(\frac{\Delta_{P(x)}}{p}\right)$.

Proof. Similar to Definition 1.11 we have

$$\left(\frac{\Delta_{P(x)}}{p}\right) = \begin{cases} 1 & \text{if } \Delta_{P(x)} \equiv x^2 \pmod{p}, \\ -1 & \text{if } \Delta_{P(x)} \not\equiv x^2 \pmod{p}, \\ 0 & \text{if } p \mid \Delta_{P(x)}. \end{cases}$$

In the first case, $\Delta_{P(x)}$ is a square in $\mathbb{F}_p$ means that $\sqrt{\Delta_{P(x)}} \in \mathbb{F}_p$. So by Lemma 3.22 we have $\operatorname{sgn}(\sigma) = 1$. For the second case, $\Delta_{P(x)}$ is not a square in $\mathbb{F}_p$ means that $\sqrt{\Delta_{P(x)}} \notin \mathbb{F}_p$. So by Lemma 3.23 we have $\operatorname{sgn}(\sigma) = -1$. So in these two cases, we find that $\left(\frac{\Delta_{P(x)}}{p}\right) = \operatorname{sgn}(\sigma)$. On the other hand, by Lemma 3.19, we know $\operatorname{sgn}(\sigma) = (-1)^S$. As we know the third case never happens because of the assumption so we have $(-1)^S = \left(\frac{\Delta_{P(x)}}{p}\right)$. □

Lemma 3.25. *Suppose $P(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ and $p \mid m$. Then for all $r \in \mathbb{N}$ and unique polynomial $P_r(x) \in (\mathbb{Z}/p^r\mathbb{Z})[x]$ such that $P_r(x) = P(x) \pmod{p}$ where ϕ permutes the roots of $P_r(x)$.*

Proof. By Lemma 3.13, we know that for some integer $i > 0$ we have $P(x) \mid x^{m^i} - x$. Then there exists a polynomial $Q(x)$ over $\mathbb{Z}/p\mathbb{Z}$ such that $x^{m^i} - x = P(x)Q(x)$. So all roots of $P(x)$ are also roots of $x^{m^i} - x$. Since $p \mid m$, then $m^i x^{m^i-1} - 1 \not\equiv 0 \pmod{p}$. So $\gcd(x^{m^i} - x, m^i x^{m^i-1} - 1) = 1$.

Now by Hensel's Lemma, let r be a positive integer. We know that if $P(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ and $\alpha \in \mathbb{Z}/p\mathbb{Z}$ which satisfies $P(\alpha) \equiv 0 \pmod{p}$, and $P'(\alpha) \not\equiv 0 \pmod{p}$ then there is a unique $\alpha' \in \mathbb{Z}/p^r\mathbb{Z}$ such that $f(\alpha') \equiv 0 \pmod{p^r}$ and $\alpha' \equiv \alpha \pmod{p}$. In this case, we apply the Hensel's Lemma to the polynomial $x^{m^i} - x$. Then we get that there is the set of the roots of the polynomial $x^{m^i} - x$ over $\mathbb{Z}/p^r\mathbb{Z}$ that is denoted by M' is equal to $M' = \{\alpha'_j \text{ s.t } \alpha'_j = \alpha_j + tp^r \text{ for all } \alpha_j \in M\}$ where $t \in \{0, 1, \cdots, p-1\}$ such that t to be unique for each α_j. So for all $\alpha'_j \in M'$ we have $\alpha_j \equiv \alpha'_j \pmod{p^r}$ or $\alpha_j \equiv \alpha'_j \pmod{p}$. By the roots α'_j, we can construct the polynomial $P_r(x) = \prod_{\alpha'_j \in M'}(x - \alpha'_j)$ over $\mathbb{Z}/p^r\mathbb{Z}$ such that $P_r(x) \mid x^{m^i} - x$ over $\mathbb{Z}/p^r\mathbb{Z}$.

Now because ϕ permutes the roots of $x^{m^i} - x$ modulo p^r with the same cycle structure as it does modulo p so ϕ must permute the roots of $P_r(x)$ with the same cycle structure as $P(x)$. Hence, by applying Hensel Lemma to polynomial $x^{m^i} - x$ we found the desired polynomial, $P_r(x)$. □

By Lemma 3.25, Lemma 3.19 and the Definition 2.16, we can reinterpret Theorem 2.18 for all prime p where $p^r \mid n$.

The forward direction is from [Grantham, 2001, Proposition 3.2].

Proposition 3.26. *Let $g_1(x), g_2(x)$ be monic polynomials in $\mathbb{Z}[x]$. Then*

$$f(x) \equiv \operatorname{gcmd}(g_1(x), g_2(x)) \pmod{n},$$

where the gcmd is taken in $(\mathbb{Z}/n\mathbb{Z})[x]$ if and only if

$$f(x) \equiv \operatorname{gcmd}(g_1(x), g_2(x)) \pmod{p^r},$$

for all $p^r || n$ where the gcmd is taken in $(\mathbb{Z}/p^r\mathbb{Z})[x]$, and $f(x) \pmod{p^r}$ are all monic and have the same degree.

Proof. For forward direction, since $f(x) = \operatorname{gcmd}(g_1(x), g_2(x)) \pmod{n}$ for $i = 1, 2$ we have

$$g_i(x) \equiv k_i(x) f(x) \pmod{n},$$

for $k_i(x) \in \mathbb{Z}[x]$. Thus $f(x) \mid g_i(x)$ in $(\mathbb{Z}/p^r\mathbb{Z})[x]$.
We have that $f(x) \equiv g_1(x)h_1(x) + g_2(x)h_2(x) \pmod{n}$ for $h_1(x), h_2(x) \in \mathbb{Z}[x]$. Thus $f(x) \equiv g_1(x)h_1(x) + g_2(x)h_2(x) \pmod{p^r}$, and by the definition of gcd, $f(x) = \gcd(g_1(x), g_2(x))$ in $(\mathbb{Z}/p^r\mathbb{Z})[x]$.

For the inverse direction, for each $p^r || n$, $\gcd(g_1(x), g_2(x)) = f(x) \pmod{p^r}$. For $i = 1, 2$ there exist $k_i'(x) \in (\mathbb{Z}/p^r\mathbb{Z})[x]$ such that $g_i(x) \equiv k_i'(x) f(x) \pmod{p^r}$. Additionally, there exist $h_1'(x)$, $h_2'(x)$ in $(\mathbb{Z}/p^r\mathbb{Z})[x]$ such that $f(x) \equiv g_1(x)h_1'(x) + g_2(x)h_2'(x) \pmod{p^r}$. Then by the Chinese Remainder Theorem there exist $k_i(x)$, $h_i(x)$ such that $g_i(x) \equiv k_i(x) f(x) \pmod{n}$ and $f(x) \equiv g_1(x)h_1(x) + g_2(x)h_2(x) \pmod{n}$. Then because $f(x) \pmod{p^r}$ are all monic and the same degree, $f(x) \pmod{n}$ is monic, hence is the gcmd. □

Corollary 3.27. *[Grantham, 2001, Corollary 3.3] If the $\operatorname{gcmd}(g_1(x), g_2(x)) \pmod{n}$ when computed in $(\mathbb{Z}/n\mathbb{Z})[x]$, then for all p dividing n, $\gcd(g_1(x), g_2(x)) \pmod{p}$ have the same degree.*

Reminder. The cycle structure σ refers to the numbers $\frac{deg F_i(x)}{i}$ as mentioned in Definition 2.27.

Remark 15. In Lemma 3.19, we found that the cycle structure of σ corresponds to the degrees of polynomials $F_i(x)$ in Grantham's definition 2.24.

In the following theorem by referring to Remark 15, we are going to reinterpret Theorem 2.18 in $(\mathbb{Z}/p^r\mathbb{Z})[x]$ with respect to the cycle structure of σ.

Theorem 3.28. *$(f(x),n)$ is a Frobenius pseudoprime with cycle structure σ if and only if for all primes $p, p^r||n$ we have*

1. *map $x \to x^n$ permutes roots of $f(x)$ mod p^r with cycle structure σ,*
2. *$\left(\frac{\Delta}{n}\right) = \text{sgn}(\sigma)$, and*
3. *The Euclidean algorithm does not accidentally find a factor of n.*

Proof. $\Longrightarrow$:
If $(f(x),n)$ is a Frobenius pseudoprime, then from the Factorization and Frobenius steps of Definition 2.24, which are

$$F_i(x) \mid x^{n^i} - x, \text{ and } F_i(x) \mid F_i(x^n) \pmod{n}.$$

The CRT implies that these divisibilities hold for each $p^r||n$. By Remark 10, $f(x) = F_1(x)\cdots F_d(x) \pmod{n}$, so by CRT again this also holds modulo p^r. Now, by Lemma 3.12 and 3.13, the map ϕ acts as a permutation of the roots of $F_i(x)$ modulo p^r. So by Lemma 3.18, the map ϕ permutes the roots of $f(x) \pmod{p^r}$ with the desired cycle structure. The third condition of this theorem holds immediately from Factorization step of Definition 2.24. In this step, the polynomials $F_i(x)$ exist if all gcmd exist, and the Euclidean algorithm does not find the factor of n, as specified by Proposition 2.22.

Finally, the Jacobi step in Definition 2.24 and Lemma 3.19 prove the second condition here, that is $\left(\frac{\Delta}{n}\right) = (-1)^S = \text{sgn}(\sigma)$, where S is defined in Definition 2.24.

$\Longleftarrow$:

The map ϕ is a permutation map and permutes the roots of polynomial $f(x)$ modulo p^r. So, we can define polynomials $G_i(x)$ by

$$G_i(x) = \prod_{\alpha_i}(x-\alpha_i), \tag{3.2}$$

where α_i are the root of $f(x)$ with $\text{ord}(\alpha_i) = i$. By this fact, we have

$$G_i(x) \mid x^{n^i} - x, \pmod{p^r} \text{ and } \text{gcmd}(G_i(x), x^{n^j} - x) = 1 \pmod{p^r} \quad j < i. \tag{3.3}$$

Now, we will prove by induction that $G_i(x) \equiv F_i(x) \pmod{p^r}$ and $f_{i-1}(x) \equiv G_i(x)\cdots G_d(x) \pmod{p^r}$ for all $i \in \{1,\cdots,d\}$, where $F_i(x)$ and $f_i(x)$ are as defined in Definition 2.24. We will also establish that $\text{gcmd}(f_{i-1}(x), x^{n^i} - x) \pmod{n}$ exists.

For $i = 1$, by the definition 2.24 and equality (3.2), we have

$$F_1(x) = \text{gcmd}(x^n - x, f_0(x)) = \text{gcmd}(x^n - x, f(x)) = \prod_{ord(\alpha_i)=1}(x-\alpha_i) = G_1(x).$$

So $F_1(x) \equiv G_1(x) \pmod{p^r}$. Also, since $f(x)$ does not have a repeated root then we have $f_0(x) \equiv G_1(x)\cdots G_d(x) \equiv f(x) \pmod{p^r}$.

The induction hypothesis is, for $i-1 = k$, we have $F_{k+1}(x) \equiv G_{k+1}(x) \pmod{p^r}$, and $f_k(x) \equiv G_{k+1}(x)\cdots G_d(x) \pmod{p^r}$. Now we are going to prove that these hold for $i-1 = k+1$ modulo p^r. Using the induction hypothesis and Definition 2.24, we have

$$f_{k+1}(x) \equiv \frac{f_k(x)}{F_{k+1}(x)} \equiv \frac{G_{k+1}(x)\cdots G_d(x)}{G_{k+1}(x)} \equiv G_{k+2}(x)\cdots G_d(x) \pmod{p^r}.$$

For the claim about $F_{k+2}(x)$, we have using equation (3.3) that

$$\text{gcmd}(x^{n^{k+2}} - x, f_{k+1}(x)) \equiv \text{gcmd}(x^{n^{k+2}} - x, G_{k+2}(x) \cdots G_d(x)) \equiv G_{k+2}(x) \pmod{p^r}.$$

So, for all $i \in \{1, \cdots, d\}$, we have $G_i(x) \equiv F_i(x) \pmod{p^r}$ and $f_{i-1}(x) \equiv G_i(x) \cdots G_d(x) \pmod{p^r}$. Because $G_i(x) \equiv \gcd(x^{n^i} - x, f_{i-1}) \pmod{p^r}$, and the $G_i(x)$ all have the same degree by the CRT and reverse direction of Proposition 3.26, the gcmd exists modulo n and we have $G_i(x) = F_i(x) \pmod{n}$. Thus $f_i(x) = \frac{f_{i-1}(x)}{F_i(x)} = \frac{f_{i-1}(x)}{G_i(x)} = G_{i+1}(x) \cdots G_d(x) \pmod{n}$. It follows from the above and the third assumption that the Factorization step of the Grantham's algorithm will complete and we will have $f_d(x) = 1$.

For Frobenius step, we know $F_i(x) = G_i(x)$ and $G_i(x) | G_i(x^n) \pmod{p^r}$ for all $p^r | n$, then by Chinese Remainder Theorem, $G_i(x) | G_i(x^n) \pmod{n}$ which gives the result.
For the Jacobi step of Grantham's algorithm, we apply Lemma 3.19 to $f(x)$. □

We need the third condition of Theorem 3.28 because of Proposition 2.22.
In the next chapter, we will focus on using this interpretation to count the number of Frobenius liar pairs (f, n) that only satisfy the first and second conditions in Theorem 3.28, and we will ignore the third condition.

Chapter 4

The Number Of Degree-3 Polynomials $f(x)$ Over $(\mathbb{Z}/p^r\mathbb{Z})$ For Which n Is A Cubic Frobenius Pseudoprime At p

In Chapter 2, we mentioned that Fiori and Shallue worked on the quadratic Frobenius pseudoprimes and liars [Fiori and Shallue, 2020]. They denote by $L_2(n)$ the number of Frobenius liars of degree 2 with respect to n and divided $L_2(n)$ into $L_2^+(n)$ and $L_2^-(n)$ with respect to the Legendre symbol $\left(\frac{\Delta}{n}\right) = \pm 1$. In this Chapter, we denote the number of Frobenius liars of degree 3 with respect to n by $L_3(n)$. By Theorem 3.28, we see that for the general form of Frobenius pseudoprime, we can use the reinterpreted form of Grantham Theorem. This means, here, in cubic Frobenius pseudoprime, we comprehend the different types of the cycle structures of permutation σ which corresponds to the different factorization structures of polynomials $F_1(x), F_2(x)$ and $F_3(x)$ in $(\mathbb{Z}/n\mathbb{Z})[x]$.

Note that if (f,n) is a liar pair, and $f(x)$ be a cubic polynomial thus by Remark 10, it can be written as $f(x) = F_1(x)F_2(x)F_3(x)$ such that $3 \mid \deg(F_3(x))$ and $2 \mid \deg(F_2(x))$. This leads to the following possibilities.

Lemma 4.1. *If n is a Frobenius pseudoprime for cubic polynomial $f(x)$ then either:*

1. *$f(x) = F_3(x)$ with $F_3(x)$ a cubic polynomial and $F_1(x) = F_2(x) = 1$,*

2. $f(x) = F_1(x)F_2(x)$ *with* $F_1(x)$ *a linear polynomial,* $F_2(x)$ *a quadratic polynomial and* $F_3(x) = 1$, *or*

3. $f(x) = F_1(x)$ *with* $F_1(x)$ *a cubic polynomial and* $F_2(x) = F_3(x) = 1$.

Remark 16. If n is a Frobenius pseudoprime for a cubic polynomial $f(x)$ then

1. The cases $f(x) = F_3(x)$ and $f(x) = F_1(x)$ correspond to $\left(\frac{\Delta}{n}\right) = 1$.

2. The case $f(x) = F_1(x)F_2(x)$ corresponds to $\left(\frac{\Delta}{n}\right) = -1$.

Definition 4.2. Let $f(x)$ be a polynomial in $(\mathbb{Z}/n\mathbb{Z})[x]$. We say a Frobenuis pseudoprime (f,n) with cycle structure σ modulo p has a factorization structure $\mathbb{F}_{p^{d_1}} \times \cdots \times \mathbb{F}_{p^{d_r}}$ if the roots of f (ordered relative to the action of σ) are in $\mathbb{F}_{p^{d_i}}$.

Remark 17. Note that we need to split the cases by factorization modulo p so we consider the factorization of $f(x)$ either

1. splits completely if all the three roots are in $\mathbb{F}_p$,

2. splits partially if one of the roots is in $\mathbb{F}_{p^2}$, or

3. is irreducible if all the three roots are in $\mathbb{F}_{p^3}$.

By augmenting the Chinese Remainder Theorem and recalling Lemma 3.25, for counting cubic Frobenius pseudoprimes (f,n) we can work with $(\mathbb{Z}/p\mathbb{Z})[x]$ for each $p^r \mid n$, instead of $(\mathbb{Z}/n\mathbb{Z})[x]$. Here, we focus on different cycle structures and the factorization structures of the roots of $f(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$.

The $F_i(x)$ indicates the cycle structure of roots of $f(x)$ and the subscript $\mathbb{F}_{p^j}$ on the superscript $F_i(x)$ indicates the factorization of $f(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$. Consequently, we have the following structures.

Definition 4.3. If n is a cubic Frobenius pseudoprime, then for each $p \mid n$ we have eight possible options for combination of cycle structures and factorization structures for $f(x)$. To count the number of polynomials $f(x)$ over $(\mathbb{Z}/n\mathbb{Z})[x]$, that satisfy the first condition of Theorem 3.28, we consider the following cases for each option:

1. Where $f(x) \equiv F_1(x) \pmod{p}$ and $F_1(x)$ splits completely over $(\mathbb{Z}/p\mathbb{Z})$. We denote by $L_3^{F_1(x)_{\mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p}}(n,p)$ the number of polynomials over $(\mathbb{Z}/p\mathbb{Z})$ that split completely which σ permutes the roots of $f(x) \pmod{p}$ with cycle structure of type $F_1(x)$.

2. Where $f(x) \equiv F_1(x) \pmod{p}$ and $F_1(x)$ splits partially over $(\mathbb{Z}/p\mathbb{Z})$. We denote by $L_3^{F_1(x)_{\mathbb{F}_p \times \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}}}(n,p)$ the number of polynomials over $(\mathbb{Z}/p\mathbb{Z})$ that split partially which σ permutes the roots of $f(x) \pmod{p}$ with cycle structure of type $F_1(x)$.

3. Where $f(x) \equiv F_1(x) \pmod{p}$ and $F_1(x)$ is irreducible over $(\mathbb{Z}/p\mathbb{Z})$. We denote by $L_3^{F_1(x)_{\mathbb{F}_{p^3} \times \mathbb{F}_{p^3} \times \mathbb{F}_{p^3}}}(n,p)$ the number of polynomials over $(\mathbb{Z}/p\mathbb{Z})$ that is irreducible which σ permutes the roots of $f(x) \pmod{p}$ with cycle structure of type $F_1(x)$.

4. Where $f(x) \equiv F_3(x) \pmod{p}$ and $F_3(x)$ splits completely over $(\mathbb{Z}/p\mathbb{Z})$. We denote by $L_3^{F_3(x)_{\mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p}}(n,p)$ the number of polynomials over $(\mathbb{Z}/p\mathbb{Z})$ that splits completely which σ permutes the roots of $f(x) \pmod{p}$ with cycle structure of type $F_3(x)$.

5. Where $f(x) \equiv F_3(x) \pmod{p}$ and $F_3(x)$ splits partially over $(\mathbb{Z}/p\mathbb{Z})$. We denote by $L^{F_3(x)_{\mathbb{F}_p \times \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}}}(n,p)$ the number of polynomials over $(\mathbb{Z}/p\mathbb{Z})$ that splits partially which σ permutes the roots of $f(x) \pmod{p}$ with cycle structure of type $F_3(x)$.

6. Where $f(x) \equiv F_3(x) \pmod{p}$ and $F_3(x)$ is irreducible over $(\mathbb{Z}/p\mathbb{Z})$. We denote by $L_3^{F_3(x)_{\mathbb{F}_{p^3} \times \mathbb{F}_{p^3} \times \mathbb{F}_{p^3}}}(n,p)$ the number of polynomials over $(\mathbb{Z}/p\mathbb{Z})$ that is irreducible which σ permutes the roots of $f(x) \pmod{p}$ with cycle structure of type $F_3(x)$.

7. Where $f(x) \equiv F_1(x)F_2(x) \pmod{p}$ and $F_2(x)$ is irreducible over $(\mathbb{Z}/p\mathbb{Z})$. We denote by $L_3^{F_1(x)_{\mathbb{F}_p} F_2(x)_{\mathbb{F}_{p^2} \times \mathbb{F}_{p^2}}}(n,p)$ the number of polynomials over $(\mathbb{Z}/p\mathbb{Z})$ that is ir-

reducible which σ permutes the roots of $f(x) \pmod p$ with cycle structure of type $F_2(x)$.

8. Where $f(x) \equiv F_1(x)F_2(x) \pmod p$ and $F_2(x)$ splits completely over $(\mathbb{Z}/p\mathbb{Z})$. We denote by $L_3^{F_1(x)\mathbb{F}_p F_2(x)\mathbb{F}_p \times \mathbb{F}_p}(n,p)$ the number of polynomials over $(\mathbb{Z}/p\mathbb{Z})$ that splits completely which σ permutes the roots of $f(x) \pmod p$ with cycle structure of type $F_2(x)$.

4.1 Formulas For Counting Degree-3 Frobenius Pseudoprimes

In this section we obtain formulas for counting the cubic Frobenius pseudoprime that localized on prime number p. Before diving into the formulas for the counting cubic liars, we mention two well-known facts that we will use them repeatedly.

Fact 4.4. The group $\mathbb{F}_{p^r}^{\times}$ is cyclic of order $p^r - 1$.

Fact 4.5. In a cyclic group of order m the number of elements whose order divides d is exactly $\gcd(d,m)$.

Definition 4.6. [Stein, 2005, Definition 2.1.16] (Multiplicative Order of an Element). Let $n \in \mathbb{N}$ and $x \in \mathbb{Z}$ such that $\gcd(x,n) = 1$. The Multiplicative *order* of x modulo n is the smallest $m \in \mathbb{N}$ such that $x^m \equiv 1 \pmod n$.

Remark 18. For proofing of all the following lemmas, we will refer it to Theorem 3.28 and Lemmas 4.4 and 4.5.

Lemma 4.7. *Fix $n > 1$ and let $p^r \| n$. Then the number of polynomials $f(x)$ which satisfy the first case in Definition 4.3 is given by*

$$L_3^{F_1(x)\mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p}(n,p) = \binom{\gcd(n-1, p-1)}{3}.$$

Proof. Referring to Remark 18 and an assumption,

$$F_1(x) = (x^n - x, f(x)) = f(x),$$

so for $\alpha_1, \alpha_2, \alpha_3$ as the roots of $f(x)$, up to a choice of labelling we have

$$\alpha_1^n = \alpha_1, \alpha_2^n = \alpha_2, \alpha_3^n = \alpha_3.$$

That means by the Lemma 3.16 the representative of the permutations of the roots is equal to $(\alpha_1)(\alpha_2)(\alpha_3)$. Then $\text{order}(\alpha_i) \mid n-1$ for $i = 1,2,3$. Now since $f(x)$ splits completely over $\mathbb{Z}/p\mathbb{Z}$ we have $\alpha_1, \alpha_2,$ and $\alpha_3 \in \mathbb{F}_p$. So, $\text{order}(\alpha_i) \mid p-1$ for $i = 1,2,3$. Thus to select α_1, α_2, and α_3 it is equivalent to select three distinct elements whose orders divide $\gcd(n-1, p-1)$. Hence

$$L_3^{F_1(x)_{\mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p}}(n,p) = \binom{\gcd(n-1,p-1)}{3}. \qquad \square$$

Lemma 4.8. *Fix $n > 1$ and let $p^r \| n$. Then the number of polynomials $f(x)$ which satisfy the second case in Definition 4.3 is equal to*

$$L_3^{F_1(x)_{\mathbb{F}_p \times \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}}}(n,p) = \frac{1}{2}\gcd(n-1,p-1)\left(\gcd(n-1,p^2-1) - \gcd(n-1,p-1)\right).$$

Proof. Similar to Lemma 4.7 we have three distinct roots α_1, α_2 and α_3 such that their permutations is equal to $(\alpha_1)(\alpha_2)(\alpha_3)$. So the $\text{order}(\alpha_i) \mid n-1$ for $i = 1,2,3$.
Since $f(x)$ splits partially over $\mathbb{Z}/p\mathbb{Z}$, up to a choice of labelling we have $\alpha_1 \in \mathbb{F}_p$ and $\alpha_2, \alpha_3 \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$.

Then, $\text{order}(\alpha_1) \mid p-1$ and $\text{order}(\alpha_i) \mid p^2-1$ for $i = 2,3$. Hence there are $\gcd(n-1, p-1)$ options for α_1 and $\gcd(n-1, p^2-1)$ options for α_2. Note that α_2 and α_3 are elements of $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. So we must subtract the $\gcd(n-1, p-1)$ choices with $\alpha_2 \in \mathbb{F}_p$.

We divide the result by 2 because α_2 and α_3 are in the same cycle. So by having one of them we can find the other one. We conclude

$$L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p)=\frac{1}{2}\gcd(n-1,p-1)\Big(\gcd(n-1,p^2-1)-\gcd(n-1,p-1)\Big). \quad \square$$

Lemma 4.9. *Fix $n>1$ and let $p^r\|n$. Then the number of polynomials $f(x)$ which satisfy the third case in Definition 4.3 is equal to*

$$L_3^{F_1(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p)=\frac{1}{3}\big(\gcd(n-1,p^3-1)-\gcd(n-1,p-1)\big).$$

Proof. Similar to Lemma 4.7 we have three distinct roots α_1,α_2 and α_3, such that their permutations is equal to $(\alpha_1)(\alpha_2)(\alpha_3)$ up to a choice of labelling. So the order$(\alpha_i)\mid n-1$ for $i=1,2,3$.

Now since $f(x)$ is an irreducible polynomial over $\mathbb{Z}/p\mathbb{Z}$ we have $\alpha_1,\alpha_2,$ and $\alpha_3\in\mathbb{F}_{p^3}$. Then, order$(\alpha_i)\mid p^3-1$ for $i=1,2,3$. Thus there is $\gcd(n-1,p^3-1)$ options for α_1,α_2 and α_3. Additionally, we need to subtract the $\gcd(n-1,p-1)$ choices for α_2 when it belongs to $\mathbb{F}_{p^3}$ and $\mathbb{F}_p$ at the same time. Note that the roots are distinct and conjugate of each other hence choosing one determines all three roots.

$$L_3^{F_1(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p)=\frac{1}{3}\big(\gcd(n-1,p^3-1)-\gcd(n-1,p-1)\big). \quad \square$$

Lemma 4.10. *Fix $n>1$ and let $p^r\|n$. Then the number of polynomials $f(x)$ which satisfy the fourth case in Definition 4.3 is equal to*

$$L_3^{F_3(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p)=\frac{1}{3}(\gcd(n^3-1,p-1)-\gcd(n-1,p-1)).$$

Proof. Referring to Remark 18 and an assumption,

$$F_3(x) = (x^{n^3} - x, f_2(x)) = f(x), \text{ and } f_2(x) = f(x),$$

so for $\alpha_1, \alpha_2, \alpha_3$ as the distinct roots of $f(x)$ we have

$$\alpha_1^{n^3} = \alpha_1, \alpha_2^{n^3} = \alpha_2, \alpha_3^{n^3} = \alpha_3.$$

The permutations of these roots by Lemma 3.16 is represented by $(\alpha_1, \alpha_2, \alpha_3)$. That means we have $\alpha_1^n = \alpha_2$, $\alpha_2^n = \alpha_3$, $\alpha_3^n = \alpha_1$. Then $\text{order}(\alpha_i) \mid n^3 - 1$ and $\text{order}(\alpha_i) \nmid n - 1$ for $i = 1, 2, 3$. By the assumption $f(x)$ splits completely over $(\mathbb{Z}/p\mathbb{Z})$ then we have $\text{order}(\alpha_i) \mid (p-1)$ for $i = 1, 2, 3$. For the Frobenius step, we have

$$\text{order}(\alpha_i) \mid n^3 - p.$$

Since $\alpha_i^{n^3} = \alpha_i$ and $\alpha_i^p = \alpha_i$, for $\alpha_i \in \mathbb{Z}_p$. Then we have $\gcd(n^3 - 1, p - 1, n^3 - p)$ options for each α_i. We need to subtract $\gcd(n-1, p-1)$ choices for α_i since we need $\text{order}(\alpha_i) \mid n^3 - 1$ and $\text{order}(\alpha_i) \nmid n - 1$. By the cycle structure of the roots, picking one root determines the other ones. This explains why we divide the result by 3.

$$\begin{aligned} L_3^{F_3(x)_{\mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p}}(n, p) &= \frac{1}{3}(\gcd(n^3 - 1, p - 1, n^3 - p) - \gcd(n - 1, p - 1)) \\ &= \frac{1}{3}(\gcd(n^3 - 1, p - 1) - \gcd(n - 1, p - 1)). \end{aligned}$$ □

Lemma 4.11. *Fix $n > 1$ and let $p^r \| n$. There are no polynomials $f(x)$ which satisfy the fifth case in Definition 4.3, that is*

$$L_3^{F_3(x)_{\mathbb{F}_p \times \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}}}(n, p) = 0.$$

Proof. Let $f(x)$ split partially, so we have $\alpha_1 \in (\mathbb{Z}/p\mathbb{Z})$ or $\alpha_1 \in \mathbb{F}_p$, and $\alpha_2, \alpha_3 \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. The permutations of these roots by Lemma 3.16 is represented by $(\alpha_1, \alpha_2, \alpha_3)$ and by the assumption we have $\alpha_1^n = \alpha_2$, and $\alpha_2 \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Namely, $\alpha_1^n \notin \mathbb{F}_p$ therefore $\alpha_1 \notin \mathbb{F}_p$ and it is contradiction. Thus

$$L_3^{F_3(x)_{\mathbb{F}_p \times \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}}}(n,p) = 0. \qquad \square$$

Lemma 4.12. *Fix $n > 1$ and let $p^r \| n$. Then the number of polynomials $f(x)$ which satisfy the sixth case in Definition 4.3 is equal to*

$$L_3^{F_3(x)_{\mathbb{F}_{p^3} \times \mathbb{F}_{p^3} \times \mathbb{F}_{p^3}}}(n,p) = \frac{1}{3}\Big(\gcd(n^3-1, p^3-1, n-p) - \gcd(p-1, n-1) + \gcd(n^3-1, p^3-1, n-p^2, n^2-p) - \gcd(p-1, n-1) \Big).$$

Proof. By recalling Remark 18, we have

$$F_3(x) = (x^{n^3} - x, f_2(x)) = f(x), \text{ and } f_2(x) = f(x),$$

so for $\alpha_1, \alpha_2, \alpha_3$ as the roots of $f(x)$ we have

$$\alpha_1^{n^3} = \alpha_1, \alpha_2^{n^3} = \alpha_2, \alpha_3^{n^3} = \alpha_3,$$

and the permutation representation of roots is equal to $(\alpha_1, \alpha_2, \alpha_3)$ up to a choice of labelling. Then $\text{order}(\alpha_i) \mid n^3 - 1$ for $i = 1, 2, 3$. By the assumption, $f(x)$ is irreducible over $(\mathbb{Z}/p\mathbb{Z})$. Then we have $\text{order}(\alpha_i) \mid p^3 - 1$ for $i = 1, 2, 3$.
In this case $F_2(x) = 1$ so we apply Frobenuis step on $F_3(x)$, means $F_3(x) \mid F_3(x^n)$. Thus α_i^n for $i = 1, 2, 3$ is also the root of $F_3(x)$ or $f(x)$. For instance, without loss of generality, assuming that $\alpha_1^n = \alpha_2$ and $\alpha_1^{n^2} = \alpha_3$. Now two cases may occur over $\mathbb{F}_{p^3}$

- If $\alpha_i^p = \alpha_{i+1}$, so in this case, $\text{order}(\alpha_i) \mid \gcd(n^3 - 1, p^3 - 1, n - p, n^2 - p^2)$. For clarity, we can say $\alpha_1^p = \alpha_2$ and by the permutation we have $\alpha_1^n = \alpha_2$ which implies $\alpha_1^{p^2} = \alpha_3$

and again by permutation, $\alpha_1^{n^2} = \alpha_3$. That is, the permutation on roots $x \mapsto x^n$ and $x \mapsto x^p$ are equal.

- If $\alpha_i^{p^2} = \alpha_{i+1}$, so in this case, $\text{order}(\alpha_i) \mid \gcd(n^3-1, p^3-1, n-p^2, n^2-p)$. For clarity, we can say $\alpha_1^p = \alpha_3$ and by the permutation we have $\alpha_1^{n^2} = \alpha_3$ which implies $\alpha_1^{p^2} = \alpha_2$ and again by permutation, $\alpha_1^n = \alpha_2$. That is, the permutation on roots $x \mapsto x^n$ and $x \mapsto x^p$ are inverses.

In both cases we must exclude the roots where the order is a divisor of $n-1$ or of $p-1$. Because the order must divide $n-p$ or $n-p^2$ the cases of order $n-1$ or $p-1$ are equivalent. Hence we have

$$\begin{aligned} L_3^{F_3(x)\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}(n,p) &= \frac{1}{3}\Big(\gcd(n^3-1,p^3-1,n-p,n^2-p^2) - \gcd(n^3-1,p-1,n-1) \\ &\quad + \gcd(n^3-1,p^3-1,n-p^2,n^2-p) - \gcd(n^3-1,p-1,n-1)\Big) \\ &= \frac{1}{3}\Big(\gcd(n^3-1,p^3-1,n-p) - \gcd(n-1,p-1) \\ &\quad + \gcd(n^3-1,p^3-1,n-p^2,n^2-p) - \gcd(p-1,n-1)\Big). \end{aligned}$$ □

Lemma 4.13. *Fix $n > 1$ and let $p^r \| n$. Then the number of polynomials $f(x)$ which satisfy the seventh case in Definition 4.3 for $L_3^{F_1(x)\mathbb{F}_p F_2(x)\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}(n,p)$ is given by*

$$\frac{1}{2}\gcd(n-1,p-1)\Big(\gcd(n^2-1,p^2-1,n-p) - \gcd(n-1,p-1)\Big).$$

Proof. By recalling Remark 18 and up to the choice of labelling we have

$$F_1(x) = \gcd(x^n - x, f(x)) = x - \alpha_1, \text{ and } F_2(x) = \gcd(x^{n^2} - x, f_1(x)) = x^2 + ax + b.$$

Means $\alpha_1^n = \alpha_1, \alpha_i^{n^2} = \alpha_i$ for $i = 2,3$. So by the Lemma 3.16 the representative of the permutations of the roots is equal to $(\alpha_1)(\alpha_2,\alpha_3)$ up to a choice of labelling. Thus we

have that order$(\alpha_1) \mid n-1$ and order$(\alpha_i) \mid n^2-1$ for $i=2,3$. Here we assumed $F_2(x)$ is irreducible over $(\mathbb{Z}/\mathbb{Z}_p)$, then order$(\alpha_1) \mid p-1$ and order$(\alpha_i) \mid p^2-1$ for $i=2,3$. For the Frobenuis step we have:

$$F_2(x) \mid F_2(x^n),$$

thus x^n is also the roots of $F_2(x)$. So, $\alpha_2^n = \alpha_3$ and $\alpha_2^p = \alpha_3$ since $\alpha_2, \alpha_3 \in \mathbb{F}_{p^2}$. Then order$(\alpha_i) \mid n-p$ for $i=2,3$. Hence we have $\gcd(n-1, p-1)$ many choices for α_1 and $\gcd(n^2-1, p^2-1, n-p)$ choices for α_2 or α_3. Note that α_2 and α_3 are in $\mathbb{F}_{p^2}$ but not in $\mathbb{F}_p$ so that means ord(α_2) and ord(α_3) do not divide $p-1$ and also they do not divide $n-1$.

We divide the result by 2, since by the permutation map if we have α_2 or α_3 we can find the other one. We find that $L_3^{F_1(x)_{\mathbb{F}_p} F_2(x)_{\mathbb{F}_{p^2} \times \mathbb{F}_{p^2}}}(n,p)$ can be calculated by

$$\begin{aligned}
&\frac{1}{2}\gcd(n-1,p-1)\Big(\gcd(n^2-1,p^2-1,n-p) - \gcd(n^2-1,n^2-p,p-1,n-1)\Big) \\
&= \frac{1}{2}\gcd(n-1,p-1)\Big(\gcd(n^2-1,p^2-1,n-p) - \gcd(n-1,p-1)\Big).
\end{aligned}$$

□

Lemma 4.14. *Fix $n>1$ and let $p^r \| n$. Then the number of polynomials $f(x)$ which satisfy the eighth case in Definition 4.3 is equal to*

$$L_3^{F_1(x)_{\mathbb{F}_p} F_2(x)_{\mathbb{F}_p \times \mathbb{F}_p}}(n,p) = \frac{1}{2}\gcd(n-1,p-1)\Big(\gcd(n^2-1,p-1) - \gcd(n-1,p-1)\Big).$$

Proof. Similar to the representative of the permutations of the roots in Lemma 4.13 we have $(\alpha_1)(\alpha_2,\alpha_3)$. Here we assumed $F_2(x)$ splits over $(\mathbb{Z}/\mathbb{Z}_p)$, then order$(\alpha_1) \mid n-1$ and order$(\alpha_i) \mid n^2-1$ and order$(\alpha_i) \nmid n-1$ for $i=2,3$. For the Frobenuis step we have:

$$F_2(x) \mid F_2(x^n),$$

so x^n is also the roots of $F_2(x)$, namely, $\alpha_2^n = \alpha_3$ and $\alpha_2 \in \mathbb{Z}_p$, then $\alpha_2^p = \alpha_2$. We figured out that $\alpha_2^{n^2} = \alpha_2$ also $\alpha_2^p = \alpha_2$. Then order$(\alpha_i) \mid n^2-p$ for $i=2,3$. Therefore we have

$\gcd(n-1,p-1)$ option for α_1 and $\gcd(n^2-1,p-1,n^2-p)$ options for α_2 and α_3. As we mentioned above, order$(\alpha_i) \nmid n-1$ for $i=2,3$ so we need to subtract the multiple choices of $\gcd(n-1,p-1)$ for α_2 and α_3. We divide the result by 2, since by the permutation map if, we have α_2 or α_3 we can find the other one. Hence

$$\begin{aligned}
L_3^{F_1(x)_{\mathbb{F}_p} F_2(x)_{\mathbb{F}_p\times\mathbb{F}_p}}(n,p) &= \frac{1}{2}\Big(\gcd(n-1,p-1)\gcd(n^2-1,p-1,n^2-p) \\
&\quad -\gcd(n-1,p-1)\gcd(n-1,p-1)\Big) \\
&= \frac{1}{2}\Big(\gcd(n-1,p-1)\gcd(n^2-1,n^2-p)-\gcd(n-1,p-1)^2\Big) \\
&= \frac{1}{2}\Big(\gcd(n-1,p-1)\gcd(n^2-1,p-1)-\gcd(n-1,p-1)^2\Big) \\
&= \frac{1}{2}\gcd(n-1,p-1)\Big(\gcd(n^2-1,p-1)-\gcd(n-1,p-1)\Big). \quad \square
\end{aligned}$$

By combining the previous counting Lemmas 4.7–4.14, we deduce the following theorem. Let $n=\prod_{r_i} p_i^{r_i}$ where r_i is even or odd.

Theorem 4.15. *The number of cubic polynomials over $(\mathbb{Z}/n\mathbb{Z})$ with $\left(\frac{\Delta}{n}\right)=1$ for the first two cases and $\left(\frac{\Delta}{n}\right)=-1$ for the last one which n is a cubic Frobenius pseudoprime is exactly*

$$\begin{aligned}
L_3^{F_1}(n) &= \frac{1}{2}\prod_{p_i|n}\Big(L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p_i)+L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)+L_3^{F_1(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p_i)\Big) \\
&\quad +\frac{1}{2}\prod_{\substack{p_i|n\\ 2|r_i}}\Big(L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p_i)+L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)+L_3^{F_1(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p_i)\Big) \\
&\quad \prod_{\substack{p_i|n\\ 2\nmid r_i}}\Big(L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p_i)+(-1)L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)+L_3^{F_1(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p_i)\Big),
\end{aligned} \tag{4.1}$$

$$L_3^{F_3}(n)=\prod_{p_i|n}\Big(L_3^{F_3(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p_i)+L_3^{F_3(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p_i)\Big), \tag{4.2}$$

and

$$\begin{aligned} L_3^{F_2}(n) = &\frac{1}{2}\prod_{p_i|n}\left((-1)L_3^{F_1(x)F_2(x)_{\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)+L_3^{F_1(x)F_2(x)_{\mathbb{F}_p\times\mathbb{F}_p}}(n,p_i)\right)\\ &-\frac{1}{2}\prod_{\substack{p_i|n\\ 2|r_i}}\left(L_3^{F_1(x)F_2(x)_{\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)+L_3^{F_1(x)F_2(x)_{\mathbb{F}_p\times\mathbb{F}_p}}(n,p_i)\right)\\ &\prod_{\substack{p_i|n\\ 2\nmid r_i}}\left((-1)L_3^{F_1(x)F_2(x)_{\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)+L_3^{F_1(x)F_2(x)_{\mathbb{F}_p\times\mathbb{F}_p}}(n,p_i)\right). \end{aligned} \tag{4.3}$$

Proof. We are going to provide the sketch of proof. The argument for the case $L_3^{F_3}(n)$ is easier than the cases $L_3^{F_1}(n)$ and $L_3^{F_2}(n)$. So for convenience we consider only the case $L_3^{F_1}(n)$ which has the similar argument to $L_3^{F_2}(n)$.

In equation (4.1), for counting the number of cubic polynomials with $\left(\frac{\Delta}{n}\right)=1$ we need to describe the possible choices of $\left(\frac{\Delta}{p_i}\right)$ which result in $\prod\left(\frac{\Delta}{p_i}\right)^{r_i}=1$. Thus by the CRT we must for each $p|n$ decide on the factorization structure, and correspondingly pick elements either from the set of all roots of possible cubic polynomials in $\mathbb{F}_p$, from the set of roots in $\mathbb{F}_{p^3}\setminus\mathbb{F}_{p^2}$, or from the set of roots that are in both $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$. The sizes of these sets are given by $L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p_i)$, $L_3^{F_1(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p_i)$, and $L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)$, respectively. This leads us to the formula

$$\prod_{p_i|n}\left(L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p_i)+L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)+L_3^{F_1(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p_i)\right), \tag{4.4}$$

if we want to count only polynomials that satisfy condition (1) in Theorem 3.28, but we also want to take condition (2) into account. For cases $L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p_i)$ and $L_3^{F_1(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}$, always $(\frac{\Delta}{p_i})=1$, but for the case $L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)$ we have $(\frac{\Delta}{p_i})=-1$. So in the case $L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)$, we need to have the even number of $(\frac{\Delta}{p_i})=-1$. Notice in the expansion

$$\prod_{\substack{p_i|n\\ 2\nmid r_i}}\left(L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p_i)+(-1)L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)+L_3^{F_1(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p_i)\right),$$

term $L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)$ with odd numbers of $(\frac{\Delta}{p_i})=-1$ will get a coefficient -1. So adding expansion (4.4) and

$$\prod_{\substack{p_i|n\\ 2|r_i}}\left(L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p_i)+L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)+L_3^{F_1(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p_i)\right)$$
$$\prod_{\substack{p_i|n\\ 2\nmid r_i}}\left(L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p_i)+(-1)L_3^{F_1(x)_{\mathbb{F}_p\times\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p_i)+L_3^{F_1(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p_i)\right),$$

then dividing by 2 leaves only the desired terms. □

Lemma 4.16. *If $n>1$ is an integer, then*

$$L_3^{F_1}(n)\le\prod_{p|n}\max\Big(\gcd(n-1,p-1)^3,\frac{3}{2}\gcd(n-1,p-1)\gcd(n-1,p^2-1),$$
$$\gcd(n-1,p^3-1)\Big),$$
$$L_3^{F_3}(n)\le\prod_{p|n}\gcd(n^3-1,p^3-1),$$

and

$$L_3^{F_2}(n)\le\prod_{p|n}\gcd(n-1,p-1)\gcd(n^2-1,p^2-1).$$

Proof. For the $L_3^{F_1}(n)$ upper bound, we use equation (4.1) and Lemmas 4.9, 4.8 and 4.7.

Then we have

$$\begin{aligned}
L_3^{F_1}(n) &\leq \prod_{p|n}\left(L_3^{F_{1_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}}(n,p)+L_3^{F_{1_{\mathbb{F}_p\times\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}}(n,p)+L_3^{F_{1_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}}(n,p)\right)\\
&\leq \prod_{p|n} 3\max\left(\frac{1}{3!}\gcd(n-1,p-1)^3,\frac{1}{2}\gcd(n-1,p-1)\gcd(n-1,p^2-1),\right.\\
&\left.\frac{1}{3}\gcd(n-1,p^3-1)\right)\\
&\leq \prod_{p|n} \max\left(\gcd(n-1,p-1)^3,\frac{3}{2}\gcd(n-1,p-1)\gcd(n-1,p^2-1),\right.\\
&\left.\gcd(n-1,p^3-1)\right).
\end{aligned}$$

For the $L_3^{F_3}(n)$ upper bound, we use equation (4.2) and Lemmas 4.12, 4.10. So we have

$$\begin{aligned}
L_3^{F_3}(n) &= \prod_{p|n}\left(L_3^{F_{3_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}}(n,p)+L_3^{F_{3_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}}(n,p)\right)\\
&\leq \prod_{p|n} 2\max\left(\frac{1}{3}\big(\gcd(n^3-1,p^3-1,n-p)\right.\\
&\left.+\gcd(n^3-1,p^3-1,n-p^2,n^2-p)-\gcd(n-1,p-1)\big),\frac{1}{3}\gcd(n^3-1,p-1)\right)\\
&= \prod_{p|n}\frac{2}{3}\big(\gcd(n^3-1,p^3-1,n-p)+\\
&\gcd(n^3-1,p^3-1,n-p^2,n^2-p)-\gcd(n-1,p-1)\big)\\
&\leq \prod_{p|n}\frac{2}{3}\gcd(n^3-1,p^3-1)\\
&\leq \prod_{p|n}\gcd(n^3-1,p^3-1).
\end{aligned}$$

For the $L_3^{F_2}(n)$ upper bound, we use equation (4.3) and Lemmas 4.14, 4.13. Then we have

$$
\begin{aligned}
L_3^{F_2}(n) &\leq \prod_{p|n} \left(L_3^{F_1(x)F_2(x)_{\mathbb{F}_{p^2}\times\mathbb{F}_{p^2}}}(n,p) + L_3^{F_1(x)F_2(x)_{\mathbb{F}_p\times\mathbb{F}_p}}(n,p) \right) \\
&\leq \prod_{p|n} 2\max\Big(\frac{1}{2}\gcd(n-1,p-1)\gcd(n^2-1,p^2-1,n-p), \\
&\frac{1}{2}\gcd(n-1,p-1)\gcd(n^2-1,p-1) \Big) \\
&= \prod_{p|n} \gcd(n-1,p-1)\gcd(n^2-1,p^2-1,n-p) \\
&\leq \prod_{p|n} \gcd(n-1,p-1)\gcd(n^2-1,p^2-1). \qquad \square
\end{aligned}
$$

Our goal in Section 4.3 will be to find the largest possible value for $L_3^{F_3}(n)$. In equation (4.2), we consider two terms: $L_3^{F_3(x)_{\mathbb{F}_{p^3}}}(n,p)$ and $L_3^{F_3(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p)$ for all $p \mid n$. The first term, $L_3^{F_3(x)_{\mathbb{F}_{p^3}}}(n,p)$, is of particular interest because it has the potential to be larger than the second term. Specifically, the term $L_3^{F_3(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p)$ is bounded above by $p-1$, whereas $L_3^{F_3(x)_{\mathbb{F}_{p^3}}}(n,p)$ is bounded by p^3-1. We see that

$$
\begin{aligned}
\prod_{p|n} L_3^{F_3(x)}(n,p) &= \prod_{p|n} \left(L_3^{F_3(x)_{\mathbb{F}_{p^3}}}(n,p) + L_3^{F_3(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p) \right) \\
&= \prod_{p|n} \Bigg(\frac{1}{3}\Big(\gcd(n^3-1,p^3-1,n-p) - \gcd(n^3-1,p-1,n-p) \\
&+ \gcd(n^3-1,p^3-1,n-p^2,n^2-p) - \gcd(n^3-1,p-1,n-p^2,n^2-p) \Big) \\
&+ \frac{1}{3}\gcd(n^3-1,p-1) \Bigg) \\
&\leq \prod_{p|n} (p^3-1) \\
&\sim n^3
\end{aligned}
$$

is an upper bound on what we can hope to obtain. Therefore, we will focus on establishing conditions that maximize $L_3^{F_3(x)}(n,p)$, aiming for it to be as close as possible to n^3.

4.2 Number Theoretical Background

In this section, we are going to recall some important number theory background that can mostly be found in [Fiori and Shallue, 2020].

Definition 4.17. For each value $x \geq 1$ denote by $M(x)$ the least common multiple of all positive integers up to $\frac{\log x}{\log\log x}$.

The following claim can be found in [Erdős and Pomerance, 1986]. We fill in the details of the proof from [Fiori and Shallue, 2020, Proposition 20].

Proposition 4.18. *We have $M(x) = x^{o(1)}$ for large x.*

Proof. Let $\max \alpha_i$ denote the largest value of α such that p_i^{α} divides numbers less than $\frac{\log(x)}{\log\log(x)}$ so we have $M(x) = \prod_{p_i < \frac{\log(x)}{\log\log(x)}} p_i^{\max \alpha_i}$. Since $p_i^{\max \alpha_i} \leq \frac{\log x}{\log\log x}$, we have

$$(\max \alpha_i) \log p_i \leq \log\left(\frac{\log x}{\log\log x}\right). \tag{4.5}$$

By dividing both sides of inequality (4.5) by $\log p_i$, we get the term

$$\frac{\log\left(\frac{\log x}{\log\log x}\right)}{\log p_i}.$$

This expression can be expanded to

$$(\max \alpha_i) \leq \frac{\log\log x - \log\log\log x}{\log p_i}. \tag{4.6}$$

By the inequality (4.6), we have

$$\begin{aligned}
M(x) &= \prod_{p_i < \log(x)/\log\log(x)} p_i^{\max \alpha_i} = \prod_{p_i < \frac{\log x}{\log\log x}} p_i^{\left\lfloor \frac{\log\log x - \log\log\log x}{\log p_i} \right\rfloor} \\
&< \prod_{p_i < \frac{\log x}{\log\log x}} p_i^{\left(\frac{\log\log x - \log\log\log x}{\log p_i}\right)} \\
&= \prod_{p_i < \frac{\log x}{\log\log x}} \frac{\log x}{\log\log x} \\
&< \left(\frac{\log x}{\log\log x}\right)^{\pi\left(\frac{\log x}{\log\log x}\right)} \\
&< \left(\frac{\log x}{\log\log x}\right)^{\frac{\frac{2\log x}{\log\log x}}{\log\left(\frac{\log x}{\log\log x}\right)}} \\
&< x^{\frac{2}{\log\log x}} \\
&< x^{o(1)}.
\end{aligned}$$

The third and fifth lines of the above claim are derived from the fact that $a^{\frac{b}{\log a}} = \exp(b)$. Additionally, we obtained the fourth line from the third by applying Theorem 1.7, and the fifth line comes from the bound $\pi(x) < \frac{2x}{\log x}$ due to [Rosser and Schoenfeld, 1962, Equation (3.6)]. □

In our construction, we shall need to use prime numbers where certain polynomial values of them are smooth. The existence of such primes has been well studied, see for example [Baker and Harman, 1998] and [Dartyge et al., 2002]. Now we introduce the following set

$$\Psi_F^*(x,y) = \#\left\{p \leqslant x : P^+(F(p)) \leqslant y\right\}, \tag{4.7}$$

where $P^+(m)$ denotes the largest prime factor of m, with the convention that $P^+(1) = 1$, and $F(x)$ is a polynomial with integer coefficients. Consider $F(x)$ to be a polynomial with integer coefficients. Let g be the largest degrees of the irreducible factors of F and let k be

the number of distinct irreducible factors of $F(X)$ of degree g. We use this notation in the next three theorems.

Theorem 4.19. *[Dartyge et al., 2002, Theorem 1.2] Consider $F(0) \neq 0$ if $g = k = 1$, and let ε be a positive real number. Then the estimate*

$$\Psi_F^*(x,y) \asymp \frac{x}{\log x} \tag{4.8}$$

holds for all large x provided $y \geqslant x^{g+\varepsilon-1/2k}$.

Conjecture 4.20. [Dartyge et al., 2002, p. 3] The asymptotic (4.9) is satisfied for any positive α.

$$\Psi_F^*(x,x^\alpha) \asymp_{F,\alpha} \frac{x}{\log x} \tag{4.9}$$

Remark 19. Cecile Dartyge, Greg Martin, and Gerald Tenenbaum have established in their paper [Dartyge et al., 2002] that a lower bound of the asymptotic (4.9) is satisfied for $\alpha \geq g - 1/2k$.

We are going to generalize Definition [Fiori and Shallue, 2020, p. 503], in the following definition.

Definition 4.21. Let $F(x)$ be a polynomial with integer coefficients. The following set is denoted by $P_{\alpha,F}(x)$,

$$\{p < (\log x)^\alpha \text{ such that } F(p) \mid M(x)\}.$$

Lemma 4.22. *Let $\alpha > 0$ and suppose for all $0 < \alpha < \alpha'$ we have $\Psi_F^*(y, y^{1/\alpha}) \sim y^{1-o(1)}$, then we have $\Psi_F^*(\log(x)^\alpha, \log(x)/\log\log(x)) \sim \log(x)^{\alpha-o(1)}$.*

Proof. Using equation (4.7), we have

$$\begin{aligned}\Psi_F^*(\log(x)^\alpha, \log(x)/\log\log(x)) &= \#\left\{p < (\log x)^\alpha \mid P^+(F(p)) \leq \frac{\log x}{\log\log x}\right\} \\ &= \#\left\{p < (\log x)^\alpha \mid P^+(F(p)) \leq \log x^{1-o(1)}\right\} \\ &= \Psi_F^*(\log(x)^\alpha, \log(x)^{1-o(1)}) \\ &\asymp \log(x)^{\alpha-o(1)}.\end{aligned}$$

By taking $y = \log(x)^\alpha$ and noting that eventually $1/\alpha - o(1) > 1/\alpha'$, then

$$\Psi_F^*(\log(x)^\alpha, \log(x)/\log\log(x)) = \Psi_F^*(\log(x)^\alpha, \log(x)^{1-o(1)}) \asymp_{F,\alpha} \frac{(\log x)^\alpha}{\log((\log x)^\alpha)}.$$

Hence, $\Psi_F^*(\log(x)^\alpha, \log(x)/\log\log(x)) \geq \log x^{\alpha-o(1)}$ for $\alpha > 0$. □

A version of the following lemma is assumed in both the Erdős-Pomerance and Fiori-Shallue papers without proof.

Lemma 4.23. *Let* $\alpha > 1/2$ *such that* $\Psi_F^*(\log(x)^\alpha, \log(x)/\log\log(x)) \sim \log(x)^{\alpha-o(1)}$ *then* $P_{\alpha,F}(x) \sim \log(x)^{\alpha-o(1)}$.

Proof. The difference between set $P_\alpha(x)$ and set $B = \{p < (\log x)^\alpha \mid \forall q \mid F(p), q \leq \frac{\log x}{\log\log x}\}$ is the set

$$A = \{p < (\log x)^\alpha \mid \forall q \mid F(p), q < \frac{\log x}{\log\log x} \text{ and } \exists q^{\beta_i} \mid F(p), q^{\beta_i} \nmid M\},$$

and q^{β_i} is the largest prime power divisor of $F(p)$.

Now we want to bound the set A, so we use the following set which contains the set A as a subset.

$$\{n < \log(x)^\alpha \mid \exists q^r, q^r | F(n), q < \log(x)/\log\log(x), q^r > \log(x)/\log\log(x)\}.$$

For convenience, we can bound the above set by counting this separately for each fixed q. Thus we define the set

$$A_q = \{n < \log(x)^\alpha \mid \exists r, q^r | F(n), q < \log(x)/\log\log(x), q^r > \log(x)/\log\log(x)\}.$$

For $q < \sqrt{\log(x)/\log\log(x)}$, by the definition of A_q, we have $n < (\log x)^\alpha$ and $F(n) \equiv 0 \bmod q^r$. So we simply count the roots of $F(n) \pmod{q^r}$ which are less than $\log(x)^\alpha$. That means the roots n of polynomial $F(x)$ have to be less that q^r. Then

$$\mid A_q \mid \leq \mathrm{Deg}(F)\frac{\log(x)^\alpha}{q^r} < \mathrm{Deg}(F)(\log x)^{\alpha-1}\log\log x.$$

For $q > \sqrt{\log(x)/\log\log(x)}$, then we have

$$\mid A_q \mid \leq \mathrm{Deg}(F)\frac{(\log x)^\alpha}{q^2}.$$

Now, we take a summation over $1 < q < \log(x)/\log\log(x)$.

$$\begin{aligned}
\mid A \mid &< \sum_q |A_q| \\
&< \sum_{1<q<\sqrt{\frac{\log(x)}{\log\log(x)}}} \mathrm{Deg}(F)(\log x)^{\alpha-1}\log\log x + \sum_{\sqrt{\frac{\log x}{\log\log x}}<q} \mathrm{Deg}(F)\frac{(\log x)^\alpha}{q^2} \\
&\ll (\sqrt{\log x/\log\log x})(\log x)^{\alpha-1}\log\log x + (\log x)^\alpha/\sqrt{\log x/\log\log x} \\
&\ll (\sqrt{\log x})(\log x)^{\alpha-1}\log\log x + (\log x)^{\alpha-\frac{1}{2}}\sqrt{\log\log x} \\
&\ll (\log x)^{\alpha-\frac{1}{2}}(\log\log x + \sqrt{\log\log x}) \\
&\ll (\log x)^{\alpha-\frac{1}{2}-o(1)}.
\end{aligned}$$

Then

$$\mid \{p < (\log x)^\alpha \mid P^+(F(p)) \leq \frac{\log x}{\log\log x}\} - P_\alpha(x) \mid < (\log x)^{\alpha-\frac{1}{2}-o(1)} < (\log x)^{\alpha-o(1)},$$

so

$$\Psi_F^*(\log(x)^\alpha, \log(x)/\log\log(x)) - \mid P_\alpha(x) \mid < (\log x)^{\alpha-\frac{1}{2}-o(1)} < \Psi_F^*(\log(x)^\alpha, \log(x)/\log\log(x)),$$

and then we have

$$\begin{aligned}(\log x)^{\alpha-o(1)} &< \Psi_F^*(\log(x)^\alpha, \log(x)/\log\log(x)) - (\log x)^{\alpha-\frac{1}{2}-o(1)} \\ &< \mid P_\alpha(x) \mid \\ &< \Psi_F^*(\log(x)^\alpha, \log(x)/\log\log(x)).\end{aligned}$$

□

We are going to generalize the proof of [Fiori and Shallue, 2020, Prop. 21], in the following proposition.

Proposition 4.24. *For all $\alpha \leq 2/3$, where $F(n) = n^3 - 1$, we have*

$$|P_{\alpha,F}(x)| \geq (\log x)^{\alpha-o(1)}$$

as $x \to \infty$.

Proof. Here $f(x) = x^3 - 1$ so $g = 2$ and $k = 1$. By applying Lemma 4.20, $\alpha^{-1} > 3/2$. □

The following conjecture is a consequence of Lemma 4.23, Proposition 4.24, and Conjecture 4.20.

Conjecture 4.25. For all $\alpha > 0$ we have $|P_{\alpha,F}(x)| \geq (\log x)^{\alpha-o(1)}$.

In Sections 4.3 and 4.4, we are going to work on the lower and upper bound of $L_3^{F_3(x)}(n)$ using Lemma 4.23 and Conjecture 4.20 frequently.

We are going to generalize the definition [Fiori and Shallue, 2020, p. 503], in the following definition.

Definition 4.26. For each value x and for each $\alpha > 0$ we define the set $P_{\alpha,F}(x,a)$ by,

$$P_{\alpha,F}(x,a) = \{p < (\log x)^{\alpha} \mid p = a \bmod F(p), \text{ and } F(p) \mid M(x)\},$$

where $F(a) = 0 \pmod{M(x)}$ for $a \in \mathbb{N}$.

If we assume Conjecture 4.20 then the conclusion of the following proposition will also hold for all $\alpha > 0$.

We are going to generalize the proof of [Fiori and Shallue, 2020, Prop. 23], in the following proposition.

Proposition 4.27. *Given $\alpha > 0$ such that $|P_{\alpha,F}(x)| \geq (\log x)^{\alpha - o(1)}$ as $x \to \infty$, then there exists integer $a \neq 1$ such that as $x \to \infty$ we have*

$$|P_{\alpha,F}(x,a)| \geq (\log x)^{\alpha - o(1)}.$$

Proof. We know that each prime $p \in P_{\alpha,F}(x,a)$ is also in $P_{\alpha,F}(x)$. Conversely, each prime $p \in P_{\alpha}(x)$ is also in $P_{\alpha}(x,a)$ for all a satisfying $p = a \bmod F(p)$. By Definition 4.26, we know

$$F(a) = 0 \bmod F(p) \text{ and } F(a) = 0 \bmod M(x),$$

so by the Chinese Reminder Theorem we have

$$F(a) = 0 \bmod M',$$

where $M^{'}$ is the largest divisor of M with $gcd(M',F(p)) = 1$.

$$A = \{a \in \mathbb{Z}/M\mathbb{Z} \mid F(a) = 0 \pmod{M}\},$$

$$A(p) = \{a \in \mathbb{Z}/F(p)\mathbb{Z} \mid F(a) = 0 \pmod{F(p)}\}.$$

Since there exists at least one value that is as large as the average, we can say that there is a value a' such that $P_{\alpha,F}(x,a') \geq \frac{1}{|A|}\sum_a \mid P_{\alpha,F}(x,a) \mid$. So we have

$$\begin{aligned}
P_{\alpha,F}(x,a') &\geq \frac{1}{\mid A \mid}\sum_a \mid P_{\alpha,F}(x,a) \mid \\
&= \frac{1}{\mid A \mid}\sum_{p\in P_\alpha(x)}\sum_{\substack{a \\ p\in P_{\alpha,F}(x,a)}} 1 \\
&= \sum_{p\in P_\alpha(x)} \frac{\mid \{ \text{ solutions to } F(a) = 0 (\bmod M^{'})\} \mid}{\mid A \mid} \\
&= \sum_{p\in P_\alpha(x)} \frac{1}{\mid A(p) \mid} \\
&= \deg(F)^{-\omega(F(p))} \log x^{\alpha - o(1)} \\
&\geq \deg(F)^{-\omega_{\max}(F(p))} (\log x)^{\alpha - o(1)} \\
&\geq (\log x)^{\alpha - o(1)}.
\end{aligned}$$

Notice that $|A(p)| \leq (\deg(F))^{\omega(F(p))}$. Since the number of prime divisors of $F(p)$ is $\omega(F(p))$. Then the number of possible solutions for equation $F(a) = 0 \pmod{F(p)}$ are at most $(\deg(F))^{\omega(F(p))}$. Now by [Hardy and Wright, 1979, Section 22.10] we know that when $p < (\log x)^\alpha$ we have

$$\omega_{\max}(F(p)) \leq (1 + o(1))\frac{\log(\log x^\alpha)}{\log(\log(\log x^\alpha))} \leq (\log x)^{o(1)},$$

where $\omega_{\max}(F(p))$ is the maximum number of primes that divide a number of size $F(p)$. Notice that in the sixth line we have $\deg(F)^{-\omega_{\max}(F(p))} = \log(x)^{o(1)}$. □

In the construction of Lemma 4.35 and 4.40, it is essential to identify auxiliary primes that satisfy specific congruence conditions and ensure they are not excessively large. The following result addresses this requirement.

Theorem 4.28 (Linnik's theorem)**.** *[Linnik, 1944, Xylouris, 2011a] Let $P(a;q)$ be the least prime in an arithmetic progression $a \bmod q$ where a and q are co prime positive integers. Then there exists an effectively computable constant $L > 0$ such that*

$$P(a;q) < q^L.$$

The current world record for the value of L is 5 due to [Xylouris, 2011b].

4.3 Lower Bound

In this section, we want to find the lower bound for $L_3^{F_3(x)}(n)$. We present two conjectural lower bounds for $L_3^{F_3(x)}(n)$, with the second relying on a significantly weaker conjecture. At the end of the section, we will briefly discuss the lower bounds for $L_3^{F_1(x)}(n)$ and $L_3^{F_2(x)}(n)$.

The following definitions generalize [Fiori and Shallue, 2020, p. 505].

Definition 4.29. For fixed $0 < \varepsilon < \alpha - 1$ and for all $x > 0$ let

- $P_\alpha(x,a) = P_{\alpha,n^3-1}(x,a)$
- $k_\alpha(x) = \left\lfloor \frac{\log x - 2L\log M}{\alpha \log\log x} \right\rfloor$,
- $S^{(3)}_{\alpha,\varepsilon}(x,a)$ be the set of integers s which are the product of $k_\alpha(x)$ distinct elements from

$$P_\alpha(x,a) \backslash P_{\alpha-\varepsilon}(x,a).$$

That is,

$$S^{(3)}_{\alpha,\varepsilon}(x,a) = \{s | s = \prod_{i=1}^{k_\alpha(x)} p_i, p_i \in P_\alpha(x,a) \backslash P_{\alpha-\varepsilon}(x,a) \text{ and }, p\text{'s are distinct}\}.$$

The following Lemma is similar to the claim [Fiori and Shallue, 2020, p. 506].

Lemma 4.30. *Given $\alpha > 1$, the elements s of $S^{(3)}_{\alpha,\varepsilon}(x,a)$ all satisfy*

$$\left((\log x)^{-k_\alpha(x)\varepsilon}\right)\frac{x}{M^{2L}} \leq s < \frac{x}{M^{2L}}$$

as $x \to \infty$.

Proof. By the definition of $S^{(3)}_{\alpha,\varepsilon}(x,a)$, let s be a product of $k_\alpha(x)$ many primes of size $\log(x)^{\alpha-\varepsilon} < p < \log(x)^\alpha$. For upper bound by the definition 4.29 we have :

$$((\log x)^\alpha)^{k_\alpha(x)} = ((\log x)^\alpha)^{\frac{\log x - 2L\log M}{\alpha \log\log x}} = (\log x)^{\left(\alpha\frac{\log(\frac{x}{M^{2L}})}{\alpha\log\log x}\right)} = (\log x)^{\left(\frac{\log(\frac{x}{M^{2L}})}{\log\log x}\right)}.$$

Let $A = (\log x)^{\left(\frac{\log(\frac{x}{M^{2L}})}{\log\log x}\right)}$. So

$$\log A = \log\left((\log x)^{\left(\frac{\log(\frac{x}{M^{2L}})}{\log\log x}\right)}\right) = \left(\frac{\log(\frac{x}{M^{2L}})}{\log\log x}\right)\cdot\log\log x = \log\left(\frac{x}{M^{2L}}\right),$$

then $A = \frac{x}{M^{2L}}$ and $s < \frac{x}{M^{2L}}$. For lower bound we have:

$$\left((\log x)^{(\alpha-\varepsilon)}\right)^{k_\alpha(x)} = (\log x)^{\alpha k_\alpha(x)}(\log x)^{-\varepsilon k_\alpha(x)}.$$

Let $B = (\log x)^{\alpha k_\alpha(x)} = (\log x)^{\alpha\frac{\log x - 2L\log M}{\alpha\log\log x}} = (\log x)^{\frac{\log x - 2L\log M}{\log\log x}}$. So

$$\log B = \log\left((\log x)^{\frac{\log x - 2L\log M}{\log\log x}}\right) = \left(\frac{\log x - 2L\log M}{\log\log x}\right)\cdot\log\log x = \log\left(\frac{x}{M^{2L}}\right),$$

then $B = \frac{x}{M^{2L}}$ and $(\log x)^{-\varepsilon k_\alpha(x)} \frac{x^{1-o(1)}}{M^L} \leq s$. □

Proposition 4.31. *If $k \leq n$ and are integer, then $\binom{n}{k} \geq (n/k)^k$.*

Proof. We have $\binom{n}{k} = \frac{n\times(n-1)\times\cdots\times(n-(k-1))}{k\times(k-1)\times\cdots\times 1} = \frac{n}{k} \times \frac{n-1}{k-1} \times \cdots \frac{n-(k-1)}{k-(k-1)} = \prod_{i=0}^{k-1} \frac{n-i}{k-i}$.
For all $0 \leq i \leq k-1$, each fraction $\frac{n-i}{k-i}$ is greater than $\frac{n}{k}$, since

$$k \leq n$$

$$-ni \leq -ki$$

$$nk - ni \leq kn - ki$$

$$n(k-i) \leq k(n-i)$$

$$\frac{n}{k} \leq \frac{n-i}{k-i}$$

Hence $\frac{n^k}{k^k} < \binom{n}{k}$. □

Lemma 4.32. *The positive integer $k_\alpha(x)$ in Definition 4.29 satisfies the following equalities*

1. $k_\alpha(x) = \alpha^{-1} \frac{\log(x)}{\log\log(x)}(1 + o(1))$.

2. $k_\alpha(x) = (\log(x))^{1+o(1)}$.

Proof. By Definition 4.29 and Proposition 4.18, we have

$$\begin{aligned} k_\alpha(x) = \left\lfloor \frac{\log x - 2L\log M}{\alpha \log\log x} \right\rfloor &< \frac{\log x + 2L\log M}{\alpha\log\log x} \\ &= \log x \left(\frac{1+\mathrm{o}(1)}{\alpha\log\log x} \right) \\ &= \alpha^{-1} \frac{\log x}{\log\log x} (1+\mathrm{o}(1)). \end{aligned}$$

Consider $\left(\frac{1+o(1)}{\alpha \log\log x}\right) = (\log x)^{f(x)}$ so

$$\log(1+o(1)) - \log(\alpha \log\log x) = f(x)\log\log x,$$

then

$$\frac{\log(1+o(1))}{\log\log x} - \frac{\log\alpha}{\log\log x} - \frac{\log\log\log x}{\log\log x} = f(x).$$

Where x goes to infinity $f(x)$ goes to zero. So we can rewrite $(\log x)^{f(x)}$ as $(\log x)^{o(1)}$. Then $\frac{\log x + 2L\log M}{\alpha \log\log x} = (\log x)^{1+o(1)}$. □

We are going to generalize the proof of [Fiori and Shallue, 2020, Prop. 29], in the following proposition.

Proposition 4.33. *Given $\alpha > 1$ for which $P_\alpha(x,a) > (\log x)^{\alpha - o(1)}$, then*

$$\left|S^{(3)}_{\alpha,\varepsilon}(x,a)\right| \geq x^{1-\alpha^{-1}+o(1)}$$

as $x \to \infty$.

Proof. Using definition 4.29, we have to chose $k_\alpha(x)$ numbers of the element of the set $P_\alpha(x,a)\backslash P_{\alpha-\varepsilon}(x,a)$. So we need to find $\begin{pmatrix} |\, P_\alpha(x,a)\backslash P_{\alpha-\varepsilon}(x,a)\,| \\ k_\alpha(x) \end{pmatrix}$. By the Definition 4.26 and Proposition 4.27, we have

$$\begin{aligned} |\, P_\alpha(x,a)\backslash P_{\alpha-\varepsilon}(x,a)\,| &\geq |\, P_\alpha(x,a)\,| - |\, P_{\alpha-\varepsilon}(x,a)\,| \\ &\geq (\log x)^{\alpha-o(1)} - (\log x)^{\alpha-\varepsilon} = (\log x)^{\alpha-o(1)}. \end{aligned}$$

Because the primes that remain from above subtraction are included in the set $P_\alpha(x)$. Using

Proposition 4.31 and Lemma 4.32, we have:

$$\begin{aligned}
\begin{pmatrix} |\, P_\alpha(x,a)\backslash P_{\alpha-\varepsilon}(x,a)\,| \\ k_\alpha(x) \end{pmatrix} &\geq \left(\frac{|\, P_\alpha(x,a)\backslash P_{\alpha-\varepsilon}(x,a)\,|}{k_\alpha(x)}\right)^{k_\alpha(x)} \\
&\geq \left(\frac{(\log x)^{\alpha-o(1)}}{k_\alpha(x)}\right)^{k_\alpha(x)} \\
&\geq \left(\frac{(\log x)^{\alpha-o(1)}}{\frac{\log x-2L\log M}{\alpha\log\log x}}\right)^{\frac{\log x-2L\log M}{\alpha\log\log x}-1} \\
&\geq \left((\log x)^{\alpha-1-o(1)}\right)^{\frac{\log x-2L\log M}{\alpha\log\log x}-1} \\
&\geq \left((\log x)^{\alpha-1-o(1)}\right)^{(\alpha^{-1}-o(1))\frac{\log x}{\log\log x}} \\
&\geq (\log x)^{(1-\alpha^{-1}+o(1))\frac{\log x}{\log\log x}}.
\end{aligned}$$

Now, assume $(\log x)^{(1-\alpha^{-1}+o(1))\frac{\log x}{\log\log x}} = A$ then A is equal to $x^{(1-\alpha^{-1}+o(1))}$. Hence

$$\left|S^{(3)}_{\alpha,\varepsilon}(x,a)\right| \geq x^{1-\alpha^{-1}+o(1)}.$$

In this Proposition, the requirement are $|P_\alpha(x)| > k_\alpha(x)$ and $\alpha > 1$ since $1-\alpha^{-1}$ has to be positive. □

Lemma 4.34. *Let n be an integer and $p \mid n$. If* $\gcd(n^3-1, p^3-1, n-p) = p^3-1$ *then*

$$L_3^{F_3(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p) \neq 0.$$

Proof. By Lemma 4.12 we have

$$\begin{aligned}
L_3^{F_3(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p) = \frac{1}{3}\Big(&\gcd(n^3-1,p^3-1,n-p) - \gcd(p-1,n-1) \\
&+ \gcd(n^3-1,p^3-1,n-p^2,n^2-p) - \gcd(p-1,n-1)\Big).
\end{aligned}$$

We know $\gcd(n-1,p-1) \leq p-1$. Without lose of generality we consider that $\gcd(n-1,p-1) = p-1$. Now we have to show that $\gcd(n^3-1,p^3-1,n^2-p,n-p^2) \neq p^3-1$. Note that

$$\gcd(n^3-1,p-1,n^2-p,n-p^2) = p-1.$$

Since $p-1 \mid n-1$ and we can write n^2-p as $(n^2-1)-(p-1)$. Then $p-1 \mid n^2-p$. For the term $n-p^2$, we can write it as $(n-1)-(p^2-1)$. So $p-1 \mid n-p^2$. By these notes we find that

$$\gcd(n^3-1,p^3-1,n^2-p,n-p^2) \geq p-1.$$

If we assume $\gcd(n^3-1,p^3-1,n^2-p,n-p^2) = p^3-1$, then $p^3-1 \mid n-p^2$, also by the assumption we know that $p^3-1 \mid n-p$ so p^3-1 divides the linear combination of $n-p$ and $n-p^2$, that is, $p^3-1 \mid p^2-p$ and this is a contradiction. Therefore,

$$p^3-1 \geq \gcd(n^3-1,p^3-1,n^2-p,n-p^2) \geq p-1,$$

and $L_3^{F_3(x)_{\mathbb{F}_{p^3}}}(n,p) \neq 0$. □

The following lemma generalizes the proof of [Fiori and Shallue, 2020, Lemma 31].

Lemma 4.35. *Let L be an upper bound for Linnik's constant. Given any element s of $S^{(3)}_{\alpha,\varepsilon}(x,a)$ and $\alpha > 1$ there exists a number $M < q < M^{2L}$ such that*

1. $sq = a \pmod{M}$,
2. $\gcd(q,s) = 1$, *and*
3. $\prod_{p \mid q} \frac{1}{3}\left(\gcd\left(n^3-1,p^3-1,n-p\right) - \gcd(n^3-1,p-1,n-p)\right) > 0$.

Moreover, if $n = sq$ then

$$L_3^{F_3(x)}(n) > x^{3-3\frac{\varepsilon}{\alpha}-o(1)},$$

as $x \to \infty$.

Proof. We construct q as the product of two primes q_1 and q_2, which are chosen as the smallest primes greater than M satisfying certain conditions, as given below. First we write $M = {\ell_1}^{r_1}{\ell_2}^{r_2}M'$ where we have picked prime numbers ℓ_1 and ℓ_2 that are not equal to 3. Let $\gcd(\ell_1, M') = \gcd(\ell_2, M') = 1$, where $a \neq 1 \pmod{\ell_1}$, and $a \neq 1 \pmod{\ell_2}$.

Now we construct the following system of congruences

$$q_1 \equiv a \,(\mathrm{mod}\, \ell_1^{r_1}) \qquad q_2 \equiv s^{-1} \,(\mathrm{mod}\, \ell_1^{r_1}) \qquad q_1 \equiv 1 \,(\mathrm{mod}\, M') \tag{4.10}$$

$$q_2 \equiv a \,(\mathrm{mod}\, \ell_2^{r_2}) \qquad q_1 \equiv s^{-1} \,(\mathrm{mod}\, \ell_2^{r_2}) \qquad q_2 \equiv as^{-1} \,(\mathrm{mod}\, M'). \tag{4.11}$$

This system has a solution by the Chinese Reminder Theorem. Additionally, by Linnik's theorem, we can bound $q = q_1 q_2 < M^{2L}$. It provides all we need for the first condition. For the third condition, since $a \neq 1 \pmod{\ell_1}$, and $a \neq 1 \pmod{\ell_2}$ then exist prime numbers τ_1, τ_2 such that

$$\tau_i \mid \gcd(n^3 - 1, q_i^3 - 1, n - q_i) \text{ and } \tau_i \nmid \gcd(n^3 - 1, q_i - 1, n - q_i) \text{ for } i = 1, 2.$$

So, $\gcd(n^3 - 1, q_i^3 - 1, n - q_i) \neq \gcd(n^3 - 1, q_i - 1, n - q_i)$ and it gives $\gcd(n^3 - 1, q_i^3 - 1, n - q_i) - \gcd(n^3 - 1, q_i - 1, n - q_i) \neq 0$ for $i = 1, 2$. For showing the second condition, at first, we show $\gcd(s, M) = 1$ then prove why $\gcd(q, s) = 1$. Assume $s \in S^{(3)}_{\alpha,\varepsilon}(x, a)$, by Definition 4.29 we find that $(\log x)^{\alpha-\varepsilon} < p < (\log x)^{\alpha}$. On the other hand, by Definition 4.17, we have $p < \frac{\log x}{\log\log x} = (\log x)^{1-o(1)}$. So all primes that divide M are greater than all primes that divide s means $M > s$, then $\gcd(s, M) = 1$.Thus that $q_1, q_2 > M$ implies they are greater than any factor of s, and thus relatively prime to s, then $\gcd(q, s) = 1$.

For the last part of the proof, we know by Theorem 4.15, equation (4.2)

$$\begin{aligned}\prod_{p|n} L_3^{F_3(x)}(n,p) &= \prod_{p|n} \left(L_3^{F_3(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p) + L_3^{F_3(x)_{\mathbb{F}_p\times\mathbb{F}_p\times\mathbb{F}_p}}(n,p)\right)\\ &\geq \prod_{p|n} L_3^{F_3(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(n,p)\\ &\geq \prod_{p|s} \frac{1}{3}\Big(\gcd(n^3-1,p^3-1,n-p) - \gcd(n-1,p-1)\Big).\end{aligned}$$

As $s \in S^{(3)}_{\alpha,\varepsilon}(x,a)$ so for all prime $p \mid s$ we have $p^3-1 \mid M$ and $p^3-1 \mid a-p$. Thus $p^3-1 \mid (n-a)-(n-p)$ and we know that $M \mid n-a$ by the first claim so $p^3-1 \mid n-p$. Consider

$$\begin{aligned}(n-p)^3 = n^3 - 3n^2p + 3np^2 - p^3 &= n^3 - 3n^2p + 3np^2 - p^3 - 1 + 1\\ &= (n^3-1) - (p^3-1) + 3np(p-n).\end{aligned}$$

We know $p^3-1 \mid n-p$ and $p^3-1 \mid p^3-1$, so $p^3-1 \mid n^3-1$. Thus

$$\begin{aligned}\prod_{p|n} L_3^{F_3(x)}(n,p) &\geq \prod_{p|s} \frac{1}{3}\Big(\gcd(n^3-1,p^3-1,n-p) - \gcd(n-1,p-1)\Big)\\ &\geq \prod_{p|s} \frac{1}{3}(p^3-1-(p-1))\\ &\geq 3^{-k_\alpha(x)} \prod_{p|s} p^{3-o(1)}\\ &\geq 3^{-k_\alpha(x)} s^{3-\mathrm{o}(1)}\\ &\geq 3^{\frac{(\log x)\,\mathrm{o}(1)}{\alpha \log\log x} - \frac{\log x}{\alpha \log\log x}} s^{3-\mathrm{o}(1)}\\ &\geq 3^{-\frac{\log x}{\alpha\log\log x}} s^{3-\mathrm{o}(1)}\\ &\geq x^{-\mathrm{o}(1)} \left((\log x)^{-k_\alpha(x)\varepsilon(3-o(1))}\right) \frac{x^{3-o(1)}}{M^{L(3-o(1))}}.\end{aligned}$$

By definition 4.29 we have $(\log x)^{k_\alpha(x)\varepsilon(3-o(1))} = (\log x)^{(\alpha^{-1}-\mathrm{o}(1)\frac{\log x}{\log\log x})\varepsilon(3-o(1))}$. Now con-

sider $A = (\log x)^{(\alpha^{-1}-o(1))\frac{\log x}{\log\log x}\varepsilon(3-o(1))}$ so $A = x^{3\frac{\varepsilon}{\alpha}-o(1)}$. Then we have

$$x^{-o(1)}\left((\log x)^{-k_\alpha(x)\varepsilon(3-o(1))}\right)\frac{x^{3-o(1)}}{M^{L(3-o(1))}} \geq x^{-o(1)}x^{(-3\frac{\varepsilon}{\alpha}+o(1))}\frac{x^{3-o(1)}}{x^{o(1)}}$$
$$\geq x^{3-3\frac{\varepsilon}{\alpha}-o(1)}. \qquad \square$$

The following theorem generalizes the proof of [Fiori and Shallue, 2020, Theorem 27].

Theorem 4.36. *For any value of $\alpha > 1$ satisfying Proposition 4.27 we have the asymptotic inequality*

$$\sum_{n<x} L_3^{F_3(x)}(n) \geq x^{4-\alpha^{-1}-o(1)}$$

as $x \to \infty$.

Proof. Note that $n = sq$ where $s \in S_\alpha(x)$, and $q = q_1q_2$ such that q_1 and q_2 are prime. By referring to the results that we obtained from Proposition 4.33 and Lemma 4.35, we have

$$\sum_{n<x} L_3^{F_3(x)}(n) \geq \sum_{\substack{sq<x \\ s\in S^{(3)}_{\alpha,\varepsilon}(x)}} L_3^{F_3(x)_{\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}\times\mathbb{F}_{p^3}}}(sq,p)$$
$$\geq (x^{1-\alpha^{-1}+o(1)})(x^{3-\varepsilon\frac{3}{\alpha}-o(1)})$$
$$\geq x^{4-\frac{3\varepsilon+1}{\alpha}-o(1)}$$
$$\geq x^{4-\alpha^{-1}-o(1)}.$$

It holds for all $\varepsilon > 0$, so it holds when $\varepsilon \to 0$ as well. $\square$

In the previous part, we worked on Theorems and Lemmas which required the strong conjecture 4.20, Now we want to introduce the alternative α that relies on weaker conjecture.

Weaker form of Lemma 4.35

At first we define the following set which we would be expected to be larger than the set

$P_\alpha(x,a)$.

Definition 4.37. $P'_{\alpha,\ell}(x) = \{p < (\log x)^\alpha \mid p = 1 \mod \ell, p-1 \mid M\}$, where ℓ is a prime number.

In contrast to Conjecture 4.20 for which no strategy of proof is known, the claim of Conjecture 4.38 would be expected to follow from the same methods used in the proof of [Dartyge et al., 2002, Theorem 1.2]. These are outside the scope of this thesis, so they remain conjectures in this thesis.

Conjecture 4.38. For all $1 < \alpha \leq 2$ we have that $\left|P'_{\alpha,\ell}(x)\right| \geq (\log x)^{\alpha - o(1)}$ as $x \to \infty$.

The value 2 above comes from using Remark 19 and Definition 4.37. We expect $\alpha < 2$, by applying $F(x) = x - 1$ where $g = 1$ and $k = 1$.

Definition 4.39. $S^{(3)}_{\alpha,\varepsilon}(x,a)$ is the set of integers s which are the product of $k_\alpha(x)$ distinct elements from

$$P'_{\alpha,\ell}(x,a) \backslash P'_{\alpha-\varepsilon,\ell}(x,a).$$

Lemma 4.40. *Let L be an upper bound for Linnik's constant. Given any element s of $S^{(3)}_{\alpha,\varepsilon}(x,a)$ and $1 < \alpha < 2$ there exists a number $q < M^{2L}$ such that*

1. $(sq)^3 = 1 \,(\mathrm{mod} M)$, *and* $(sq) \neq 1 \,(\mathrm{mod}\, \ell)$,
2. $\gcd(q,s) = 1$, *and*
3. $\prod_{p|q} \frac{1}{3}\left(\gcd(n^3-1, p-1) - \gcd(n-1, p-1)\right) > 0$.

Moreover, if $n = sq$ then

$$L_3^{F_3(x)} \geq x^{1 - \frac{\varepsilon}{\alpha} - o(1)}$$

as $x \to \infty$.

Proof. We construct q as the product of two primes q_1 and q_2. We write $M = 7^{r_1} \cdot 13^{r_2} \cdot M'$ such that $\gcd(7, M') = 1$ and $\gcd(13, M') = 1$. Now, we construct the following system of congruences

$$sq_1 \equiv 2 \pmod 7 \qquad q_1 \equiv 1 \pmod{M'} \qquad q_1 \equiv 1 \pmod{13} \tag{4.12}$$

$$q_2 \equiv 1 \pmod 7 \qquad q_2 \equiv s^{-1} \pmod{M'} \qquad sq_2 \equiv 3 \pmod{13}. \tag{4.13}$$

This system has a solution by the Chinese Remainder Theorem (CRT). Additionally, by Linnik's theorem you can bound $q < M^L$ and these provide all we need for the first condition. For the third condition, we want to show that

$$\big(\gcd(n^3-1, q_1-1) - \gcd(n-1, q_1-1)\big)\big(\gcd(n^3-1, q_2-1) - \gcd(n-1, q_2-1)\big) \neq 0.$$

By equation (4.12), we have

$$13 \mid n^3-1, \quad 13 \mid q_1-1, \text{ and } \quad 13 \nmid n-1,$$

and thus $13 \mid \gcd(n^3-1, q_1-1)$ but $13 \nmid \gcd(n-1, q_1-1)$. Then $\gcd(n^3-1, q_1-1) - \gcd(n-1, q_1-1) \neq 0$. Also, by equation (4.13), we have

$$7 \mid n^3-1, \quad 7 \mid q_2-1, \text{ and } \quad 7 \nmid n-1,$$

then $7 \mid \gcd(n^3-1, q_2-1)$ but $7 \nmid \gcd(n-1, q_2-1)$. Then $\gcd(n^3-1, q_2-1) - \gcd(n-1, q_2-1) \neq 0$. Hence the third case is verified.

For the last condition, we have

$$\begin{aligned}\prod_{p|n} L_3^{F_3(x)}(n,p) &\geq \prod_{p|s} \frac{1}{3}\Big(\gcd(n^3-1,p-1)-\gcd(n-1,p-1)\Big)\\ &\geq \prod_{p|s} \frac{1}{3}(p-1-\frac{p-1}{7}))\\ &\geq (\frac{7}{2})^{-k_{\alpha'}(x)} \prod_{p|s} p^{o(1)}\\ &\geq 4^{-k_{\alpha'}(x)} \prod_{p|s} p^{o(1)}\\ &\geq x^{-o(1)} \left((\log x)^{-k_{\alpha(x)}\varepsilon(4-o(1))}\right) \frac{x^{1-o(1)}}{M^{L(1-o(1))}}\\ &\geq x^{1-\frac{\varepsilon}{\alpha'}-o(1)}.\end{aligned}$$

□

In the following theorem that is a weaker form of theorem 4.38, we are going to use Conjecture 4.36 as an assumption.

Theorem 4.41. *For any value of* $1<\alpha<2$ *satisfying Conjecture 4.38 we have the asymptotic inequality*

$$\sum_{n<x} L_3^{F_3(x)}(n) \geq x^{2-\alpha^{-1}-o(1)}$$

as $x \to \infty$.

Proof. The proof structure is exactly similar to Theorem 4.36. □

For the last part of this section, we want to interpret the lower bound for $L_3^{F_1(x)}(n)$ and $L_3^{F_2(x)}(n)$. So at first, we define the sets $P_\alpha^1(x,a)$ and $P_\alpha^2(x,a)$.

Definition 4.42. We defined the set $P_\alpha^1(x) = \{p < (\log x)^\alpha$ such that $p-1 \mid M\}$ and $P_\alpha^2(x,a) = \{p < (\log x)^\alpha \mid a = p \mod (p^2-1), p^2-1 \mid M\}$, where $a^2-1 = 0 \pmod M$.

Proposition 4.43. *For all* $1<\alpha\leq 2$ *we have that* $\left|P_\alpha^1(x)\right| \geq (\log x)^{\alpha-o(1)}$ *as* $x \to \infty$.

Proof. In the Definition 4.42, $F(x) = x - 1$ so $g = 1$ and $k = 1$ by applying the Remark 19 we find $\alpha^{-1} > 1 - 1/2$ then $\alpha < 2$. □

Proposition 4.44. *For all* $1 < \alpha \leq 4/3$ *we have that* $\left|P_\alpha^2(x,a)\right| \geq (\log x)^{\alpha - o(1)}$ *as* $x \to \infty$.

Proof. In the Definition 4.42, $F(x) = x^2 - 1$ thus $g = 1$ and $k = 2$ by applying the Remark 19 we find $\alpha^{-1} > 1 - 1/4$ then $\alpha < 4/3$. □

4.3.1 Lower Bound For $L_3^{F_1(x)}(n)$

Definition 4.45. $S_{\alpha,\varepsilon}^{(3)}(x)$ be the set of integers s which are the product of $k_\alpha(x)$ distinct elements from

$$P_\alpha^1(x) \backslash P_{\alpha-\varepsilon}^1(x).$$

Lemma 4.46. *Let L be an upper bound for Linnik's constant. Given any element s of* $S_{\alpha,\varepsilon}^{(3)}(x)$ *and* $1 < \alpha < 2$ *there exists a prime number* $q < M^L$ *such that*

1. $sq = 1 \pmod{M}$,
2. $\gcd(q,s) = 1$,
3. $\left(\gcd(n-1,q-1)^3 - \gcd(n-1,q-1)^2\right) \neq 0$.

Moreover, if $n = sq$ *then*

$$L_3^{F_1(x)}(n) \geq x^{3 - 3\frac{\varepsilon}{\alpha} - o(1)}$$

as $x \to \infty$.

Proof. For the first claim, all prime divisors of $s \in S_{\alpha,\varepsilon}^{(3)}(x,a)$ are greater than all prime divisors of M since all $p|s$ satisfy $(\log x)^{\alpha-\varepsilon} < p < (\log x)^\alpha$ where $1 < \alpha < 2$. Then $\gcd(s,M) = 1$. Now by Linnik's theorem, we can choose $q < M^L$ to be the smallest prime

such that $sq = 1 (\bmod M)$ where $\gcd(q,s) = 1$. The third and forth claims are obvious. For the last part, we use Theorem 4.15, equation (4.1)

$$\begin{aligned}
L_3^{F_1(x)}(n) &= \prod_{p|n} \left(L_3^{F_1(x)_{\mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p}}(n,p) + (-1) L_3^{F_1(x)_{\mathbb{F}_p \times \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}}}(n,p) + L_3^{F_1(x)_{\mathbb{F}_{p^3} \times \mathbb{F}_{p^3} \times \mathbb{F}_{p^3}}}(n,p) \right) \\
&\geq \prod_{p|s} L_3^{F_1(x)_{\mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p}}(n,p) \\
&= \prod_{p|s} \frac{1}{3!} \left(\gcd(n-1,p-1)^3 - \gcd(n-1,p-1)^2 \right) \\
&\geq \prod_{p|s} \frac{1}{6} ((p-1)^3 - (p-1)^2) \\
&= 6^{-k_\alpha(x)} \prod_{p|s} (p^3 - 4p^2 + 5p) \\
&\geq 6^{-k_\alpha(x)} \prod_{p|s} p^{3-o(1)} \\
&\geq 6^{-k_\alpha(x)} s^{3-\mathrm{o}(1)} \\
&\geq x^{-\mathrm{o}(1)} \left((\log x)^{-\frac{\log x - L \log M}{\alpha \log \log x} \varepsilon (3-o(1))} \right) \frac{x^{3-o(1)}}{M^{L(3-o(1))}} \\
&\geq x^{3-3\frac{\varepsilon}{\alpha}-\mathrm{o}(1)}.
\end{aligned}$$

To get the fourth line above, we note that $\gcd(n-1,p-1) = p-1$ since by Definition 4.42 and the first condition, we know

$$p-1 \mid M \mid n-1,$$

and we get the result. □

Theorem 4.47. *For any value of* $1 < \alpha < 2$ *satisfying Proposition 4.43 we have the asymptotic inequality*

$$\sum_{n<x} L_3^{F_1(x)}(n) \geq x^{4-\alpha^{-1}-o(1)}$$

as $x \to \infty$.

Proof. The proof structure is similar to Theorem 4.36. □

4.3.2 Lower Bound For $L_3^{F_2(x)}(n)$

Definition 4.48. $S^{(3)}_{\alpha,\varepsilon}(x)$ be the set of integers s which are the product of $k_\alpha(x)$ distinct elements from

$$P^2_\alpha(x,a)\backslash P^2_\alpha(x,a).$$

Lemma 4.49. *Let L be an upper bound for Linnik's constant. Given any element s of $S^{(3)}_{\alpha,\varepsilon}(x,a)$ and $1<\alpha<4/3$ there exists a number $q<M^{2L}$ such that*

1. $sq = a \pmod M$,
2. $\gcd(q,s)=1$, *and*
3. $\prod_{p|q}\frac{1}{2}\Big(\gcd(n-1,p-1)\gcd(n^2-1,p^2-1,n-p)-\gcd(n-1,p-1)^2\Big)>0$.

Moreover, if $n=sq$ then

$$L_3^{F_2(x)}(n)\geq x^{3-3\frac{\varepsilon}{\alpha}-o(1)}$$

as $x\to\infty$.

Proof. The proof of this lemma is similar to the proof of lemma 4.40. □

Theorem 4.50. *For any value of $1<\alpha<4/3$ satisfying Proposition 4.44 we have the asymptotic inequality*

$$\sum_{n<x} L_3^{F_2(x)}(n)\geq x^{4-\alpha^{-1}-o(1)}$$

as $x\to\infty$.

Proof. The proof structure is similar to Theorem 4.36. □

4.4 Upper Bound

In this section, we are going to show that there is an upper bound for $L_3^{F_3(x)}(n)$ given by $x^4\mathcal{L}(x)^{-1+o(1)}$. Also, briefly we will provide similar upper bounds for $L_3^{F_1(x)}(n)$ and $L_3^{F_2(x)}(n)$.

The following definition generalizes [Fiori and Shallue, 2020, p. 508].

Definition 4.51. Given an integer m, define

$$\lambda_1(m) = \operatorname{lcm}_{p|m}(p-1), \quad \lambda_2(m) = \operatorname{lcm}_{p|m}(p^2-1), \quad \lambda_3(m) = \operatorname{lcm}_{p|m}(p^3-1).$$

The following lemma generalizes the proof of [Fiori and Shallue, 2020, Lemma 33] and [Erdős and Pomerance, 1986, p. 264].

Lemma 4.52. *As $x \to \infty$ we have*

$$\#\{m \le x : \lambda_3(m) = n\} \le x \cdot \mathcal{L}(x)^{-1+o(1)}.$$

Proof. For convenience, first we simplify the right hand side of the inequality.

$$x \cdot \mathcal{L}(x)^{-1+o(1)} = x \cdot \exp\left(\frac{\log x \log_3 x}{\log_2 x}\right)^{-1+o(1)} = x^{\left(\frac{\log_2 x - \log_3 x}{\log_2 x} + o\left(\frac{\log_3 x}{\log_2 x}\right)\right)}.$$

So for any $c > 0$ with $m \le x$ we have $1 \le (\frac{x}{m})^c$ we can compute:

$$\begin{aligned}\#\{m \le x : \lambda_3(m) = n\} = \sum_{\substack{m \le x \\ \lambda_3(m)=n}} 1 &\le x^c \sum_{\lambda_3(m)=n} m^{-c} \\ &\le x^c \sum_{\substack{p|m \\ p^3-1|n}} m^{-c} \le x^c \sum_{\substack{p|m \\ p-1|n}} m^{-c}.\end{aligned}$$

Now we apply the Euler Product Theorem to $\sum_{\substack{p|m \\ p-1|n}} m^{-c}$, namely

$$\sum_{\substack{p-1|n\\ p|m}} m^{-c} = \prod_{p-1|n} \left(1-p^{-c}\right)^{-1}.$$

Rename the product by A and consider $c = 1 - \frac{\log_3 x}{\log_2 x}$. If we can show that

$$A < x^{o\left(\frac{\log_3 x}{\log_2 x}\right)} \text{ or } \log A = o(\log x \log\log\log x/\log\log x), \tag{4.14}$$

then we have

$$x^c \sum_{\substack{p-1|n\\ p|m}} m^{-c} = x^{1-\frac{\log_3 x}{\log_2 x}} \cdot A = x^{\left(\frac{\log_2 x - \log_3 x}{\log_2 x}\right)} \cdot A \leq x^{\left(\frac{\log_2 x - \log_3 x}{\log_2 x}\right)} \cdot x^{o\left(\frac{\log_3 x}{\log_2 x}\right)} = x \cdot \mathcal{L}(x)^{-1+o(1)},$$

which would give the result.

To show the inequality (4.14), take x large enough such that $\frac{\log_3 x}{\log_2 x} \leq 1/2$, from this it follows for all primes $p \geq 2$ and $c \geq 1/2$ we have $\frac{1}{1-p^{-c}} \leq \frac{1}{1-2^{-1/2}} \leq 4$. Now we have

$$\begin{aligned}
\log A = -\sum_{p-1|n} \log(1-p^{-c}) = \sum_{p-1|n} \sum_{t=1}^{\infty} \frac{p^{-ct}}{t} &= \sum_{p-1|n} (p^{-c} + \frac{1}{2}p^{-2c} + \frac{1}{3}p^{-c} + \cdots) \\
&\leq \sum_{p-1|n} \frac{p^{-c}}{1-p^{-c}} \\
&\leq 4 \sum_{d|n} d^{-c} \\
&\leq 4 \prod_{p|n} \left(1-p^{-c}\right)^{-1},
\end{aligned}$$

where on the third line we took $d = p-1$. Then we again take the logarithm of both sides,

so we have

$$\begin{aligned}\log\log A \le \log 4 + \sum_{p|n} \log(1-p^{-c}) &\le \log 4 + \sum_{p|n} \frac{p^{-c}}{1-p^{-c}} \\ &\le \log 4 + 4\sum_{p|n} p^{-c} \\ &= \log 4 + 4 \sum_{\substack{i=1 \\ p_i|n \\ p_i \text{ is the i-th prime}}}^{\#p|n} p_i^{-c}.\end{aligned}$$

The largest possible values of $\sum_{\substack{i=1 \\ p_i|n}}^{\#p|n} p_i^{-c}$ comes from n divisible by largest possible number of small primes, namely when it is the product of all primes up to $\log(x)$ and hence

$$\log 4 + 4 \sum_{\substack{i=1 \\ p_i|n \\ p_i \text{ is the i-th prime}}}^{\#p|n} p_i^{-c} < \sum_{p<\log x} p^{-c} < \sum_{|p|<\log x} p^{-c}.$$

We estimate the $\sum_{|p|<\log x} p^{-c}$ using the partial summation formula, then we have

$$\begin{aligned}\sum_{|p|<\log x} p^{-c} &= \pi(\log x)\frac{1}{(\log x)^c} + c\int_2^{\log x} \pi(t) t^{-c-1} dt \\ &\ll \frac{\log x}{\log\log x}\cdot(\log x)^{-c} + c\int_2^{\log x} \frac{t^{-c}}{\log t} dt \\ &\ll \frac{(\log x)^{1-c}}{\log\log x} + c\int_2^{\sqrt{\log x}} \frac{t^{-c}}{\log t} dt + c\int_{\sqrt{\log x}}^{\log x} \frac{t^{-c}}{\log t} dt \\ &\ll \frac{(\log x)^{1-c}}{\log\log x} + \frac{c}{(1-c)}(\log x)^{\frac{1-c}{2}} + \frac{2c}{(1-c)\log\log x}(\log x)^{1-c} \\ &= O\left(\frac{(\log x)^{1-c}}{(1-c)\log\log x}\right).\end{aligned}$$

Hence $\log\log A = O\left(\frac{(\log x)^{1-c}}{(1-c)\log\log x}\right)$. Now we substitute c that is equal to $1 - \frac{\log_3 x}{\log_2 x}$, so we have

$$\log\log A = O\left(\frac{\log x^{\frac{\log_3 x}{\log_2 x}}}{\log_3 x}\right) = O\left(\frac{\log_2 x}{\log_3 x}\right),$$

or there exists positive constant C' such that $\log A < \log(x)^{C'/\log\log\log(x)}$. On the other hand we have $\log(x)^{C'/\log\log\log(x)} = o\left(\log x \frac{\log_3 x}{\log_2 x}\right)$ and so $\log A \ll \log x \frac{\log_3 x}{\log_2 x}$ or $\log A = o(\log x \log\log\log x/\log\log x)$ and it gives the result. □

The following lemma generalizes the proof of [Fiori and Shallue, 2020, Lemma 34].

Lemma 4.53. *Assume n is composite and let k be the smallest integer such that $\lambda_3(n) \mid k\left(n^3-1\right)$. Then*

$$L_3^{F_3(x)}(n) \leq \frac{1}{k}\prod_{p\mid n}\left(p^3-1\right).$$

Proof. We introduce the smallest integer k by the equation $k = \lambda_3(n)/\gcd\left(\lambda_3(n), n^3-1\right)$. Also by Lemma 4.16 we know that $L^{F_3(x)}(n) \leq \prod_{p\mid n}\gcd\left(n^3-1, p^3-1\right)$. To prove the lemma, it is sufficient to prove

$$\frac{\lambda_3(n)}{\gcd\left(\lambda_3(n), n^3-1\right)}\prod_{p\mid n}\gcd\left(p^3-1, n^3-1\right) \Big| \prod_{p\mid n}\left(p^3-1\right).$$

Note that the above claim is stronger than the claim of the Lemma. Without lose of generality we may consider a prime q and the integer $\alpha > 0$ such that

$$q^{\alpha} \Big\| \frac{\lambda_3(n)}{\gcd\left(\lambda_3(n), n^3-1\right)}\prod_{p\mid n}\gcd\left(p^3-1, n^3-1\right).$$

Now the approach here is to show that $q^{\alpha} \big| \prod_{p\mid n}\left(p^3-1\right)$.

Thus there is integer $d \geq 0$ such that $q^d || n^3-1$. We fix the integer d throughout the proof. Also, there is integer $\beta_i \geq 0$ such that $q^{\beta_i} \mid p_i^3-1$. Based on the definition of $\lambda_3(n)$ as an least common multiple of p_i^3-1, we have $q^{\max\beta_i} || \lambda_3(n)$.
Now two cases happen; First, $d > \beta_i$ for all i and the second one is $d < \beta_i$ for some β_i.

- $d \geq \beta_i$ for all i, and $q^{\beta_i} \mid p_i^3-1$. We set the order for β_i and without loss of generality,

we may consider $\beta_1 \le \beta_2 \le \cdots \le \beta_r$, namely, β_r is the largest power of q which $q^{\beta_r} \mid p_r^3 - 1$. Then we have $\alpha = \max \beta_i - \min(\max \beta_i, d) + \sum_{i=1}^r \beta_i = \sum_{i=1}^r \beta_i$ from the following divisibility

$$q^{\alpha} \Big\| \frac{q^{\max \beta_i}}{q^{\min(\max \beta_i, d)}} q^{\sum_{i=1}^r \beta_i}, \text{ or } q^{\alpha} \Big\| q^{\sum_{i=1}^r \beta_i}.$$

On the other hand, $q^{\beta_1} q^{\beta_2} \cdots q^{\beta_r} \Big| \prod_{p_i | n} (p_i^3 - 1)$ meaning $q^{\sum_{i=1}^r \beta_i} \Big| \prod_{p_i | n} (p_i^3 - 1)$.

- Otherwise, if d is not larger than all of the β_i we may assume, $\beta_1 \le \beta_2 \le \cdots \beta_j \le d \le \beta_{j+1} \cdots \le \beta_r$. So

$$q^{\alpha} \Big\| q^{\max \beta_i - \min(\max \beta_i, d)} q^{\sum_{i=1}^j \beta_i} q^{d(r-j)} \Big| q^{\beta_r} q^{\sum_{i=1}^j \beta_i} q^{d(r-j-1)}$$
$$\Big| q^{\beta_r} q^{\sum_{i=1}^j \beta_i} q^{\sum_{i=j+1}^{r-1} \beta_i} = q^{\sum_{i=1}^r \beta_i} \Big| \prod_{p | n} \left(p^3 - 1\right).$$

Hence, we get the result. □

The following theorem generalizes the proof of [Fiori and Shallue, 2020, Theorem 36].

Theorem 4.54. *For large x we have the asymptotic inequality*

$$\sum_{n<x} L_3^{F_3(x)}(n) \le x^4 \mathcal{L}(x)^{-1+o(1)}.$$

Proof. Let $C_k(x)$ denote the set of composite $n \le x$ where k is the smallest integer such that $\lambda_3(n) \mid k(n^3 - 1)$. If $n \in C_k(x)$, then $L_3^{F_3(x)}(n) \le \frac{1}{k} \prod_{p | n} p^3 = n^3/k$. Thus

$$\begin{aligned}
\sum_{n<x} L_3^{F_3(x)}(n) = \sum_k \sum_{n \in C_k(x)} L_3^{F_3(x)}(n) &\le \sum_k \sum_{n \in C_k(x)} \frac{n^3}{k} \\
&\le \sum_{k \ge \mathcal{L}(x)} \sum_{n \in C_k(x)} \frac{n^3}{\mathcal{L}(x)} + \sum_{k \le \mathcal{L}(x)} \sum_{n \in C_k(x)} \frac{n^3}{k} \\
&\le \frac{x^4}{4\mathcal{L}(x)} + x^3 \sum_{k \le \mathcal{L}(x)} \frac{|C_k(x)|}{k}.
\end{aligned}$$

By the Euler's summation formula, we find that $\sum_{k\leq\mathcal{L}(x)}\frac{1}{k}=\log(\mathcal{L}(x))+o(1)$ which is less than $\mathcal{L}(x)^{o(1)}$. Thus the proof will be completed if we can prove that

$$|C_k(x)|\leq x\mathcal{L}(x)^{-1+o(1)}.$$

For every $n\in C_k(x)$, either

1. $n\leq x/\mathcal{L}(x)$
2. n is divisible by some prime $p>\sqrt[3]{k\mathcal{L}(x)}$, and/or
3. $n\geq x/\mathcal{L}(x)$ and $p\mid n$ implies $p\leq\sqrt[3]{k\mathcal{L}(x)}$.

By assumption the number of integers in the first case is at most $x\mathcal{L}(x)^{-1}$.
In the second case, if $n\in C_k(x)$ and $p\mid n$, notice that p^3-1 divides $k\left(n^3-1\right)$ by Lemma 4.53. Then

$$\frac{p^3-1}{\gcd\left(k,p^3-1\right)}\mid n^3-1, \tag{4.15}$$

namely,

$$n^3=1 \bmod \frac{p^3-1}{\gcd\left(k,p^3-1\right)}. \tag{4.16}$$

By the application of Chinese remainder theorem, we find that the number of solutions for n mod $\frac{p^3-1}{\gcd\left(k,p^3-1\right)}$ is at most $3^{\omega\left(\frac{p^3-1}{\gcd\left(k,p^3-1\right)}\right)+1}$.

Take $\omega_{\max}(p^3-1)$ as the maximum number of distinct prime factors of p^3-1 for all $p\mid n$, then we have

$$3^{\omega\left(\frac{p^3-1}{\gcd\left(k,p^3-1\right)}\right)+1}\leq 3^{\omega_{\max}(p^3-1)+1}. \tag{4.17}$$

So in equation (4.16), the number of solutions for n that are less than x and satisfy $p\mid n$ for

all p, modulo $\frac{p^3-1}{\gcd\left(k,p^3-1\right)}$, is bounded by

$$\frac{1}{p}\times\frac{x3^{\omega_{\max}(p^3-1)+1}}{(p^3-1)/\gcd(k,p^3-1)}+C\leq\frac{xk\mathcal{L}(x)^{o(1)}}{p\,(p^3-1)}. \tag{4.18}$$

In (4.18), we have $3^{\omega_{\max}(p^3-1)+1}\leq\mathcal{L}(x)^{o(1)}$. As demonstrated in [Hardy and Wright, 1979, Section 22.10], it has been established that for $n<x$, the inequality $\omega(n)\leq(1+o(1))\frac{\log x}{\log\log x}$ holds. In our specific case, considering the range $p^3-1<n^3<x^3$, we deduce that

$$\begin{aligned}
(\omega_{max}(p^3-1)+1)\log 3 &\leq (1+o(1))\left(\frac{\log x^3}{\log\log x^3}\right)\log 3\\
(\omega_{max}(p^3-1)+1) &\leq (1+o(1))\left(\frac{3\log x}{\log 3+\log_2 x}\right)\\
&\leq (3+o(1))\left(\frac{\log x}{\log_2 x}\frac{\log_3 x}{\log_3 x}\right)\\
&\leq \left(\log x\frac{\log_3 x}{\log_2 x}\right)\frac{(1+o(1))}{\log_3 x}\\
&\leq \log(\mathcal{L}(x))o(1)\\
&\leq o(\log(\mathcal{L}(x))).
\end{aligned}$$

We conclude that the maximum number of n in the second case is

$$\begin{aligned}
\sum_{p>\sqrt[3]{k\mathcal{L}(x)}}\frac{3xk\mathcal{L}(x)^{o(1)}}{p^4(1+o(1))} &\leq \sum_{p>\sqrt[3]{k\mathcal{L}(x)}}\frac{3xk\mathcal{L}(x)^{o(1)}}{p^4}\\
&\leq \sum_{p>\sqrt[3]{k\mathcal{L}(x)}}\frac{3xk}{p^4}\mathcal{L}(x)^{o(1)}\\
&\leq xk\mathcal{L}(x)^{o(1)}\sum_{p>\sqrt[3]{k\mathcal{L}(x)}}\frac{1}{p^4}\\
&= xk\mathcal{L}(x)^{o(1)}\int_{p>\sqrt[3]{k\mathcal{L}(x)}}\frac{1}{p^4}\mathrm{dp}\\
&= x\mathcal{L}(x)^{-1+o(1)}.
\end{aligned}$$

For n in the third case, since all primes dividing n by the assumption of third case are

smaller than $\sqrt[3]{k\mathcal{L}(x)}$, we can construct a divisor d of n such that it satisfies the following inequality

$$\frac{x}{\mathcal{L}(x)\sqrt[3]{k\mathcal{L}(x)}} < d \leq \frac{x}{\mathcal{L}(x)}.$$

To construct such a divisor, we remove primes from n until the remaining integer is smaller than $x/\mathcal{L}(x)$; since each prime dividing n is at most $\sqrt[3]{k\mathcal{L}(x)}$, the lower bound follows, as well.

We have $d \mid n$ so $\lambda_3(d) \mid \lambda_3(n)$. Since $\lambda_3(n) \mid k\left(n^3-1\right)$ then $\lambda_3(d) \mid k\left(n^3-1\right)$, and by a similar argument we had in equations (4.15) and inequality (4.18). We conclude that the number of $n \in C_k(x)$ with $d \mid n$ is at most

$$\frac{x\mathcal{L}(x)^{o(1)}}{d\lambda_3(d)/\gcd\left(k,\lambda_3(d)\right)}.$$

We define the set A by

$$\left\{ d \in \mathbb{Z} \mid \frac{x}{\mathcal{L}(x)\sqrt[3]{k\mathcal{L}(x)}} < d \leq \frac{x}{\mathcal{L}(x)} \right\}.$$

Now, the number of $n \in C_k(x)$ in the third case is at most

$$\begin{aligned}
\sum_{d\in A} \frac{x\mathcal{L}(x)^{o(1)}\gcd\left(k,\lambda_3(d)\right)}{d\lambda_3(d)} &= x\mathcal{L}(x)^{o(1)} \sum_{d\in A} \frac{\gcd\left(k,\lambda_3(d)\right)}{d\lambda_3(d)} \\
&= x\mathcal{L}(x)^{o(1)} \sum_{m\leq x} \frac{1}{m} \sum_{\substack{d\in A \\ \frac{\lambda_3(d)}{\gcd\left(k,\lambda_3(d)\right)}=m}} \frac{1}{d} \\
&\leq x\mathcal{L}(x)^{o(1)} \sum_{m\leq x} \frac{1}{m} \sum_{u\mid k} \sum_{\substack{d\in A \\ \lambda_3(d)=mu}} \frac{1}{d}.
\end{aligned}$$

Note that if $\frac{\lambda_3(d)}{\gcd\left(k,\lambda_3(d)\right)} = m$, then $\lambda_3(d) = m\gcd\left(k,\lambda_3(d)\right)$ for some $u \mid k$. We define the set A_{mu} by

$$\{d \in A;\ \lambda_3(d) = mu\}.$$

To evaluate the inner sum we use partial summation and Lemma 4.52 to get

$$\begin{aligned}
\sum_{\substack{d\in A\\ \lambda_3(d)=mu}}\frac{1}{d} &= \sum_{m}\sum_{\frac{x}{\mathcal{L}(x)\sqrt[3]{k\mathcal{L}(x)}}<d\le\frac{x}{\mathcal{L}(x)}}\chi_{A_{mu}}(d)\frac{1}{d}\\
&\le \sum_{d\in A_{mu}}\chi_{A_{mu}}\Big(\frac{1}{x/\mathcal{L}(x)}\Big)-\int_{x/\mathcal{L}(x)\sqrt[3]{k\mathcal{L}(x)}}^{x/\mathcal{L}(x)}\sum_{d<t}\chi_{A_{mu}}(t)\frac{-1}{t^2}dt\\
&\le \frac{1}{x/\mathcal{L}(x)}\sum_{d\in A_{mu}}1+\int_{x/\mathcal{L}(x)\sqrt[3]{k\mathcal{L}(x)}}^{x/\mathcal{L}(x)}\frac{1}{t^2}\sum_{\substack{d<t\\ d\in A_{mu}}}1dt\\
&\le \frac{\mathcal{L}(x)}{x}\frac{x/\mathcal{L}(x)}{\mathcal{L}(x/\mathcal{L}(x))^{1+o(1)}}+\int_{x/\mathcal{L}(x)\sqrt[3]{k\mathcal{L}(x)}}^{x/\mathcal{L}(x)}\frac{1}{t^2}\frac{x/\mathcal{L}(x)}{\mathcal{L}(x/\mathcal{L}(x))^{1+o(1)}}\mathrm{d}t\\
&\le \frac{1}{\mathcal{L}(x/\mathcal{L}(x))^{1+o(1)}}+\frac{x/\mathcal{L}(x)}{\mathcal{L}(x/\mathcal{L}(x))^{1+o(1)}}\frac{1}{x/\mathcal{L}(x)\sqrt[3]{k\mathcal{L}(x)}}\\
&\le \mathcal{L}(x)^{-1+o(1)},
\end{aligned}$$

for large enough x and uniformly for $k\le\mathcal{L}(x)$. Notice that $\chi_{A_{mu}}(d)$ is a characteristic function over set A_{mu}. Note in the following that we shall use that the count of divisors of an integer k is bounded above by $3^{(1+o(1))\log k/\log\log k}$ (see for instance [Hardy and Wright, 1979, Theorem 317]). Notice that since $k\le\mathcal{L}(x)$ then

$$\begin{aligned}
3^{(1+o(1))\log k/\log\log k} &\le 3^{(1+o(1))\log(\mathcal{L}(x))/\log\log(\mathcal{L}(x))}\\
&= \exp\Big(\log 3^{(1+o(1))\log(\mathcal{L}(x))/\log\log(\mathcal{L}(x))}\Big)\\
&= \mathcal{L}(x)^{o(1)}.
\end{aligned}$$

Thus the count in case (3) is

$$\begin{aligned} x\mathcal{L}(x)^{o(1)} \sum_{m\le x}\frac{1}{m}\sum_{u|k}\sum_{\substack{d\in A\\ \lambda_3(d)=mu}}\frac{1}{d} &\le x\mathcal{L}(x)^{o(1)}\sum_{m\le x}\frac{1}{m}\sum_{u|k}(\mathcal{L}(x)^{-1+o(1)}) \\ &\le x\mathcal{L}(x)^{-1+o(1)}\sum_{m\le x}\frac{1}{m}\sum_{u|k}1 \\ &\le x\mathcal{L}(x)^{-1+o(1)}\sum_{m\le x}\frac{1}{m}3^{(1+o(1))\log k/\log\log k} \\ &\le x\mathcal{L}(x)^{-1+o(1)}3^{(1+o(1))\log k/\log\log k}\log x \\ &\le x\mathcal{L}(x)^{-1+o(1)}. \end{aligned}$$

□

4.4.1 Upper Bound For $L_3^{F_1(x)}(n)$

In this section, we will present the upper bound for $L_3^{F_1(x)}(n)$ and highlight its differences compared to the $L_3^{F_3(x)}(n)$ case. Note that by applying Lemma 4.16, we will focus on three terms, as outlined in inequality (4.4.1).

$$\begin{aligned} L_3^{F_1}(n) \le \prod_{p|n}\max\Big(&\gcd(n-1,p-1)^3, \frac{3}{2}\gcd(n-1,p-1)\gcd(n-1,p^2-1), \\ &\gcd(n-1,p^3-1)\Big). \end{aligned}$$

The following definition generalizes [Fiori and Shallue, 2020, p. 510].

Definition 4.55. We do need a new piece of notation, namely given a prime p we shall define

$$d_n(p) = \begin{cases} (p-1)^3 & \text{when } \gcd(n-1,p-1)^3 \text{ is largest,} \\ (p-1)(p^2-1) & \text{when } \gcd(n-1,p-1)\gcd(n-1,p^2-1) \text{ is largest,} \\ p^3-1 & \text{when } \gcd(n-1,p^3-1) \text{is largest.} \end{cases}$$

Lemma 4.56. *Suppose n is composite and let k be the smallest integer such that $\lambda_1(n) \mid k(n^3-1)$. Then*

$$L_3^{F_1(x)}(n) \leq \frac{1}{k}\prod_{p\mid n} d_n(p).$$

Proof. The proof structure is exactly similar to the Lemma 4.53 with some modification as in [Fiori and Shallue, 2020, Lemma 35]. □

Theorem 4.57. *For large x we have the asymptotic inequality*

$$\sum_{n<x} L_3^{F_1(x)}(n) \leq x^4 \mathcal{L}(x)^{-1+o(1)}.$$

Proof. Let $D_k(x)$ denote the set of composite $n \leq x$ where k is the smallest integer such that $\lambda_1(n) \mid k(n^3-1)$. If $n \in D_k(x)$, then $L_3^{F_1(x)}(n) \leq \frac{1}{k}\prod_{p\mid n} p^3 = n^3/k$. If you check piece wise function $h_n(p)$ for each case, we have $h_n(p) \leq p^3$. So in general, If $n \in D_k(x)$, then $L_3^{F_1(x)}(n) \leq \frac{1}{k}\prod_{p\mid n} p^3 = n^3/k$. The rest of proof is similar to Theorem 4.54 with some modifications. □

4.4.2 Upper Bound For $L_3^{F_2(x)}(n)$

In this section, we will present the upper bound for $L_3^{F_2(x)}(n)$. Note that by applying Lemma 4.16, we will just focus on term $\gcd(n-1,p-1)\gcd(n^2-1,p^2-1)$ in this case.

Lemma 4.58. *Suppose n is composite and let k be the smallest integer such that $\lambda_2(n) \mid k(n^3-1)$. Then*

$$L_3^{F_2(x)}(n) \leq \frac{1}{k}\prod_{p\mid n}(p-1)(p^2-1).$$

Proof. The proof structure is exactly similar to Lemma 4.53. □

Theorem 4.59. *For large x we have the asymptotic inequality*

$$\sum_{n<x} L_3^{F_2(x)}(n) \leq x^4 \mathcal{L}(x)^{-1+o(1)}.$$

Proof. The proof structure is exactly similar to Theorem 4.54. □

Chapter 5

Conclusion and Further Work

In this thesis, we derived explicit formulas for counting cubic liars (f,n). The results we obtained in the cubic case exhibit essentially the same lower and upper bounds as those found by Erdős-Pomerance and Fiori-Shallue for quadratic and Fermat pseudoprimes, respectively once one takes into account the difference in the number of linear, quadratic and cubic polynomials.

Based on the bounds established by Erdős-Pomerance, the probability that (f,n) a Fermat pseudoprime for $n \sim x$ is given by

$$x^{\frac{-8}{23}} \leq Pr((f,n)) \leq \mathcal{L}(x)^{-1+o(1)}.$$

The probability that (f,n) is a quadratic pseudoprime for $n \sim x$, according to the bounds established by Fiori-Shallue, is

$$x^{-\alpha^{-1}-o(1)} \leq Pr((f,n)) \leq \mathcal{L}(x)^{-1+o(1)}.$$

Similarly, in the cubic case, using the bounds we have established, the probability is

$$x^{-\alpha^{-1}-o(1)} \leq Pr((f,n)) \leq \mathcal{L}(x)^{-1+o(1)}.$$

We expect the probability for quadratic pseudoprimes to be lower than those for linear pseudoprimes, despite the fact that the current bounds are similar. Furthermore, we anticipate that the probability for cubic pseudoprimes will be lower that that of the quadratic case. Some ideas to better understand or improve the bounds are as follows.

One interesting area of work would be to improve the precision of the estimates. For example, our bounds all include a $o(1)$ term. It would be interesting to attempt to further analyze this term so as to describe a more precise asymptotic. This might reveal differences between various tests.

An additional interesting discussion is how often $L_3^{F_3}(n,p)$ is equal to zero, and knowing it helps find the actual value of $L_3^{F_3}(n)$. One way to study this would be by computing the actual values of $L_3^{F_3}(n,p)$ and $L_3^{F_3}(n)$. Alternatively, using the Chebotarev density theorem shows the probability of the factorization structures $\mathbb{F}_{p^3} \times \mathbb{F}_{p^3} \times \mathbb{F}_{p^3}$, $\mathbb{F}_{p^2} \times \mathbb{F}_{p^2} \times \mathbb{F}_p$, and $\mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p$ occurring is $\frac{1}{3}$, $\frac{1}{2}$, and $\frac{1}{6}$, respectively. Also, by Lemma 4.11 we know that $L_3^{F_3(x)_{\mathbb{F}_p \times \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}}}(n,p) = 0$ so the consequence is that the probability that $L_3^{F_3(x)}(n) = 0$ should be at least $1 - (1/2)^{\omega(n)}$. Making this estimate more robust, or using it in our upper bounds somehow, would be interesting projects to pursue.

Finally, Generalizing the approach that we used for finding the upper and lower bounds in Chapter 4 will be interesting for polynomials with degrees greater than 3.

Bibliography

[Aebi and Cairns, 2008] Aebi, C. and Cairns, G. (2008). Catalan numbers, primes, and twin primes. *Elemente der Mathematik*, 63(4):153–164.

[Alford et al., 1994] Alford, W. R., Granville, A., and Pomerance, C. (1994). There are infinitely many Carmichael numbers. *Annals of Mathematics*, 139(3):703–722.

[Baillie et al., 2021] Baillie, R., Fiori, A., and Wagstaff Jr, S. (2021). Strengthening the Baillie-PSW primality test. *Mathematics of Computation*, 90(330):1931–1955.

[Baillie and Wagstaff, 1980] Baillie, R. and Wagstaff, S. S. (1980). Lucas pseudoprimes. *Mathematics of Computation*, 35(152):1391–1417.

[Baker and Harman, 1998] Baker, R. and Harman, G. (1998). Shifted primes without large prime factors. *Acta Arithmetica*, 83(4):331–361.

[Barwick, 2016] Barwick (8 April 2016). *Determinants & Permutations Lecture Notes*. MIT.

[Cox, 2011a] Cox, D. A. (2011a). *Galois theory*, volume 61. John Wiley & Sons.

[Cox, 2011b] Cox, D. A. (2011b). *Galois theory*, volume 61. John Wiley & Sons.

[Dartyge et al., 2002] Dartyge, C., Tenenbaum, G., and Martin, G. (2002). Polynomial values free of large prime factors. *Periodica Mathematica Hungarica*, 43:111–119.

[Dent and Mitchell, 2005] Dent, A. W. and Mitchell, C. J. (2005). A companion to user's guide to cryptography and standards.

[Erdős and Renyi, 1956] Erdős, P. and Renyi, R. (1956). On pseudoprimes and carmichael numbers. *Publ. Math. Debrecen*, 4(1956):201–206.

[Erdős and Pomerance, 1986] Erdős, P. and Pomerance, C. (1986). On the number of false witnesses for a composite number. *Mathematics of Computation*, 46(173):259–279.

[Fiori and Shallue, 2020] Fiori, A. and Shallue, A. (2020). Average liar count for degree-2 Frobenius pseudoprimes. *Mathematics of Computation*, 89(321):493–514.

[Gallier and Quaintance, 2017] Gallier, J. and Quaintance, J. (2017). Notes on primality testing and public key cryptography. part I: Randomized algorithms, miller–rabin and solovay–strassen tests. *Philadelphia: University of Pennsylvania*, pages 2–163.

[Gordon and Pomerance, 1991] Gordon, D. M. and Pomerance, C. (1991). The distribution of Lucas and elliptic pseudoprimes. *Mathematics of Computation*, 57(196):825–838.

[Grantham, 1998] Grantham, J. (1998). A probable prime test with high confidence. *Journal of Number Theory*, 72(1):32–47.

[Grantham, 2001] Grantham, J. (2001). Frobenius pseudoprimes. *Mathematics of Computation*, 70(234):873–891.

[Grantham, 2010] Grantham, J. (2010). There are infinitely many Perrin pseudoprimes. *Journal of Number Theory*, 130(5):1117–1128.

[Grantham, 2020] Grantham, J. (2020). An unconditional improvement to the running time of the quadratic frobenius test. *Journal of Number Theory*, 210:476–480.

[Hardy and Wright, 1979] Hardy, G. H. and Wright, E. M. (1979). *An introduction to the theory of numbers*. Oxford university press.

[Jacobsen, 2020] Jacobsen, D. (2020). Pseudoprime statistics, tables, and data. https://ntheory.org/pseudoprimes.html.

[Knapp, 2006] Knapp, A. W. (2006). *Basic algebra*. Springer Science & Business Media.

[Korselt, 1899] Korselt, A. (1899). Probleme chinois. *L'intermédiaire des mathématiciens*, 6:142–143.

[Lehmer, 1930] Lehmer, D. H. (1930). An extended theory of Lucas' functions. *Annals of Mathematics*, pages 419–448.

[Linnik, 1944] Linnik, U. (1944). On the least prime in an arithmetic progression II. The Deuring–Heilbronn phenomenon. *Rec. Math.(Sbornik)*, 15(3):347–368.

[Morain, 1998] Morain, F. (1998). Primality proving using elliptic curves: an update. In *International Algorithmic Number Theory Symposium*, pages 111–127. Springer.

[Pomerance et al., 1980] Pomerance, C., Selfridge, J. L., and Wagstaff, S. S. (1980). The pseudoprimes to $25 \cdot 10^9$. *Mathematics of Computation*, 35(151):1003–1026.

[Rabin, 1980] Rabin, M. O. (1980). Probabilistic algorithm for testing primality. *Journal of number theory*, 12(1):128–138.

[Rosser and Schoenfeld, 1962] Rosser, J. B. and Schoenfeld, L. (1962). Approximate formulas for some functions of prime numbers. *Illinois Journal of Mathematics*, 6(1):64–94.

[Rotkiewicz, 1982] Rotkiewicz, A. (1982). On Euler Lehmer pseudoprimes and strong Lehmer pseudoprimes with parameters L, Q, n arithmetic progressions. *Mathematics of Computation*, 39(159):239–247.

[Smith, 2021] Smith, G. G. (2021). Linear algebra lecture notes-Queens university. https://mast.queensu.ca/ ggsmith/Math110/notes12.pdf.

[Stein, 2005] Stein, W. (2005). Elementary number theory.

[Xylouris, 2011a] Xylouris, T. (2011a). On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions. *Acta Arithmetica*, 150:65–91.

[Xylouris, 2011b] Xylouris, T. (2011b). *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression*. PhD thesis, Universitäts-und Landesbibliothek Bonn.

Appendix A

Appendix

Source codes of Example 2.29

```
#We take R as a polynomial ring
\frac{\mathbb{Z}}{\mathbb{Z}_89}[x]
R=PolynomialRing(GF(89),\text{'x'})
#Means the variable here is "x"
x=R.gen()
{f=x^4+12*x+1}
#S=\frac{\frac{\mathbb{Z}}{\mathbb{Z}_89}[x]}{f(x)}
S=R.quotient(f,\text{'a'})
#Means the variable here is "a",
a=S.gen()
#Here we reduced polynomial f(x) module of polynomial ring
\frac{\mathbb{Z}}{\mathbb{Z}_89}[x]
a^{89}-a
Answer:59*x^3 + 51*x^2 + 19*x + 86


R=PolynomialRing(GF(89),'x')
x=R.gen()
f=x^4+12*x+1
#Here g(x) is the reduced form of polynomial f(x) which we found it
in the previous part
g=59*x^3 + 51*x^2 + 19*x + 86
#Here we want to find the GCD(f(x),g(x))
f.gcd(g)
#Rename it as F_1(x), F_1(x) is the product of 1-degree irreducible
polynomials
F_1=f.gcd(g)
Answer:x+78
```

```
f=x^4+12*x+1
#By the GCD that we found we use the factor code here to factorize
polynomial f(x)
f.factor()
Answer:(x + 78) * (x^3 + 11*x^2 + 32*x + 8)


R=PolynomialRing(GF(89),'x')
x=R.gen()
#f_1(x)= \frac{f_0(x)}{F_1(x)}
f_1=(x^3 + 11*x^2 + 32*x + 8)
S=R.quotient(f_1,'a')
a=S.gen()
a^{(89^2)}-a
Answer:64*a^2 + 86*a + 19


R=PolynomialRing(GF(89),'x')
x=R.gen()
f_1=(x^3 + 11*x^2 + 32*x + 8)
c=64*x^2 + 86*x + 19
f_1.gcd(c)
Answer:1


R=PolynomialRing(GF(89),'x')
x=R.gen()
f_2=(x^3 + 11*x^2 + 32*x + 8)
S=R.quotient(f_2,'a')
a=S.gen()
a^{(89^3)}-a
Answer:0


R=PolynomialRing(GF(89),'x')
x=R.gen()
f_3=1
S=R.quotient(f_3,'a')
a=S.gen()
a^{(89^4)}-a
Answer:0


R=PolynomialRing(GF(89),'x')
x=R.gen()
```

```
f_2=(x^3 + 11*x^2 + 32*x + 8)
S=R.quotient(f_2,'a')
a=S.gen()
a^{(89)}
Answer:25*a^2 + a + 59


f_2(x=25*a^2 + a + 59)
Answer=0
#Checking the third step of Grantham's test
R=PolynomialRing(GF(89),'x')
x=R.gen()
f=x^4+12*x+1
#discriminant f(x)
d=f.discriminant();d
Answer:16

#Legendre symbol \frac{d}{89}
kronecker(d, 89)
Answer:1

T.<x>=PolynomialRing(IntegerModRing(1763))
f=x^2-3*x-1
S=T.quotient(f,'a')
a=S.gen()
a^{(1763)}-a
Answer:1760


y_1=1760
F_1=f.gcd(y_1);F_1
Answer:1


a^{(1763)^2}-a
Answer:0


a^{1763}
Answer:a + 1760


f(x=a+1760)
Answer:1757*a + 18
```

```
T.<x>=PolynomialRing(IntegerModRing(1763))
f=x^2+x+1
S=T.quotient(f,'a')
a=S.gen()
a^{1763}-a
Answer:1761*a + 1762


y_1=1761*x + 1762
F_1=f.gcd(y1);F_1
Answer:1


a^{(1763)^2}-a
Answer:0


F_2=f.gcd(0);F_2
Answer:x^2 + x + 1


a^{1763}
Answer:1762*a + 1762


f(x=1762*a + 1762)
Answer:0


d=f.discriminant();d
Answer:1760


kronecker(d, 1763)
Answer:-1
```