Graduate School ETD Form 9
(Revised 12/07)

PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance

This is to certify that the thesis/dissertation prepared

By Sangil Nahm

Entitled Several Problems in Number Theory

For the degree of Doctor of Philosophy

Is approved by the final examining committee:

Samuel Wagstaff, Jr.
Chair

Freydoon Shahidi

William Heinzer

Edray Goins

To the best of my knowledge and as understood by the student in the *Research Integrity and Copyright Disclaimer (Graduate School Form 20)*, this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

Approved by Major Professor(s): Samuel Wagstaff, Jr.

Approved by: Steven Bell 03/22/2011
Head of the Graduate Program Date

Graduate School Form 20
(Revised 9/10)

PURDUE UNIVERSITY
GRADUATE SCHOOL

Research Integrity and Copyright Disclaimer

Title of Thesis/Dissertation:

Several Problems in Number Theory

For the degree of Doctor of Philosophy

I certify that in the preparation of this thesis, I have observed the provisions of *Purdue University Executive Memorandum No. C-22,* September 6, 1991, *Policy on Integrity in Research.**

Further, I certify that this work is free of plagiarism and all materials appearing in this thesis/dissertation have been properly quoted and attributed.

I certify that all copyrighted material incorporated into this thesis/dissertation is in compliance with the United States' copyright law and that I have received written permission from the copyright owners for my use of their work, which is beyond the scope of the law. I agree to indemnify and save harmless Purdue University from any and all claims that may be asserted or that may arise from any copyright violation.

Sangil Nahm

Printed Name and Signature of Candidate

03/22/2011

Date (month/day/year)

*Located at http://www.purdue.edu/policies/pages/teach_res_outreach/c_22.html

SEVERAL PROBLEMS IN NUMBER THEORY

A Dissertation

Submitted to the Faculty

of

Purdue University

by

Sangil Nahm

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

May 2011

Purdue University

West Lafayette, Indiana

To my mom in heaven

ACKNOWLEDGMENTS

It is a great pleasure to express my thanks to all the people who made this dissertation possible.

I owe my deepest gratitude to my advisor, Dr. Samuel Wagstaff, Jr., whose encouragement, supervision and support enabled me to finish my dissertation.

I would like to thank all my thesis committee members, Dr. Edray Goins, Dr. William Heinzer and Dr. Freydoon Shahidi. I appreciate their guiding my research with passion.

I am grateful to Dr. Peter Montgomery for working with me and suggesting wonderful ideas.

Special thanks goes to Dr. Ning Shang, who as a good friend, always encouraged me when I went through hard times. As a colleague, his suggestion helped me to find one of my research topics.

Finally, I would like to thank my family. They were always supporting me and encouraging me with their best wishes.

The memory in Purdue campus would be unforgettable in my life. I also would like to thank all the people who shared the happy moments with me.

TABLE OF CONTENTS

Page

LIST OF TABLES vi

ABSTRACT vii

1 INTRODUCTION 1
1.1 Topics of the Thesis 1
1.2 Contribution of the Thesis 4
1.3 Structure of the Thesis 6

2 PROBABILITY OF SPLITTING POLYNOMIAL 7
2.1 Introduction 7
2.1.1 Motivation of the Problem 7
2.1.2 Contribution of This Chapter 9
2.1.3 Outline of This Chapter 10
2.2 Preliminary Work 11
2.2.1 Connection to the Point Counting Problem 11
2.2.2 Useful Theorems in the Point Counting Problem 12
2.3 Non-singularity and Irreduciblity 13
2.3.1 Case $n = 3$ 13
2.3.2 General Case 17
2.3.3 Non-singular Condition 20
2.4 Conclusion 24

3 PROBABILITY DISTRIBUTIONS IN THE SQUFOF ALGORITHM . . 30
3.1 Introduction 30
3.1.1 The SQUFOF Algorithm 30
3.1.2 Contribution of This Chapter 30
3.1.3 Outline of This Chapter 31
3.2 Background 31
3.2.1 Binary Quadratic Forms 31
3.2.2 Periodic Continued Fractions 35
3.2.3 Continued Fractions Description of SQUFOF 36
3.2.4 Identifying Proper Square Forms 37
3.3 Probability Distribution 38
3.3.1 Probability Distribution of W 39
3.3.2 Probability Distribution of Q 41
3.4 The Effect of Racing Multipliers 42
3.4.1 Probability Distribution of W 43

Page
3.4.2 Probability Distribution of Q 45
3.5 Conclusion with Experimental Data 46
4 PRIME FACTORS OF $N_p = (p^p - 1)/(p - 1)$ 50
4.1 Introduction 50
4.2 Heuristic Data for Prime Factors 50
4.3 Interpretation of Data 52
4.4 Conclusion 57
5 THE PERIOD OF THE BELL NUMBERS MODULO A PRIME 58
5.1 Introduction 58
5.2 The Heuristic Argument 61
LIST OF REFERENCES 65
VITA 68

LIST OF TABLES

Table		Page
2.1	Arithmetic genus for $3 \leq n \leq 20$ with GP/Pari	14
2.2	Probability of GCD$(f', f'') = 1$	26
2.3	Probability that GCD$(f^p - f, f') = 1$ or has distinct linear factors only	27
3.1	Two-prime statistics for FWRD and QUEUE.	47
3.2	Two-prime racing statistics for FWRD and QUEUE, $m_1 = 1$.	49
4.1	Probability that $2kp + 1$ divides N_p when k is odd	51
4.2	Probability that $2kp + 1$ divides N_p when k is even	52
5.1	Some new prime factors	60

ABSTRACT

Sangil Nahm Ph.D., Purdue University, May 2011. Several Problems in Number Theory. Major Professor: Samuel Wagstaff, Jr.

For a long time, number theory has influenced information security and cryptography. This thesis adds examples of its influence.

The first topic is related with Broadcast Group Key Management (BGKM) in cryptography. After the Access Control Polynomial (ACP) BGKM scheme was proposed [38], people tried to check its basic security properties in BGKM [28]. They found that it has a weakness in the key hiding property by finding a counterexample when $p = 2$. Here, we give strong evidence that it has a weakness in its key hiding property for all sufficiently large primes.

The second topic is a well known integer factoring algorithm SQUFOF, which stands for SQUare FOrm Factorization, invented by Daniel Shanks. At present, SQUFOF is the fastest factoring algorithm for numbers between 10^{10} and 10^{18}. In Gower's thesis [13], he made conjectures about the probability distribution of the number of forms that SQUFOF must examine before finding a proper square form and the number of forms enqueued during the factorization of N. We propose a different probability distribution (geometric rather than exponential) than did Gower, and we use Gower's data to support our conclusions.

The third topic is the period of the Bell numbers $B(n)$ modulo a prime. It was proved by Williams [37] that the minimum period of the sequence $\{B(n) \bmod p\}$, $n = 0, 1, 2, \ldots$, divides $N_p = (p^p - 1)/(p - 1)$. In fact, the minimum period equals N_p for every prime p for which this period is known. Several people have conjectured that the minimum period is always N_p. This thesis presents a heuristic argument supporting the conjecture.

1. INTRODUCTION

1.1 Topics of the Thesis

This dissertation consists of several topics in number theory.

The first topic was derived from the process of researching Broadcast Group Key Management (BGKM) in Cryptography.

Efficient symmetric-key encryption algorithms like AES, Twofish, Blowfish, RC4 are widely used in many Internet-based protocols and applications for securing data. In general, the strength of data encryption with a symmetric-key algorithm depends on the strength of the secret key, which must be known by all participating parties in communication. The process of selecting, distributing, storing and updating secret keys is called key management.

Consider a server that sends data to a group of users in a broadcast session through an open communication channel. To ensure data confidentiality, the server shares a secret group key K with all group members and encrypts the broadcast data using a symmetric encryption algorithm with K as the encryption key. Knowing the symmetric key K, any valid group member can decrypt the encrypted broadcast message. When a new user joins or an existing user leaves the group, a new group key must be generated and redistributed in a secure way to all current group members. This process is called update. The technique to maintain, distribute, and update the group keys is called group key management (GKM).

A number of approaches have been proposed for group key management. The centralized approaches use a single trusted party to generate, distribute and update shared group keys. The decentralized approaches assume an infrastructure of group members and make use of multiple collaborating trusted entities to manage the group

keys. In the distributed approaches, the data server can be treated as a group member, and all group members cooperate to compute the shared group keys.

Roughly speaking, we call a centralized group key management protocol a broadcast GKM (BGKM) scheme if it only uses a broadcast communication channel for update. An important advantage of BGKM is that it is easy to maintain, in that an existing group member does not need to privately communicate with any other party when update happens.

However, the security of such existing schemes have neither been analyzed fully nor proven formally. Our topic is related with the key hiding property, one of the basic security properties in BGKM, in the Access Control Polynomial (ACP) BGKM scheme.

As we will explain later, this problem from computer science leads naturally to the following interesting mathematical problem.

Question 1.1.1 *Given a positive integer n, a prime p and distinct $x_1, \ldots, x_n \in \mathbb{F}_p$, how many a's in $\mathbb{F}_p$ make $\prod_{i=1}^{n}(x-x_i)+a$ a factor linearly in $\mathbb{F}_p[x]$ when p is sufficiently large compared to $n!$?*

The second topic is about a famous integer factoring algorithm SQUFOF, which stands for SQUare FOrm Factorization, invented by Daniel Shanks. During the last few hundred years, many people have spent time looking for good factorization algorithm. As a result, today there are several algorithms to choose from if one needs to factor large numbers. For each size of integer, there is a fastest general purpose algorithm among known methods to factor that size number. At present, the number field sieve (NFS) is best for integers greater than 10^{120},and the quadratic sieve (QS) is best for numbers between 10^{50} and 10^{120}. With 32-bit computer architecture, SQUFOF is clearly the best factoring algorithm for numbers between 10^{10} and 10^{18}, and will likely remain so. SQUFOF is extraordinarily simple and efficient, so it is used in most implementations of NFS and QS to factor small auxiliary numbers arising in factoring large N.

In Gower's thesis, he completed the heuristic argument started by Shanks in [29] and generalized the argument to the case where multipliers are used to factor N. In the last chapter, he posed a problem about the probability distributions of W and Q, which represent the time and space complexity of SQUFOF, respectively. These are the two main measures of the efficiency of the algorithm. Our research in this thesis found a better answer than Gower's under the same assumptions. We support our conclusion with his data from his thesis.

The third topic is about the period of the Bell numbers modulo a prime. The Bell exponential numbers $B(n)$ are positive integers that arise in combinatorics. These numbers have been studied for a long time and have a variety of interesting interpretations. Simply speaking, we can say that $B(n)$ is the number of partitions of a set of n numbers or equivalently, the number of equivalence relations on it.

For a study of the arithmetic properties of $B(n)$, the congruence of Touchard [31],

$$B(n+p) \equiv B(n) + B(n+1) \bmod p$$

for a prime p, is important. It was proved by Williams [37] that the minimum period of the sequence (reduced mod p)

$$B(0), B(1), B(2), \ldots, B(n), \ldots$$

is a divisor of

$$N_p = \frac{p^p - 1}{p - 1}.$$

In fact, the minimum period equals N_p for every prime p for which this period is known. Williams [37] proved this fact for $p = 2, 3$ and 5. Levine and Dalton [20] showed it for $p = 7, 11, 13$ and 17. Wagstaff [33] showed the statement for each prime $p < 102$. With these results, many people conjectured that the minimum period is always N_p. Our thesis presents a heuristic argument supporting the conjecture.

1.2 Contribution of the Thesis

We convert Question 1.1.1 into a point counting problem on an algebraic set. We prove that the algebraic set will be a complete non-singular curve if we assume that it is non-singular, so we can use Weil's inequality to approximate the number of points. Furthermore, we state what the non-singular condition is exactly in terms of the roots in the algebraic closure $\bar{\mathbb{F}}_p$ of $\prod_{i=1}^{n}(x - x_i) + a$. Then we suggest an algorithm to determine whether a given polynomial $f(x) = \prod_{i=1}^{n}(x - x_i)$ satisfies the condition no matter what a is.

According to the algorithm, and under some conjectures and assumptions, we claim that f satisfies the condition at least 98% of the time. With this high probability, the number of a's in Question 1.1.1 is quite a small value. When f satisfies the condition, one can guess the cryptographic key from a menu of two possible keys. In cryptography, if one can do this with probability significantly larger than 0.5, then there is a serious problem with the algorithm. Our result shows that one can guess the key with probability at least 0.98, which is significantly larger than 0.5. This answer proves that ACP-BGKM has a weakness in the key hiding property. Our result motivated the development of a new scheme, Access Control Vector (ACV) BGKM [28].

For the SQUFOF algorithm, we found one assumption Gower actually used, but did not declare. With this assumption, we have a better interpretation of Gower's experimental data. Let W be the number of forms that SQUFOF must examine before finding a proper square form and Q be the number of forms enqueued during factorization of N. In [14], Gower computed the expectations $E[W], E[Q]$ under assumptions he made. He supported his results by experimental data. He recognized that the expectation and the standard deviation for $Y = W/\sqrt[4]{N}$ are approximately equal. So he guessed it must be the exponential distribution. However, according to the assumption we found, W will have a geometric distribution for a given N and Q will have a binomial distribution for given N and W. This explains not only

$Var[Y] \approx E[Y]^2$, but also, $Var[Q] \approx E[Q]^2 + E[Q]$ in Gower's experimental data better than his guess did. Also, we explain why we have a harmonic mean in $E[Y]$ when we race multipliers.

If the conjecture about the period of the Bell numbers $B(n) \bmod p$ fails, then there is a prime factor q of N_p such that the period of $B(n) \mod p$ divides $N = N_p/q$. The period will divide N if and only if $B(N+i) \equiv B(i) \pmod p$ for all i in $0 \le i \le p-1$. Under reasonable assumptions, we show that the probability that the minimum period is N_p is $(1-p^{-p})^{d_p}$, where d_p is the number of distinct prime factors of N_p. In order to estimate d_p, we used a argument similar to that in [32], which uses the Bateman-Horn conjecture and prime number theorem. It is well known that every prime factor of N_p has the form $2kp+1$. Then the expected number of prime factor of N_p between A and B is

$$F_p(A,B) \approx \sum_{\substack{k \\ A<2kp+1\le B}} \frac{2}{\log(2kp)} \cdot \frac{c(k)}{k}, \tag{1.1}$$

where $c(k)/k$ is the probability that $2kp+1$ divides N_p when p and $2kp+1$ are both prime. We found several theorems about $c(k)$ when k varies. The average value of $c(k)$ is $3/4$. On the way to determining the average value of $c(k)$, we discover beautiful divisibility properties of the numbers N_p, like these two theorems we will prove in Chapter 4.

Theorem 1.2.1 *If p is odd and $q = 2p+1$ is prime, then q divides N_p if and only if $p \equiv 1 \bmod 4$.*

Theorem 1.2.2 *If $q = 16p+1$ is prime, then q divides $p^{2p}-1$.*

Substituting the average value of $c(k)$ into (1.1) gives

$$F_p(A,B) \approx \sum_{\substack{k \\ A<2kp+1\le B}} \frac{3}{2k\log(2kp)} \approx \frac{3}{2}\log\left(\frac{\log B}{\log A}\right),$$

so the expected value of d_p is

$$F_p\left(2p, N_p\right) \approx \frac{3}{2}\log\left(\frac{\log N_p}{\log(2p)}\right) = \frac{3}{2}\log\left(\frac{\log_p N_p}{\log_p(2p)}\right) \approx \frac{3}{2}\log p.$$

When p is large, $(1-p^{-p})^{d_p}$ is approximately $1-(3\log p)/(2p^p)$ by the binomial theorem. This shows that the heuristic probability that the minimum period of the Bell numbers modulo p is N_p is exceedingly close to 1 when p is a large prime.

1.3 Structure of the Thesis

The rest of the thesis is organized as follows: Chapter 2 is about the key hiding property of ACP-BGKM. Chapter 3 concerns the probability distributions in the SQUFOF algorithm. Chapter 4 treats the prime factors of N_p, where we evaluate $c(k)$ in (1.1). In Chapter 5, we conclude our heuristic argument for the period of Bell number modulo a prime.

2. PROBABILITY OF SPLITTING POLYNOMIAL

2.1 Introduction

In this chapter we study a problem concerning the security of a proposed Broadcast Group Key Management scheme described in [38]. In this chapter, we show that the scheme is insecure. Our conclusion led others to repair the scheme in [28].

2.1.1 Motivation of the Problem

According to [38], in order to distribute a secret key $K \in \mathbb{F}_p$ to a specific group Ψ, the trusted central server uses an Access Control Polynomial (ACP) in the following way.

1. Compute $H(SID_i, z)$ for each recipient $i \in \Psi$, where SID_i is the personal permanent secret shared with a recipient when he or she registers with the system, H is a a public cryptographic hash function, and z is a random integer which is changed with each use.

2. Compute the Access Control Polynomial with this formula

$$A(x) = \prod_{i \in \Psi} (x - H(SID_i, z)) \in \mathbb{F}_p[x].$$

3. Broadcast $(z, P(x))$, where $P(x) = A(x) + K$. Then each recipient $i \in \Psi$ can obtain K by computing $P(H(SID_i, z))$.

This scheme is called ACP-BGKM. It is simple and elegant, so it has many applications. However, any Broadcast Group Key Management (BGKM) scheme should satisfy the following security properties:

1. Correctness, meaning that a user with a valid SID can derive the correct key with overwhelming probability.

2. Soundness, meaning that the probability that a user without a valid SID can obtain the correct key is negligible.

3. Key Hiding, meaning that a user without a valid SID cannot distinguish the real key from a randomly chosen value in the keyspace with nonnegligible probability.

4. Forward/Backward Key Protecting, meaning that when a user leaves the group, he or she cannot distinguish the new updated key from a random value in the keyspace with nonnegligible probability. Also, when a new user joins the group, he or she cannot learn anything about the previous group keys.

In this thesis, we are interested only in Key Hiding. In order to explain this concept more fully, we introduce the following game.

[The adversary game for ACP-BKGM's key hiding property]

Stage 1. Challenger picks Param (p, the degree of ACP, H).

Stage 2. Challenger sends Param to Adversary.

Stage 3. Adversary picks K_0, K_1 in $\mathbb{F}_p$.

Stage 4. Adversary sends K_0, K_1 to Challenger.

Stage 5. Challenger chooses a random b in $\{0, 1\}$ and a random integer z, produces a random ACP $A(x)$, and then produces $P(x) = A(x) + K_b$.

Stage 6. Challenger sends PubInfo $(P(x), z)$ to Adversary.

Stage 7. Adversary chooses b' in $\{0, 1\}$.

The adversary wins the game if $b = b'$.

Definition 2.1.1 *A BGKM is Key Hiding if for any adversary $\mathcal{A}$, Pr[$\mathcal{A}$ wins the game] $\leq 1/2 + f(k)$, where f is a negligible function in k.*

Definition 2.1.2 *A function $f : \mathbb{N} \to \mathbb{R}$ is negligible if for every positive polynomial $p(\cdot)$ there exists an N such that for all $n > N$, we have $f(n) < 1/p(n)$.*

Unfortunately, ACP-BGKM does not satisfy the key hiding property. In order to show this, first we show the following toy example.

Example 2.1.3 *Let $N = 2$ and the finite field be $\mathbb{F}_2$ in ACP-BGKM. Suppose Challenger broadcasts a polynomial $P(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ through the broadcast channel. Note that in this case, the key space is $\mathbb{F}_2$ and thus ideally the probability that 0 or 1 is the designated group key should be 0.5 for anyone without a valid SID. However, note that $P(x)$ is irreducible over $\mathbb{F}_2$. Hence, the only way to write $P(x)$ in the form $\prod_{i=1}^{N}(x - a_i) + K$ is*

$$P(x) = x(x + 1) + 1.$$

Therefore, knowing only the polynomial $P(x)$, anyone can conclude that the shared group key K must be 1.

In general, to win the adversary game, the adversary can compute two polynomials $A_0(x) = P(x) - K_0$ and $A_1(x) = P(x) - K_1$, and check whether one of them fails to split completely into a product of linear polynomials in $\mathbb{F}_p[x]$. If this happens, the other polynomial must correspond to the real group key.

2.1.2 Contribution of This Chapter

What concerns us now is the probability of choosing a $K \in \mathbb{F}_p$ that makes $P(x)-K$ factor linearly in $\mathbb{F}_p[x]$ for a given $P(x)$. If it is small, the probability that an adversary wins the game in Section 2.1.1 is much more than 1/2.

In our thesis, under a non-singular condition, we show that the number of a's in $\mathbb{F}_p$ which make $\prod_{i=1}^{n}(x - x_i) + a$ factor linearly in $\mathbb{F}_p[x]$ when p is sufficiently large

compared to $n!$ is approximately $p/n!$. Therefore, the probability that $\prod_{i=1}^{n}(x-x_i)+a$ splits completely into a product of linear polynomials in $\mathbb{F}_p[x]$ is about $1/n!$, which is quite a small value. This is the reason why ACP-BGKM does not satisfy the key hiding property.

We also state what the non-singular condition is exactly in terms of the roots in the algebraic closure $\bar{\mathbb{F}}_p$ of $\prod_{i=1}^{n}(x-x_i)+a$. Then we suggest an algorithm to determine whether a given polynomial $f(x)=\prod_{i=1}^{n}(x-x_i)$ satisfies the condition no matter what a is.

According to the algorithm, and under some conjectures and assumptions, we claim that f satisfies the condition at least 98% of the time.

2.1.3 Outline of This Chapter

In Section 2.2, we convert our problem into point counting problem of an algebraic set. Then we introduce the famous Weil's inequality and a genus calculating formula. In Section 2.3, first we show that non-singular condition makes our algebraic set irreducible, that is, a complete non-singular curve. This allows us to use Weil's inequality. Then we state the non-singular condition and suggest an algorithm to catch the $\prod_{i=1}^{n}(x-x_i)$ that do not satisfy the condition. In Section 2.4, we analyze the probability for $\prod_{i=1}^{n}(x-x_i)$ to pass through the algorithm under some conjectures and assumptions. Finally, we compute the probability $\Pr(a \in \mathbb{F}_p | \prod_{i=1}^{n}(x-x_i)+a$ splits over $\mathbb{F}_p) = (1/p)\cdot$ (the number of a) is $1/n!$ and analyze the error using the genus calculating formula.

2.2 Preliminary Work

2.2.1 Connection to the Point Counting Problem

Given distinct values x_i in $\mathbb{F}_p$, our goal is to approximate the number of a's in $\mathbb{F}_p$ which make $\prod_{i=1}^{n}(x - x_i) + a$ factor linearly in $\mathbb{F}_p[x]$ when p is sufficiently large compared to $n!$.

First, we can see that the number of a's in $\mathbb{F}_p$ which make $\prod_{i=1}^{n}(x - x_i) + a$ have repeated roots is at most $n-1$. Suppose that $\prod_{i=1}^{n}(x-x_i)+a = (x-b)^2 g(x)$ for some monic polynomial g over $\mathbb{F}_p$. Use the translation $x \to x+b$. Then $\prod_{i=1}^{n}(x+b-x_i)+a = x^2 g(x+b)$. Therefore, $\sum_{i=1}^{n} \prod_{j=1, j\neq i}^{n}(b - x_j) = 0$ and $a = -\prod_{j=1}^{n}(b - x_j)$. The first equation is a polynomial of b with degree $n-1$. So it has at most $n-1$ solutions. Therefore, we will ignore a's which lead to repeated roots, and assume that all y_i's are distinct in

$$\prod_{i=1}^{n}(x - x_i) + a = \prod_{i=1}^{n}(x - y_i). \tag{2.1}$$

Then for fixed $x_1, \ldots, x_n$, there exists a one-to-one correspondence between a and ordered n-tuples $(y_1 < y_2 < \cdots < y_n)$ in (2.1). The number of a's ignored is negligible due to the size of p. Therefore, from now on, instead of counting the number of a's, we will count the number of ordered n-tuples.

Therefore, we are interested in the number of n-tuples $(y_1, y_2, \ldots, y_n)$ satisfying the following system of equations.

$$\begin{array}{rcccccl} e_1 & := & y_1 + \cdots + y_n & = & x_1 + \cdots + x_n & =: & c_1 \\ e_2 & := & y_1y_2 + y_2y_3 + \cdots & = & x_1x_2 + x_2x_3 + \cdots & =: & c_2 \\ & & \vdots & & \vdots & & \\ e_{n-1} & := & y_1y_2\ldots y_{n-1} + \cdots & = & x_1x_2\ldots x_{n-1} + \cdots & =: & c_{n-1} \end{array} \tag{2.2}$$

where, $\prod_{i=1}^{n}(x - x_i) + a = x^n - c_1x^{n-1} + c_2x^{n-2} - \cdots + (-1)^n c_n + a = \prod_{i=1}^{n}(x - y_i)$, and e_i is the elementary symmetric polynomial with degree i in $\mathbb{F}_p[y_1, \ldots, y_n]$.

Now we can see that the solution of (2.2) is nothing but an intersection of $n-1$ hypersurfaces. Concerning intersection theory, we have the following theorem.

Theorem 2.2.1 *[34, p.86] Let V^r be a variety in S^n, defined over a field k; and let $F_j(X)$, for $1 \leq j \leq s$, be s polynomials in $k[X]$. Then there is a uniquely determined bunch of varieties $\mathfrak{B}$ in S^n, such that a point of S^n is in $\mathfrak{B}$ if and only if it is in V and satisfies all the equations $F_j(X) = 0$, $1 \leq j \leq s$; this bunch is normally algebraic over k, and its components have a dimension at least $r - s$.*

Let $X = Z(I)$, where $I = (\{e_i - c_i | i = 1, \ldots, n-1\})$ be an algebraic set corresponding to the solution of (2.2). By Theorem 2.2.1, X is a uniquely determined bunch of varieties, which is normally algebraic over $\mathbb{F}_p$, and its components have a dimension at least 1.

2.2.2 Useful Theorems in the Point Counting Problem

We prefer most the case that X is a non-singular variety with dimension 1, that is, a non-singular curve because in it we can use the following theorem to count the number of points in X.

Theorem 2.2.2 *[35] Let X be a complete non-singular curve of (geometric) genus g over a finite field $\mathbb{F}_q$. Let $N(X)$ be the number of rational points of X. We have*

$$\left|N(X) - (q+1)\right| \leq 2g\sqrt{q}$$

Finally, we need to compute the genus to explain the accuracy of this approximation. In the case of a non-singular curve, we know that the arithmetic genus and the geometric genus coincide. (See [16, p.181].) The following theorem allows us to compute the arithmetic genus of X easily.

Theorem 2.2.3 *[1] Let S denote the homogeneous coordinate ring $k[x_0, \ldots, x_n]$ of $\mathbb{P}_k^n$, where k is an algebraic closed field. We assume that there are hypersurfaces $H_1, H_2, \ldots, H_r$ of $\mathbb{P}_k^n$ of degree $d_1, \ldots, d_r$ respectively such that $X_r = H_1 \cap \cdots \cap H_r$. The hypersurfaces $H_1, \ldots, H_r$ correspond to homogeneous polynomials $f_1, \ldots, f_r \in S$ of degrees $d_1, \ldots, d_r$ respectively.*

Then the arithmetic genus, $g_a(X_r)$, of X_r is given by the formula

$$g_a(X_r) = \sum_{m=1}^{r} (-1)^{m+n-r} \sum_{1 \le i_1 < \cdots < i_m \le r} \varphi(-d_{i_1} - \cdots - d_{i_m}),$$

where

$$\varphi(z) = \frac{1}{n!}(z+1)(z+2)\cdots(z+n) = \begin{pmatrix} z+n \\ n \end{pmatrix}.$$

Our case has $r = n-1$ and $d_i = i$.

We have computed the arithmetic genus for n up to 20 with GP/Pari in Table 2.1.

In the following section, we will try to find a condition for x_i's or c_i's to make X be a non-singular curve. In order to do that, we need to check the following.

(a) X is absolutely irreducible.

(b) X is non-singular.

(c) $\dim X = 1$.

2.3 Non-singularity and Irreduciblity

2.3.1 Case $n = 3$

Let's begin with the easiest case, which means $n = 3$. We want to count the number of a's which make $(x-x_1)(x-x_2)(x-x_3)+a$ factor into linear terms for given distinct values x_1, x_2,and x_3. That is,

$$(x-x_1)(x-x_2)(x-x_3)+a = (x-y_1)(x-y_2)(x-y_3).$$

The above triple (y_1, y_2, y_3) will be a solution of the following system of equations.

$$\begin{array}{rcccl} y_1+y_2+y_3 & = & x_1+x_2+x_3 & = & c_1 \\ y_1y_2+y_2y_3+y_3y_1 & = & x_1x_2+x_2x_3+x_3x_1 & = & c_2 \end{array} \tag{2.3}$$

Table 2.1
Arithmetic genus for $3 \leq n \leq 20$ with GP/Pari

n	$g_a(X_{n-1})$
3	0
4	4
5	49
6	481
7	4681
8	47881
9	524161
10	6168961
11	78019201
12	1057795201
13	15328051201
14	236626790401
15	3879433958401
16	67345229952001
17	1234444603392001
18	23831057682432001
19	483379214782464001
20	10279010984546304001

As mentioned before, the difference between the number of a's which make f factor linearly and the number of ordered 3-tuples of solutions of (2.3) is at most 2, which is negligible comparing to the size of p.

Let's look at the algebraic set $X = Z(I)$, where $I = (y_1 + y_2 + y_3 - c_1, y_1y_2 + y_2y_3 + y_3y_1 - c_2)$ is an ideal of $\bar{\mathbb{F}}_p[y_1, y_2, y_3]$. We have

$$\begin{aligned} Z(I) &= Z(y_1y_2 + (y_1 + y_2)(c_1 - (y_1 + y_2)) - c_2) \\ &= Z(y_1^2 + y_2^2 + y_1y_2 - c_1y_1 - c_1y_2 + c_2) \end{aligned} \tag{2.4}$$

First, we will determine whether X is irreducible or not. Assume that it is reducible. Then X will be written in the form of $Z((y_1 + ay_2 + c)(y_1 + by_2 + d))$ for some $a, b, c, d \in \bar{\mathbb{F}}_p$. When we compare the coefficients with the coefficients in (2.4), we will get the following two systems of equations.

$$\begin{aligned} ab &= 1 & \qquad c + d &= -c_1 \\ a + b &= 1 & \qquad ad + bc &= -c_1 \end{aligned} \tag{2.5}$$

The first system of equations in (2.5) has a solution (a, b), where $a \neq b$ because p is a large prime. After solving the first system of equations, we can solve the second system of equations in (2.5) and compute $cd = c_1^2/3$. Therefore, X is reducible if and only if $c_1^2 = 3c_2$. In fact, these a, b, c, and d are in $\mathbb{F}_p$ when $p \equiv 1 \pmod 6$.

Second, we determine whether X is non-singular or not. We can compute easily that $(y_1, y_2, y_3) = (c_1/3, c_1/3, c_1/3)$ is the unique singular point of X. It means that X can be singular only when $c_1^2 = 3c_2$.

Third, we determine whether $\dim X = 1$ or not. If we assume that X is irreducible, that is, I is prime, then X is an affine variety. Thus, we can use the following definition.

Definition 2.3.1 *[24, p 224] The dimension of the affine variety X defined over $\mathbb{F}_q$ is the transcendence degree of the absolute function field $\bar{\mathbb{F}}_q(X)$ over $\bar{\mathbb{F}}_q$.*

Theorem 2.3.2 *[17, p 139] Let $e_1, \ldots, e_n$ be the elementary symmetric polynomials in $k[y_1, \ldots, y_n]$. Then they are algebraically independent over k.*

Now we show that if X is an affine variety, then X is a curve.

Theorem 2.3.3 *Let $X = Z(I)$, where $I = (\{e_i - c_i | i = 1, \ldots, n-1\})$ is an ideal of $k[y_1, \ldots, y_n]$, where k is an algebraically closed field. If I is prime, then dim X is 1.*

Proof If I is prime, then the quotient field of the coordinate ring

$$A(X) = k[y_1, \ldots, y_n]/I(X)$$

is a field extension of the quotient field of

$$B(X) = k[e_1, \ldots, e_n]/I \cap k[e_1, \ldots, e_n] \cong k[e_n].$$

In fact, all y_i's are algebraic over the quotient field of $B(X)$ because

$$\prod_{i=1}^{n}(x - y_i) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots + (-1)^n e_n.$$

Therefore, the transcendence degree of the quotient field of $A(X)$ equals the transcendence degree of the quotient field of $B(X)$, which is 1 by Theorem 2.3.2. Consequently, dim $X = 1$ by Definition 2.3.1. ■

Finally, we claim the following statement.

Proposition 2.3.4 *Let $X = Z(I)$, where $I = (y_1+y_2+y_3-c_1, y_1y_2+y_2y_3+y_3y_1-c_2)$ is an ideal of $\bar{\mathbb{F}}_p[y_1, y_2, y_3]$, and $p > 3$.*

If $c_1^2 = 3c_2$, X is a non-singular curve.

If $c_1^2 = 3c_2$, X is a union of two straight lines with one intersection $(c_1/3, c_1/3, c_1/3)$. In this case, if $p \equiv 1 \pmod 6$, then all the points on two straight lines are rational over $\mathbb{F}_p$. However, if $p \equiv 5 \pmod 6$, then the intersection is the only rational point.

Proof By the work done in advance, we just need to show that X has the only rational point $(c_1/3, c_1/3, c_1/3)$ when $c_1^2 = 3c_2$, and $p \equiv 5 \pmod 6$. When $p \equiv 5 \pmod 6$, $f(x) = x^3$ is a bijective map on $\mathbb{F}_p$, because $x^3 - b^3 = (x-b)(x^2+bx+b^2)$, and $\left(\frac{-3b^2}{p}\right) = -1$ for all $b = 0 \in \mathbb{F}_p$. So $(x-\alpha)^3 + a$ will have only one linear factor for all $a = 0 \in \mathbb{F}_p$. ■

2.3.2 General Case

In this section, we will count the number of solution of (2.2). In order to use Theorem 2.2.2, we first need to homogenize our polynomials. We define $S = \bar{\mathbb{F}}_p[y_0, y_1, \ldots, y_n]$, $f_i = e_i - c_i y_0^i$ for $i = 1, \ldots, n-1$ and $I = (f_1, \ldots, f_{n-1})$ an ideal of S. Then $X = V(I) = \{P \in \text{Proj } S | I \subseteq P\}$ is a closed subscheme of $\mathbb{P}^n$.

As we mentioned in section 2.2., we will check the following list.

(a) X is irreducible, or I is prime.

(b) X is non-singular.

(c) dim $X = 1$.

First, we review some basic definitions.

Definition 2.3.5 *[12]*

- *Let R be a commutative ring and $\mathfrak{p}$ a prime ideal of R. Then the height of $\mathfrak{p}$ is the supremum of all integers n such that there exists a chain $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$ of distinct prime ideals. The height of $\mathfrak{p}$ is denoted by $\mathrm{h}(\mathfrak{p})$.*
- *The (Krull) dimension of R is the supremum of the heights of all prime ideals.*
- *Let I be an ideal of R. We define*
  - dim $I :=$ dim R/I
  - codim $I := \begin{cases} \text{dim } R_{\mathfrak{p}} & \text{if } I = \mathfrak{p} \text{ prime} \\ \inf_{I \subset \mathfrak{p}} \text{codim } \mathfrak{p} & \text{otherwise} \end{cases}$

Now we will show that $f_1, \ldots, f_{n-1}$ is a regular sequence.

Definition 2.3.6 *[12, p 419] Let R be a ring and let M be an R-module. A sequence of elements $x_1, \ldots, x_n \in R$ is called a regular sequence on M if*

1. $(x_1, \ldots, x_n)M = M$, *and*

2. For $i = 1, \ldots, n, x_i$ is a nonzerodivisor on $M/(x_1, \ldots, x_{i-1})M$.

We define depth (I, M) as the length of a (indeed any) maximal regular sequence on M in I. When $M = R$, we shall simply speak of the depth of I.

Proposition 2.3.7 *[12, p 448] We have* depth $(I, R) \leq$ codim I.

We also know that codim $I \leq$ number of generators of I by the principal ideal theorem.

In our case, $M = R = \bar{\mathbb{F}}_p[y_0, y_1, \ldots, y_n] =: S$. Consider the sequence $f_0, f_1, \ldots, f_n$, where $f_0 := y_0$, $f_n := e_n$. First, $(f_0, \ldots, f_n) = S$ because they are all homogeneous polynomials. Second, $S/(f_0, \ldots, f_i) \cong \frac{S}{(f_0)}/(\bar{f}_1, \ldots, \bar{f}_i)$, where $\frac{S}{(f_0)} = \bar{\mathbb{F}}_p[y_1, \ldots, y_n]$ and $\bar{f}_i = e_i$ for $i = 1, \ldots, n$. Here, we already know that the elementary symmetric polynomials form a regular sequence [30, p 142]. Therefore, $f_0, f_1, \ldots, f_n$ form a regular sequence and any subsequence will be a regular sequence because they are all homogeneous.

Remark 2.3.8 *In general, a set of n homogeneous polynomials in n variables is a regular sequence if the associated polynomial system has only the obvious solution* $(0, 0, \ldots, 0)$.

Definition 2.3.9 *[16, p 188] A closed subscheme X of $\mathbb{P}^n_k$ is called a complete intersection if the homogeneous ideal I of X in $S = k[y_0, y_1, \ldots, y_n]$ can be generated by $r =$* codim $(X, \mathbb{P}^n)$ *elements.*

It is obvious that X is a complete intersection if a set of generators of the homogeneous ideal I of X form a regular sequence. In our case, codim $(X, \mathbb{P}^n) =$ codim $(I, S) = n - 1$. And, $\dim X = \dim \mathbb{P}^n -$ codim $(X, \mathbb{P}^n) = 1$. Moreover, by the following proposition, S/I will be Cohen-Macaulay which are rings R in which depth $(I, R) =$ codim I for every ideal I.

Proposition 2.3.10 *[12, p 455] Let R be a Cohen-Macaulay ring, If I is an ideal generated by n elements in R such that* codim $I = n$, *the largest possible value, then R/I is a Cohen-Macaulay ring.*

Finally, we are ready to apply the following theorem in order to prove that I is prime.

Theorem 2.3.11 *[12, p 457] Let $R = k[x_1, \ldots, x_r][U^{-1}]/I$ be a localization of an affine ring over a perfect field k. Suppose that $I = (f_1, \ldots, f_n)$ has codimension c. Let $J \subset R$ be the ideal generated by the $c \times c$ minors of the Jacobian matrix $\mathcal{J} = (\partial f_i/\partial x_j)$, taken modulo I. Suppose R is Cohen-Macaulay.*

a. R is reduced iff J has codimension ≥ 1 in R.

b. R is a direct product of domains iff condition a. holds and R_P is a domain for every prime P of codimension ≤ 1.

c. R is a direct product of normal domains iff J has codimension ≥ 2 in R.

In our case, we use trivial localization, which means $U = \{1\}$ (in which case $R = S/I$) and we will apply Statement c. Here, we will assume that (b) X is non-singular. In other words, we assume that the Jacobian matrix $\mathcal{J} = (\partial f_i/\partial y_j) \pmod I$, whose size is $(n-1) \times (n+1)$ has full rank $n-1$ except the origin. Let J' be the ideal in S generated by the $(n-1) \times (n-1)$ minors of $(\partial f_i/\partial y_j)$, then $J = (J' + I)/I$. Consider a prime ideal P in S containing $J' + I$. Let H_P be the ideal generated by all homogeneous polynomials in P, then H_P contains $J' + I$. Then it should be the maximal homogeneous ideal $\mathfrak{m} = (y_0, y_1, \ldots, y_n)$. Otherwise, it contradicts our assumption. So $H_P = \mathfrak{m}$, then P itself should be $\mathfrak{m}$.

Lemma 2.3.12 *Let J be defined as above. Then* codim $(J, R) \geq 2$.

Proof By definition, codim $(J, R) = \inf_{J \subset P \text{ prime}} \text{codim } (P, R) = \text{codim } (\mathfrak{m}/I, S/I)$. We already know that codim $I = n - 1$ and codim $\mathfrak{m} = n + 1$ in S. Now we will use the following equation when H is prime.

$$\dim S/H = \text{codim } (\mathfrak{m}/H, S/H) + \dim(\mathfrak{m}/H, S/H)$$

The fact codim $I = n - 1$ tells us there exists a prime ideal $Q \supset I$ such that codim $(Q, S) =$ codim $(H_Q, S) = n - 1$. Note that H_Q is also prime. On LHS,

$\dim S/H_Q = \dim(H_Q, S) = \dim S - \text{codim }(H_Q, S) = (n+1) - (n-1) = 2$. On RHS, $\dim(\mathfrak{m}/H_Q, S/H_Q) = \dim(S/H_Q/\mathfrak{m}/H_Q) = \dim(S/\mathfrak{m}) = \dim k = 0$. Therefore, $\text{codim }(\mathfrak{m}/I, S/I) \geq \text{codim }(\mathfrak{m}/H_Q, S/H_Q) = 2$. ■

So far, we have proved that S/I is a direct product of normal domains by applying Lemma 2.3.12 to Theorem 2.3.11. The following proposition tells us that S/I is actually just one normal domain, which means that I is prime.

Proposition 2.3.13 *[16, p 231] Let X be a closed subscheme of $\mathbb{P}^n_k$ with dimension ≥ 1, which is a complete intersection. Then X is connected.*

We summarize the result of this section in the following theorem, which we have just proved.

Theorem 2.3.14 *Let $S = k[y_0, y_1, \ldots, y_n]$, where $k = \bar{\mathbb{F}}_p$ and $f_i = e_i - c_i y_0^i$ for $i = 1, \ldots, n-1$, where e_i is the i-th elementary symmetric polynomial in $k[y_1, \ldots, y_n]$ and $I = (f_1, \ldots, f_{n-1})$ an ideal of S. Then $X = V(I)$ is a connected closed subscheme of $\mathbb{P}^n_k$ with dimension 1. Moreover, assuming X is non-singular makes X be a complete non-singular curve.*

2.3.3 Non-singular Condition

For convenience of computations, we use Newton's identities to replace (2.2) by the following equivalent system of equations.

$$\begin{aligned} y_1 + y_2 \cdots + y_n &= c_1 \\ y_1^2 + y_2^2 + \cdots + y_n^2 &= c_1^2 - 2c_2 \\ y_1^3 + y_2^3 + \cdots + y_n^3 &= c_1^3 - 3c_1c_2 + 3c_3 \\ \vdots & \quad \vdots \\ y_1^{n-1} + y_2^{n-1} + \cdots + y_n^{n-1} &= g(c_1, \ldots, c_{n-1}) \end{aligned} \tag{2.6}$$

for some $g \in \mathbb{F}_p[x_1, \ldots, x_n]$. We name the right-hand side constants $-k_i$. After that, we homogenize the polynomials by setting $h_i := \sum_{j=1}^{n} y_j^i + k_i y_0^i$. Then $X = V(I)$,

where $I = (h_i | i = 1, \ldots, n-1)$, an ideal of $\bar{\mathbb{F}}_p[y_0, y_1, \ldots, y_n]$. In this case, the corresponding Jacobian matrix is

$$\mathcal{J} = (n-1)! \begin{pmatrix} 1 & 1 & \ldots & 1 & k_1 \\ y_1 & y_2 & \ldots & y_n & k_2 y_0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ y_1^{n-2} & y_2^{n-2} & \ldots & y_n^{n-2} & k_{n-1} y_0^{n-2} \end{pmatrix}_{(n-1)\times(n+1)} \tag{2.7}$$

Because p is sufficiently large compared to $n!$, $(n-1)!$ does not affect the rank of $\mathcal{J}$. Now it is obvious that $\mathcal{J}$ has the full rank $n-1$ if there exist always at least $n-1$ distinct y_i's among $i = 1, \ldots, n$. In order to satisfy this condition, we need to avoid the following cases.

Let $f(x) = \prod_{i=1}^{n}(x - x_i)$, where $x_i \in \mathbb{F}_p$ are distinct. There exists $a \in \bar{\mathbb{F}}_p$ such that

Type 1. $f + a = \prod_{i=1}^{n}(x - y_i)$ has a triple root.

Type 2. $f + a = \prod_{i=1}^{n}(x - y_i)$ has two pairs of double roots.

We can easily avoid Type 1 by checking $\mathrm{GCD}(f', f'') = 1$. After checking Type 1, we can say that $f'(x) = n \prod_{i=1}^{n-1}(x - z_i)$ has distinct roots in $\bar{\mathbb{F}}_p$.

Now we propose an algorithm which enables us to avoid Type 2, in other words, to check whether there exists a match among $f(z_i)$'s for $1 \leq i \leq n-1$. It is easy to see that this statement is equivalent to Type 2, because we just need to set $-a = f(z_i) = f(z_j)$.

If there exists a match among $f(z_i)$'s, it will be one of the followings.

Case 1. z_i, z_j are roots of distinct irreducible factors with same degree.

Case 2. z_i, z_j are roots of distinct irreducible factors with distinct degrees.

Case 3. z_i, z_j are roots of same irreducible factor.

Here, we state the main procedure of our algorithm. Let s be the maximum degree of the irreducible factors of f'.

From $m = 1$ to s, compute all the irreducible factors of $\mathrm{GCD}(f^{p^m} - f, f') = g_1 g_2 \cdots g_r$, then execute the following Test 1 and 2 for each m.

Test 1. If the GCD has a irreducible factor of degree greater than m, then stop the loop because f has Case 3 match.

Test 2. If the GCD has several irreducible factors g_i with degree m, then compare the irreducible polynomials of $f(z_i)$'s where z_i is any root of g_i. If there exists a match, stop the loop because f has Case 1 match.

Finally, our conclusion is this:

If $f(x) = \prod_{i=1}^{n}(x - x_i)$ passes through Test 1 and 2, f has no Type 2 for any $a \in \bar{\mathbb{F}}_p$.

We explain why the algorithm works. The following propositions will show how Test 1 catches both Case 2 and Case 3 matches.

Proposition 2.3.15 *Let g_1, g_2 be irreducible polynomials over $\mathbb{F}_p$ with distinct degrees m, l, respectively, where $m < l$. Let z_1, z_2 be roots of g_1, g_2, respectively. If $f(z_1) = f(z_2)$, then $g_2 | f^{p^m} - f$.*

Proof We know that $z_1^{p^m} = z_1$. Thus,

$$f(z_2) = f(z_1) = f(z_1^{p^m}) = f(z_1)^{p^m} = f(z_2)^{p^m}$$

and z_2 is a root of $f^{p^m} - f$. Therefore, $g_2 | f^{p^m} - f$ ■

Proposition 2.3.16 *Let g be an irreducible polynomial over $\mathbb{F}_p$ with $\deg g = l$. If there exist z_1, z_2 such that $g(z_1) = g(z_2) = 0$ and $f(z_1) = f(z_2)$, then $g | f^{p^m} - f$ for some $m < l$.*

Proof Because z_1, z_2 are roots of g, there exists $m < l$ such that $z_1^{p^m} = z_2$. Then $f(z_1) = f(z_2) = f(z_1^{p^m}) = f(z_1)^{p^m}$, that is, z_1 is a root of $f^{p^m} - f$. Therefore, $g | f^{p^m} - f$. ■

In Case 2 and Case 3, there exist an irreducible factor g of f' over $\mathbb{F}_p$ with degree l such that $g|f^{p^m} - f$ for some $m < l$, by Proposition 2.3.15 and 2.3.16, respectively. However, Proposition 2.3.17 tells us that the inverse is true also.

Proposition 2.3.17 *Let* $\mathrm{GCD}((f^{p^m} - f, f') = g_1 \cdots g_r$ *where* $\deg g_i \leq \deg g_j$ *for* $i < j$. *If* $\deg g_r > m \geq 1$, f *has a Case 3 match.*

Proof Let $\deg g_r = l$. There exists $z_1 \in \mathbb{F}_{p^l}$ such that $g_r(z_1) = 0$, so $f(z_1)^{p^m} = f(z_1)$. Let $z_2 = z_1^{p^{l-m}} = z_1$. Then z_2 satisfies $g_r(z_2) = 0$, so $f(z_2)^{p^m} = f(z_2)$, also. Because f is a polynomial over $\mathbb{F}_p$, $f(z_2) = f(z_1^{p^{l-m}}) = f(z_1)^{p^{l-m}}$. Then $f(z_2)^{p^m} = f(z_1)^{p^l} = f(z_1)$. Therefore, $f(z_2) = f(z_1)$. ■

Therefore, Test 1 will be able to catch a Case 2 and a Case 3 match exactly.

Remark 2.3.18

1. *If f has a Case 2 match, then f has a Case 3 match at the same time.*
2. *If an irreducible polynomial g over $\mathbb{F}_p$ with degree l satisfies $g|f^{p^m} - f$ for some $m < l$, then $m|l$.*

Assume that f has a Case 1 match, that is, there exist roots z_i and z_j of f' in $\bar{\mathbb{F}}_p$ that have distinct irreducible polynomials over $\mathbb{F}_p$ with same degree, but $f(z_i) = f(z_j)$. Because f is a polynomial over $\mathbb{F}_p$, $f(z_i)$ has the same irreducible polynomial over $\mathbb{F}_p$ with $f(z)$ for any root z of the irreducible polynomial of z_i over $\mathbb{F}_p$. Therefore, Test 2 will be able to catch a Case 1 match.

The inverse is also true. Suppose that there are two irreducible factors g_i, g_j with degree m of $\mathrm{GCD}(f^{p^m} - f, f')$ such that z_i, z_j are roots of g_i, g_j, respectively, and $f(z_i), f(z_j)$ have the same irreducible polynomial. Then $f(z_j) = f(z_i)^{p^n} = f(z_i^{p^n})$ for some $n < m$ and $z_i^{p^n}$ is a root of g_i.

2.4 Conclusion

The number of monic polynomials with degree n over $\mathbb{F}_p$ is p^n, and The number of splitting monic polynomials with degree n over $\mathbb{F}_p$ is

$$\begin{pmatrix} n+p-1 \\ p-1 \end{pmatrix} = \begin{pmatrix} n+p-1 \\ n \end{pmatrix} = \frac{(p+n-1)\cdots(p+1)p}{n!}.$$

Therefore, the probability that a random monic polynomial splits over $\mathbb{F}_p$ approaches $1/n!$ as the prime p increases. This statement gives us a rough guess that $\Pr(a \in \mathbb{F}_p | \quad \prod_{i=1}^{n}(x-x_i)+a$ splits over $\mathbb{F}_p)$ also approaches $1/n!$ as the prime p grows. Now we will support this guess with what we have done so far.

In Section 2.3.3., we have presented an algorithm which enables us to avoid singularity. Under some conjectures and assumptions, we would like to claim that our algebraic set X is non-singular with at least 98%.

The number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ is given by

$$N(q,n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}},$$

where μ is the Möbius function [17].

Proposition 2.4.1 *The probability that a randomly chosen monic polynomial f over $\mathbb{F}_p$ makes* $\mathrm{GCD}(f, f') = 1$ *is close to* 1 *as p approaches infinity.*

Proof Consider the factorization of $f = \prod g_i$ over $\mathbb{F}_p$. Let $\deg g_i = m_i'$ and $m_i' \geq m_j'$ when $i < j$. Then $n = \sum m_i'$. Rewrite it as a partition of n like $n = \sum a_i m_i$, where $m_i > m_j$ when $i < j$.

Now for a given partition of n, count the number of monic polynomials the factorization of which has the same partition of n. We are counting a number of combinations with repetition. Then the total number of monic polynomials over $\mathbb{F}_p$ of degree n is

$$p^n = \sum_{n=\sum a_i m_i} \prod_i \begin{pmatrix} N_{m_i} + a_i - 1 \\ a_i \end{pmatrix},$$

where $N_{m_i} = N(p, m_i)$. The number of monic polynomials over $\mathbb{F}_p$ of degree n with distinct roots only is

$$\sum_{n=\ a_i m_i} \prod_i \binom{N_{m_i}}{a_i}.$$

Therefore, the number of monic polynomials over $\mathbb{F}_p$ of degree n with multiple roots is

$$\sum_{n=\ a_i m_i} \left(\prod_i \binom{N_{m_i} + a_i - 1}{a_i} - \prod_i \binom{N_{m_i}}{a_i} \right) = o(p^n).$$

Consider both $\prod_i \binom{N_{m_i}+a_i-1}{a_i}$ and $\prod_i \binom{N_{m_i}}{a_i}$ as polynomials of N_{m_i}'s. Then the term with the largest degree is $\frac{1}{a_i!} \prod_i (N_{m_i})^{a_i}$, and it will be cancelled out. However, this is the only term containing p^n. ■

Corollary 2.4.2 *For randomly chosen ordered n-tuples $(x_1 < x_2 < \cdots < x_n)$ where $x_i \in \mathbb{F}_p$, the probability that $\mathrm{GCD}(f', f'') = 1$, where $f = \prod_{i=1}^{n}(x - x_i)$, is more than 99% when p is sufficiently large compared to $n!$.*

Conjecture 2.4.3

$$\sum_{n=\ a_i m_i} \left(\prod_i \binom{N_{m_i} + a_i - 1}{a_i} - \prod_i \binom{N_{m_i}}{a_i} \right) = 1 \cdot p^{n-1} + o(p^{n-1}).$$

In general, the probability that two randomly chosen positive degree polynomials over $\mathbb{F}_q$ are relatively prime is $1 - 1/q$ [6]. Conjecture 2.4.3 claims that the formal derivative behaves almost randomly when we consider relative primality. It can be proved for small integers $n = 4, 5, 6$ and is also supported by the data in Table 2.2, which were computed by MAGMA.

Conjecture 2.4.4 *For randomly chosen ordered n-tuples $(x_1 < x_2 < \cdots < x_n)$, where $x_i \in \mathbb{F}_p$, the probability that $f(x) = \prod_{i=1}^{n}(x - x_i)$ will pass through Test 1 in Section 2.3.3 is more than 98% when p is sufficiently large compared to $n!$.*

We support Conjecture 2.4.4 by the data in Table 2.3 which were computed by MAGMA.

Table 2.2
Probability of GCD$(f', f'') = 1$

p	$n = 4$	$n = 5$
101	.9894867038	.9906024265
103	.9904950495	.9908790879
107	.9912087912	.9911447776
109	.9910068771	.9910824496
113	.9916461916	.9916146338
127	.9922580645	.9925098348
131	.9927325581	.9926066654
137	.9930348259	.9930173693
139	.9935594676	.9929869758

Assumption 2.4.5 *Let* $f(x) = \prod_{i=1}^{n}(x-x_i)$, *where* $x_i \in \mathbb{F}_p$ *and* $f'(x) = n\prod_{i=1}^{n-1}(x-z_i)$, *where* $z_i \in \bar{\mathbb{F}}_p$. *For given* m, *we consider* $z_1, z_2, \cdots \in \mathbb{F}_{p^m}$ *to be random if they have distinct irreducible polynomials with degree* m *over* $\mathbb{F}_p$. *Also, we consider* $f(z_i)$*'s to be random if they have distinct irreducible polynomials with degree* m *over* $\mathbb{F}_p$.

Actually, we are not concerned with the case that $f(z_i)$ has an irreducible polynomial with degree $n < m$ over $\mathbb{F}_p$ because it will be caught in Test 1 when the loop index becomes $n < m$.

Under Assumption 2.4.5, the probability that f will pass through Test 2 in Section 2.3.3 is at least

$$\prod_{m=1}^{s} \frac{{}_N P_{n(m)}}{N^{n(m)}},$$

where ${}_N P_k = N!/(N-k)!$ is the number of permutations of N different things taken k at a time, $N = N(p, m)$ and $n(m)$ is the number of degree m factors of f'. We claim that the probability is really close to 1 because p is sufficiently large compared to $n!$ which is much larger than $n(m)$.

Table 2.3
Probability that GCD$(f^p - f, f') = 1$ or has distinct linear factors only

p	$n = 4$
149	.9829466033
151	.9831307818
157	.9841642229
163	.9850931677
167	.9844789357
173	.9853457172
179	.9861325116
181	.9862532170
191	.9864910503
193	.9872692202
197	.9871530531
199	.9872578473

So far, we have supported conjectures and assumptions which lead us to say that our algebraic set X corresponding to (2.2) is non-singular by 98%.

Now by Theorem 2.3.14, X will be a complete non-singular curve. As we can see in Theorem 2.2.3, the arithmetic genus totally depends on n. If we fix n and a large number l, then for all $p > (2lg)^2$, we have

$$\left|N(X) - (p+1)\right| \leq 2g\sqrt{p} \leq \frac{1}{l}\ p \tag{2.8}$$

$$1 - \frac{1}{l} \quad p + 1 < N(X) < \quad 1 + \frac{1}{l} \quad p + 1 \tag{2.9}$$

Because the system of equations (2.2) consists of elementary symmetric polynomials, we can get an approximation of the number of a's in $\mathbb{F}_p$ which makes $\prod_{i=1}^{n}(x - x_i) + a$ factored linearly in $\mathbb{F}_p[x]$ by dividing both sides by $n!$. We have

$$\frac{1}{n!} \quad 1 - \frac{1}{l} \quad p + 1 \quad < \text{the number of } a < \frac{1}{n!} \quad 1 + \frac{1}{l} \quad p + 1 \tag{2.10}$$

Therefore, $\Pr(a \in \mathbb{F}_p | \quad \prod_{i=1}^{n}(x - x_i) + a$ splits over $\mathbb{F}_p) = (1/p) \cdot$ (the number of a) is $1/n!$ with error $1/(l \cdot n!)$. Notice that we have ignored two things so far, but both of them have negligible probability.

First, the actual number of a might be $(n-1)/2$ less than we thought because we allow up to one double root. However, considering the size of p, this is negligible.

Second, the number of rational points at infinity is $(n-1)!$ if $n|p-1$. Otherwise, it is 0. However,

$$\frac{1}{n!}N(X) - 1 < \frac{1}{n!}\left(N(X) - (n-1)!\right) < \frac{1}{n!}N(X) \tag{2.11}$$

So it affects the number of a by at most 1, which is negligible, too.

Now we wrap up this chapter by showing an example for a singular case.

Example 2.4.6 *Let $p = 199$ and $f(x) = x(x+1)(x-1)(x-2) \in \mathbb{F}_p[x]$. According to the computation by MAGMA, there are 26 a's in $\mathbb{F}_p$ which make $f+a$ factor into linear terms. Two of them make $f + a$ have repeated roots. One of those two makes $f + a$ have one repeated root, and the other makes $f + a$ have two repeated roots which make singular points. Except for the singular points, there are $24 \cdot 4! + 4!/2 = 576 + 12 = 588$ points on the algebraic set X. Also, there are $\frac{4!}{2!2!} = 6$ singular points. Therefore, X will be expected to have at least 2, maybe 3 irreducible factors, because $594 \approx 3 \cdot 200$ (where, $2g\sqrt{p} \approx 2 \cdot 4 \cdot 14 = 112$)*

In fact, there are 3 irreducible factors. Therefore, the corresponding irreducible component has intersections at 2 points with other components respectively. So each component has $588/3 = 196$ non-singular points and $2 + 2 = 4$ singular points from intersections. By the following example, we know that there is no rational point at infinity. So total number of rational points in each component is 200, which is exactly same with $p + 1$.

The following example explains why our algebraic set X has no rational point at infinity when $n = 4$ and $p \equiv 3 \pmod 4$.

Example 2.4.7 *Suppose that $x^4 + a$ splits over $\mathbb{F}_p$ Then for some $b \in \mathbb{F}_p$, $b^4 = -a$ and $x^4 - b^4 = (x-b)(x+b)(x^2+b^2)$. So $\frac{-1}{p} = (-1)^{\frac{p-1}{2}} = 1$. However, it is true*

only when $p \equiv 1 \pmod 4$*. In other words,* $x^4 + a$ *never splits over* $\mathbb{F}_p$ *for non-zero* a *when* $p \equiv 3 \pmod 4$*.*

3. PROBABILITY DISTRIBUTIONS IN THE SQUFOF ALGORITHM

3.1 Introduction

This chapter answers a question left in the "future work" section of the Ph.D. thesis of Jason Gower [13].

3.1.1 The SQUFOF Algorithm

SQUFOF, which stands for SQUare FOrm Factorization, is an integer factoring algorithm invented by Daniel Shanks. For each size of integer, there is a fastest general purpose algorithm among known methods to factor a number of that size. For example, the number field sieve (NFS) is best for integers greater than 10^{120},and the quadratic sieve (QS) is best for numbers between 10^{50} and 10^{120}. With 32-bit computer architecture, SQUFOF is clearly the best factoring algorithm for numbers between 10^{10} and 10^{18}, and will likely remain so. SQUFOF is extraordinarily simple and efficient, so it is used in most implementations of NFS and QS to factor small auxiliary numbers arising in factoring large N.

3.1.2 Contribution of This Chapter

In Gower's thesis, he made conjectures about the probability distribution of the number of binary quadratic forms that SQUFOF must examine before finding a proper square form and the number of forms enqueued during the factorization of N. These two numbers represent the time and space complexity of SQUFOF, respectively, so they are the main measures of the efficiency of the algorithm. We propose a different

probability distribution (geometric rather than exponential) than did Gower, and we use Gower's data to support our conclusions.

3.1.3 Outline of This Chapter

In Section 3.2, we explain what a proper square form is and why we need to find one to factor a given integer N. We also explain why some forms need to be enqueued. In Section 3.3 and 3.4, we present our main results about probability distribution of the number of forms that SQUFOF must examine before finding a proper square form and the number of forms enqueued during factorization of N without/with multipliers respectively. In Section 3.5, we verify our results with the experimental data Gower presented.

3.2 Background

Here, we try to explain the notion of proper square form as briefly as possible. For more detail, you can see [13] for a short version, or [9] for a long version.

3.2.1 Binary Quadratic Forms

Elementary Concepts

A *binary quadratic form* is a polynomial over $\mathbb{Z}$ in two variables x, y in the form $f(x, y) = ax^2 + bxy + cy^2$. We denote it simply by (a, b, c) and its discriminant by $\Delta = b^2 - 4ac$. One of classic topics in binary quadratic forms is the question of what forms can represent a given integer. If a form (a, b, c) can represent an integer m, then $m = ax^2 + bxy + cy^2$ for some x and y, so we have the equation $4am = (2ax+by)^2-\Delta y^2$. For positive values of Δ, one representation might imply an infinite number of representations. So it would be better if we can say a "Fundamental"

representation. First, we define the group action of $\mathrm{SL}_2(\mathbb{Z})$ on the set of binary quadratic forms by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot f(x,y) = f(\alpha x + \beta y, \gamma x + \delta y).$$

Then define $f_1 \sim f_2$ when f_1 and f_2 are equivalent modulo the action of $\mathrm{SL}_2(\mathbb{Z})$. Note that this equivalence relation preserves the discriminant. We make two special notes about this equivalence:

1. $(a, b+2na, a+nb+c) \sim (a,b,c)$ for any $n \in \mathbb{Z}$, using the matrix $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

2. We say f_1 and f_2 are improperly equivalent if $\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = -1$.

Indefinite Forms

The binary quadratic forms with positive discriminant Δ are called *indefinite* forms. Each equivalence class of indefinite forms of Δ contains a set of canonical representatives, called *reduced* forms. The form $f = (a,b,c)$ is called *reduced* if $\left|\sqrt{\Delta} - 2|a|\right| < b < \sqrt{\Delta}$. For any indefinite form $f = (a,b,c)$, with $ac = 0$, we define the *standard reduction operator* by

$$\rho(a,b,c) = \quad c, r(-b,c), \frac{r(-b,c)^2 - \Delta}{4c} \quad ,$$

where $r(-b,c)$ is defined to be the unique integer r such that $r + b \equiv 0 \bmod 2c$ and

$$-|c| < r \leq |c| \quad \text{if} \quad \sqrt{\Delta} < |c| \,,$$
$$\sqrt{\Delta} - 2|c| < r < \sqrt{\Delta} \quad \text{if} \quad |c| < \sqrt{\Delta} \,.$$

$\rho(f)$ is called the *reduction* of f and the result of n applications of ρ is written $\rho^n(f)$. We also define the *inverse reduction operator* by

$$\rho^{-1}(a,b,c) = \quad \frac{r(-b,a)^2 - \Delta}{4a}, r(-b,a), a \quad ,$$

where $r(-b, a)$ is defined as in the definition of ρ.

If f is reduced, then both $\rho(f)$ and $\rho^{-1}(f)$ are reduced. If f is not reduced, then $\rho^n(f)$ is reduced for some finite n. Similarly f can be reduced after a finite number of applications of ρ^{-1}. The identities $\rho(\rho^{-1}(f)) = \rho^{-1}(\rho(f)) = f$ hold only when f is reduced. The unique reduced form $(1, b, c)$ is called the *principal* form.

We say that (a, b, c) and (c, b', c') are *adjacent* if $b + b' \equiv 0 \mod 2c$. More specifically, we say that (a, b, c) is adjacent to the left of (c, b', c') and (c, b', c') is adjacent to the right of (a, b, c). It is easy to see that there is a unique reduced form adjacent to the right and to the left of any given reduced form, these forms being $\rho(a, b, c)$ and $\rho^{-1}(a, b, c)$, respectively. We now see that within each equivalence class of forms with $\Delta > 0$ there are *cycles* of reduced forms. The cycle that contains the principal form is called the *principal cycle*. The number of reduced forms in any cycle is always even.

The two forms (a, b, c) and (c, b, a) are said to be *associated*. If the form f_1 and its associate f_2 are in different cycles, then this will be the case for all forms in either cycle, and in this case the two cycles are said to be *associated cycles*.

The form $(a, -b, c)$ is the *opposite* of the form (a, b, c). A form (a, b, c) is improperly equivalent to both its associate and its opposite. Hence, (a, b, c) is equivalent to the associate of its opposite: $(a, b, c) \sim (c, -b, a)$.

Any form (k, kn, c) is called *ambiguous*. Any cycle which contains an ambiguous form (called an *ambiguous cycle*) contains exactly two ambiguous forms and is its own associate. Conversely, a cycle which is its own associate contains exactly two ambiguous forms. The principal cycle is ambiguous since it contains the principal form $(1, b, c)$. Because there exists an ambiguous form (k, kn, c) of discriminant Δ for each divisor k of Δ, finding a nontrivial factor of N is equal to finding an ambiguous form which has a nontrivial $k = 1, 2$.

From the facts listed above, we can see the following easily: Assume that (a, b, c) is reduced. Then (a, b, c) is ambiguous if and only if (c, b, a) is adjacent to the left of (a, b, c).

Composition of Forms

We now define *composition* of forms. Let $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ be two forms with the same discriminant. Let $\beta = (b_1 + b_2)/2$, $m = \gcd(a_1, \beta)$, and $n = \gcd(m, a_2)$. Solve $a_1 x + \beta y = m$ for x and y and

$$mz/n \equiv x \quad \frac{b_2 - b_1}{2} \quad - c_1 y \bmod a_2/n \quad \text{for } z\ .$$

Then the composition of f_1 and f_2, written $f_1 \circ f_2$ is

$$a_1 a_2/n^2, b_1 + 2a_1 z/n, * \quad ,$$

where the third coefficient may be determined by the discriminant formula. Composition is easily seen to be commutative and associative. Further, for any forms $(1, b', c')$ and (a, b, c), we have

$$(1, b', c') \circ (a, b, c) \sim (a, b, c)$$

$$(a, b, c) \circ (a, -b, c) \sim (a, b, c) \circ (c, b, a) \sim (ac, b, 1)$$

In other words, the principal form is the identity and the associate is the inverse up to the equivalence. Thus the set of equivalence classes of forms of a given discriminant is an abelian group under composition. We note that even if f_1 and f_2 are reduced, their composition need not be reduced.

As a special case, we present the formula for $f^2 = f \circ f$ as follows. Suppose $f = (a, b, c)$, $n = \gcd(a, b)$, and y is a solution for $by/n \equiv 1 \bmod a/n$. Then f^2 is equivalent to

$$a^2/n^2, b - 2acy/n, * \quad .$$

Note that if $\gcd(a, b) = 1$, then

$$(a, b, -ac)^2 \sim \quad a^2, b, -c \quad .$$

Moreover, g is equivalent to an ambiguous form if and only if $g \circ g$ is equivalent to the principal form. This implies that the square of $g \circ (a, b, -ac)$ is equivalent to $(a^2, b, -c)$.

3.2.2 Periodic Continued Fractions

Let $N > 0$ be a real quadratic irrational number. The *simple continued fraction expansion* of $\sqrt{N}$ is given by

$$\sqrt{N} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots}} \, .$$

We will always abbreviate the expansion as $[q_0, q_1, \dots]$, where q_i's are called the *partial quotients* of the continued fraction. The expansion is ultimately periodic, meaning that for some $\pi > 0$ we will have $q_i = q_{i+\pi}$ for all $i > 0$, where π is the period of the continued fraction. In this case, we will write $\sqrt{N} = [q_0, \overline{q_1, \dots, q_\pi}]$.

We define the n^{th} *complete quotient* by

$$x_n = \begin{cases} \sqrt{N} & \text{if } n = 0 \, , \\ 1/\left(x_{n-1} - q_{n-1}\right) & \text{if } n \geq 1 \, . \end{cases}$$

It can be shown that $x_n = (P_n + \sqrt{N})/Q_n$ for $n \geq 0$, where

$$P_n = \begin{cases} 0 & \text{if } n = 0 \, , \\ q_0 & \text{if } n = 1 \, , \\ q_{n-1}Q_{n-1} - P_{n-1} & \text{if } n \geq 2 \, , \end{cases} \tag{3.1}$$

and

$$Q_n = \begin{cases} 1 & \text{if } n = 0 \, , \\ N - q_0^2 & \text{if } n = 1 \, , \\ Q_{n-2} + (P_{n-1} - P_n)q_{n-1} & \text{if } n \geq 1 \, . \end{cases} \tag{3.2}$$

If we do not have the q_n, they can be computed using

$$q_n = \begin{cases} \left\lfloor \sqrt{N} \right\rfloor & \text{if } n = 0 \, , \\ \\ \left\lfloor \dfrac{q_0 + P_n}{Q_n} \right\rfloor & \text{if } n > 0 \, . \end{cases}$$

We can see easily that x_n is periodic with period π for $n > 0$. Therefore, P_n, Q_n are also periodic with period π for $n > 0$.

Some important facts that we shall need are as follows.

$$N = P_n^2 + Q_n Q_{n-1}, \quad 0 \leq P_n,\, Q_n < 2\sqrt{N}, \quad \forall n > 0. \tag{3.3}$$

See [26] for a proof of these facts.

3.2.3 Continued Fractions Description of SQUFOF

Let $N = 1$ be a square-free integer, and define

$$\Delta = \Delta(N) = \begin{cases} 4N & \text{if } N \equiv 2, 3 \bmod 4\ , \\ N & \text{if } N \equiv 1 \bmod 4\ . \end{cases}$$

For the convenience of explanation, we assume $\Delta = 4N$. There is a correspondence between binary quadratic forms and continued fractions. By (3.3), the binary quadratic form

$$F_n = \ (-1)^{n-1} Q_{n-1}, 2P_n, (-1)^n Q_n \ = \rho^{n-1}(F_1)$$

has discriminant $4N$, where $F_1 = (1, 2q_0, q_0^2 - N)$ is the principal form. It means that the sequence of forms $F_1, F_2, \ldots, F_\pi = (q_0^2 - N, 2q_0, 1)$ constitutes the principal cycle of forms of discriminant $4N$. Sometimes, we rename F_π by F_0 because it is adjacent to the left of F_1.

We seek a *square* form $(*, *, c^2)$, which can only occur when n is even. Suppose we have found a square form $F_n = (-Q, 2P, S^2)$, where $Q > 0$. Define $F^{-1/2} = (-S, 2P, SQ)$, an inverse square root of F_n under composition of forms. $(F^{-1/2})^2$ is equivalent to the associate of F_n, so $F^{-1/2}$ is equivalent to an ambiguous form. This form may not be reduced so let $G_0 = (-S_{-1}, 2R_0, S_0)$ be its reduction, where

$$R_0 = P + S \ \frac{q_0 - P}{S} \ , \quad S_{-1} = S, \quad S_0 = \frac{N - R_0^2}{S}$$

Using $R_m = t_{m-1}S_{m-1} - R_{m-1}, S_m = S_{m-2} + t_{m-1}(R_{m-1} - R_m)$, and $t_m = \lfloor \frac{q_0 + R_m}{S_m} \rfloor$ for $m \geq 1$, which are completely analogous to formulas for P_n, Q_n, q_n in Section 3.2.2, we generate a new sequence of forms

$$G_m = ((-1)^{m-1}S_{m-1}, 2R_m, (-1)^m S_m)$$

Now we try to find m such that $R_m = R_{m+1}$ because for such an m, $S_{m+1} = S_{m-1}$. Therefore, G_m and G_{m+1} are symmetric and adjacent, which means G_{m+1} is ambiguous. We expect this to happen at approximately $m \approx n/2$. For reasons, see Infrastructure of the Class Group in [13]. At this m, we will have $R_m = t_m S_m/2$ and $N = R_m^2 + S_{m-1}S_m$, which gives

$$N = S_m \quad S_{m-1} + S_m \frac{t_m^2}{4}$$

a possible factorization of N. We call the square form F_n *improper* if this factorization is trivial. If a non-trivial factor of N is found, then F_n is a *proper* square form.

3.2.4 Identifying Proper Square Forms

Now our concern is the possibility of ending with the trivial factorization. We could save and return to the last square form F_n, but this is time consuming. Instead, we will keep track of certain forms and use them in a test for proper square forms. We begin with a few propositions about square roots of square forms.

Proposition 3.2.1 *[13, p. 21] Suppose that a is a positive odd integer, b is a positive integer, $\gcd(a, b) = 1$, and that $(-c, 2b, a^2)$ is a square form on the principal cycle of discriminant $4N$ with $c > 0$. Then $(-a, 2b, ac)^{-2} \sim (-c, 2b, a^2)$.*

Let $b = \sqrt{N}$ and $\mathbf{1} = (1, 2b, c)$ denote the principal form. Let $b' = \sqrt{N}$ or $\sqrt{N} - 1$, whichever is odd, and let $\mathbf{2}$ denote the reduced ambiguous form $(2, 2b', c')$. By $-\mathbf{1}$, $-\mathbf{2}$ we mean the forms $(-1, 2b, -c)$, $(-2, 2b', -c')$, respectively. It is easy to see that $\pm\mathbf{1} \circ (\alpha, 2\beta, \gamma) \sim (\pm\alpha, 2\beta, \pm\gamma)$ and that $\pm\mathbf{2} \circ (\alpha, 2\beta, *) \sim (\pm 2\alpha, 2\beta, *)$, when α is odd and $\pm\mathbf{2} \circ (\alpha, 2\beta, *) \sim (\pm\alpha/2, 2\beta, *)$, when α is even.

Proposition 3.2.2 *[14, Prop. 3.2] Suppose that a is a positive odd integer, b is a positive integer,* $\gcd(a,b) = 1$*, and that $F_n = (-c, 2b, a^2)$ is a square form on the principal cycle of discriminant $4N$, with $c > 0$. Some form $(*, 2\beta, \alpha)$ appears on the principal cycle at position $m < n$ with $\alpha \in \{\pm a, \pm 2a\}$ and $\beta \equiv b \bmod a$ if and only if $(-a, 2b, ac)$ is equivalent to one of the ambiguous forms $\pm\mathbf{1}$, $\pm\mathbf{2}$.*

We now describe Shanks' method for determining when a square form is proper. For each form F_m that is examined, we perform the following test. Define $L = 2\sqrt{2\sqrt{N}}$. If Q_m is even and less than L, then put the pair $Q_m/2$, $\overline{P_m}$ into a queue, where $\overline{P_m}$ is the least positive residue of P_m modulo $Q_m/2$. If Q_m is odd and less than $L/2$, then put the pair Q_m, $\overline{P_m}$ into the queue, where $\overline{P_m}$ is the least positive residue of P_m modulo Q_m. If we come to the square form $F_n = (-c, 2b, a^2) \sim (a^2, 2b, -c)^{-1} \sim (-a, 2b, ac)^{-2}$, then we search the queue in the order that items are put into the queue for the pair $(a, b \bmod a)$, taking $a > 0$. Proposition 3.2.2 says that if this pair is in the queue, then the form $(-a, 2b, ac)$ is equivalent to one of the forms $\pm\mathbf{1}, \pm\mathbf{2}$, hence the square form is improper. If on the other hand the pair $(a, b \bmod a)$ is not in the queue, then Proposition 3.2.2 says that $(-a, 2b, ac)$ is not equivalent to one of the forms $\pm\mathbf{1}, \pm\mathbf{2}$, hence the square form is proper.

3.3 Probability Distribution

Let W be the number of forms that SQUFOF must examine before finding a proper square form during the factorization of N and Q be the number of forms enqueued during the factorization of N. Here, we will explain explicitly the probability distribution of W and Q under Gower's assumption in his thesis. We always assume that there is at least one proper square form on the principal cycle, so that W and Q are defined.

3.3.1 Probability Distribution of W

Assume that N is a product of k distinct odd primes. Let X be the total number of reduced forms with discriminant Δ on the principal cycle and X_{sq} be the number of reduced square forms on the principal cycle. In order to make understanding easy, we present some assumptions Gower made. If you want to check all the assumptions he made, see [14] or [13].

Assumption 3.3.1 *[14]*

1. *Let $D = X/X_{sq}$ be the average number of reduced forms between successive square forms in the principal cycle. Then as Δ approaches ∞, we have $E[D] \sim E[X]/E[X_{sq}]$*

2. *Let f be one of the 2^k reduced ambiguous forms of discriminant Δ. If one begins with a square form $(*, *, c^2)$ on the principal cycle of reduced forms of discriminant Δ, computes its inverse square root as SQUFOF does, and follows its cycle to the first ambiguous form, then there is one chance in 2^k that this ambiguous form will be f.*

Under Assumption 3.3.1, Gower claimed that the probability that a given form on the principal cycle is a square form is taken to be $E[X_{sq}]/E[X]$. Then he computed the probability that a given square form is proper is $\frac{2^k-2}{2^k}$.

Here, we suggest one more assumption which Gower actually used, but did not declare.

Assumption 3.3.2 *We consider each step as a Bernoulli trial for finding a proper square form.*

By Assumption 3.3.2, W will follow a geometric distribution with probability $p = \frac{2^k-2}{2^k} \cdot E[X_{sq}]/E[X]$ for a given N. Actually, this is the way Gower computed $E[W]$ for a given N in his thesis. A new symbol will be introduced to present his result here.

Proposition 3.3.3 *[13, p. 44] Let W be the number of forms that SQUFOF must examine before finding a proper square form during the factorization of N. Then*

$$\mu := \frac{E[W|N]}{\sqrt[4]{N}} = \frac{1}{p\sqrt[4]{N}} \sim \begin{cases} \frac{2(\sqrt{2}+1)\log 2}{2^k-2} & \text{if } \Delta(N) \equiv 1 \bmod 4 \\ \frac{3(\sqrt{2}+2)\log 2}{2(2^k-2)} & \text{if } \Delta(N) \equiv 0 \bmod 4 \end{cases}$$

Note that μ is constant with respect to N when k is fixed.

Next we consider N as a random variable which follows a uniform distribution with the following conditions;

1. k is fixed.

2. N is odd with k distinct prime factors and larger than 10^{10}.

3. The congruence class of $\Delta(N)$ is fixed (either 0 or 1 mod 4).

The range of N for which SQUFOF is the fastest algorithm is $10^{10} < N < 10^{18}$. All of our numerical experiments lie in this range.

Proposition 3.3.4 *Assume Assumption 3.3.2. Let $Y = W/\sqrt[4]{N}$, where N and W are defined as above. Then $E[Y] = \mu$ and $Var[Y] \approx \mu^2$.*

Proof We have

$$\begin{aligned} E[Y] &= E\left[\frac{W}{\sqrt[4]{N}}\right] = E\left[E\left[\frac{W}{\sqrt[4]{N}}|N\right]\right] \\ &= E\left[\frac{1}{\sqrt[4]{N}}E\left[W|N\right]\right] = E\left[\frac{1}{\sqrt[4]{N}}\mu\sqrt[4]{N}\right] = E[\mu] = \mu \\ Var[Y] &= E[Y^2] - (E[Y])^2 = E[Y^2] - \mu^2 \end{aligned}$$

$$
\begin{aligned}
E[Y^2|N] &= E\left[\frac{W^2}{\sqrt{N}}|N\right] = \frac{1}{\sqrt{N}}E[W^2|N] \\
&= \frac{1}{\sqrt{N}}(Var[W|N] + E[W|N]^2) \\
&= \frac{1}{\sqrt{N}}\left[\frac{1}{p^2} - \frac{1}{p} + \left(\frac{1}{p}\right)^2\right] = \frac{1}{\sqrt{N}}\left[\frac{2}{p^2} - \frac{1}{p}\right] \\
&= \frac{1}{\sqrt{N}}(2\mu^2\sqrt{N} - \mu\sqrt[4]{N}) = 2\mu^2 - \frac{\mu}{\sqrt[4]{N}} \\
E[Y^2] &= E[E[Y^2|N]] = E\left[2\mu^2 - \frac{\mu}{\sqrt[4]{N}}\right] = 2\mu^2 - \mu E\left[\frac{1}{\sqrt[4]{N}}\right] \\
Var[Y] &= \mu^2 - \mu E\left[\frac{1}{\sqrt[4]{N}}\right]
\end{aligned}
$$

Now μ has a value near 1 when k is a small integer and gets even smaller when k gets larger. Moreover, $E[1/\sqrt[4]{N}] < 1/10^4$. This is why we can claim that $Var[Y] \approx \mu^2$. ■

3.3.2 Probability Distribution of Q

Gower also made the following assumption in [14].

Assumption 3.3.5 *In each step of factorization of N, the form has the chance to be enqueued with the probability* $\hat{p} = \begin{cases} 1/\sqrt[4]{N} & \text{if } \Delta(N) \equiv 1 \bmod 4 \\ 5/(3\sqrt[4]{4N}) & \text{if } \Delta(N) \equiv 0 \bmod 4 \end{cases}$.

In other words, given N and W, Q has a binomial distribution $B(W, \hat{p})$. In fact, this is the way he computed $E[Q]$ for a given N in his thesis. A new symbol will be introduced to present his result here.

Proposition 3.3.6 *[13, p. 45] Let Q be the number of forms enqueued during the factorization of N. Then*

$$
\begin{aligned}
\hat{\mu}: &= E[Q|N] = E[E[Q|W]|N] = E[W \cdot \hat{p}|N] \\
&= \hat{p} \cdot E[W|N] = \hat{p}(\mu\sqrt[4]{N}) \sim \begin{cases} \frac{2(\sqrt{2}+1)\log 2}{2^k-2} & \text{if } \Delta(N) \equiv 1 \bmod 4 \\ \frac{5(\sqrt{2}+1)\log 2}{2(2^k-2)} & \text{if } \Delta(N) \equiv 0 \bmod 4 \end{cases}
\end{aligned}
$$

Note that $\hat{\mu}$ is constant with respect to N when k and $(\Delta(N) \bmod 4)$ are fixed.

Next we consider N as a random variable as above.

Proposition 3.3.7 *Assume Assumption 3.3.5. Then* $E[Q] = \hat{\mu}$ *and* $Var[Q] \approx \hat{\mu}^2 + \hat{\mu}$.

Proof We have

$$E[Q] = E[E[Q|N]] = E[\hat{\mu}] = \hat{\mu}$$

$$\begin{aligned}
Var[Q] &= E[Q^2] - (E[Q])^2 = E[Q^2] - \hat{\mu}^2 \\
E[Q^2|N] &= E[E[Q^2|W]|N] = E[Var[Q|W] + (E[Q|W])^2|N] \\
&= E[W\hat{p}(1-\hat{p}) + (W\hat{p})^2|N] \\
&= \hat{p} \cdot E[W|N] - \hat{p}^2 \cdot E[W|N] + \hat{p}^2 \cdot E[W^2|N] \\
&= \hat{\mu} - \hat{p} \cdot \hat{\mu} + \hat{p}^2(2\mu^2\sqrt{N} - \mu\sqrt[4]{N}) \\
&= \hat{\mu} - 2\hat{p} \cdot \hat{\mu} + 2\hat{\mu}^2 \\
E[Q^2] &= E[E[Q^2|N]] = E[\hat{\mu} - 2\hat{p} \cdot \hat{\mu} + 2\hat{\mu}^2] = 2\hat{\mu}^2 + \hat{\mu} - 2\hat{\mu} \cdot E[\hat{p}] \\
Var[Q] &= \hat{\mu}^2 + \hat{\mu} - 2\hat{\mu} \cdot E[\hat{p}]
\end{aligned}$$

Now $\hat{\mu}$ has a value near 2 when k is a small integer and gets smaller when k gets larger. Moreover, $E[\hat{p}] < 1/10^4$. This is why we can claim that $Var[Y] \approx \hat{\mu}^2 + \hat{\mu}$. ■

3.4 The Effect of Racing Multipliers

Gower explained well the effect of multipliers on W and Q in his thesis. We will use his arguments to explain explicitly the probability distribution of W and Q in the case of racing multipliers. The version of SQUFOF with racing multipliers works as follows. Let the n multipliers be $m_1, \ldots, m_n$. We run SQUFOF simultaneously on $m_i N$ for $1 \leq i \leq n$. Specifically, perform one step of SQUFOF for factoring $m_1 N$, then one step for $m_2 N$, etc., to one step for $m_n N$. Then perform the second step of SQUFOF for $m_1 N$, the second step for $m_2 N$, etc., to the second step for $m_n N$. Then perform the third steps, etc. Maintain n separate queues, one for each $m_i N$. Stop when the first proper square form is found. Suppose it is in the algorithm for $m_i N$. Then finish the algorithm just for $m_i N$ to find a proper factor of N.

3.4.1 Probability Distribution of W

Again we present Gower's result with our new symbol. Everything is the same as in Section 3.3 except that we have mN instead of N, where m is the multiplier.

Proposition 3.4.1 *[13, p. 57] Let $m = \Pi_{j=1}^{r} q_j$, where $q_1, \ldots, q_r$ are r distinct small odd primes with $q_j \nmid N$ for all j. Let W be the number of forms that SQUFOF must examine before finding a proper square form during the factorization of mN. Then*

$$\mu := \frac{E[W|N]}{\sqrt[4]{N}} = \frac{1}{p\sqrt[4]{N}} \sim \begin{cases} \frac{2(\sqrt{2}+1)\log 2}{2^k-2} \Pi_{j=1}^{r} \frac{q_j+1}{2q_j^{3/4}} & \text{if } \Delta(mN) \equiv 1 \bmod 4 \\ \frac{3(\sqrt{2}+2)\log 2}{2(2^k-2)} \Pi_{j=1}^{r} \frac{q_j+1}{2q_j^{3/4}} & \text{if } \Delta(mN) \equiv 0 \bmod 4 \end{cases}$$

Note that W follows a geometric distribution with p for a given N and this is how to prove the above proposition actually.

Now consider the case that we use n multipliers and race them. Let W_i be the number of forms that SQUFOF must examine before finding a proper square form during the factorization of $m_i N$. Then the total number of forms that SQUFOF must examine before finding a proper square form during the factorization of N is equal to $n \cdot W = n \cdot \min_{1 \le i \le n}(W_i|N)$. Define μ for each multiplier by $\mu_i := \frac{E[W_i|N]}{\sqrt[4]{N}} = \frac{1}{p_i \sqrt[4]{N}}$, where W_i follows a geometric distribution with p_i. Because $W = \min_{1 \le i \le n}(W_i|N)$, W also follows a geometric distribution with $p = 1 - \Pi_{i=1}^{n}(1 - p_i)$ for a given N.

Next we consider N as a random variable which follows a uniform distribution with the following conditions;

1. k is fixed.

2. N is odd with k distinct prime factors and larger than 10^{10}.

3. The congruence class (either 0 or 1 mod 4) of $\Delta(m_i N)$ is fixed for all i.

Proposition 3.4.2 *Let $Y = nW/\sqrt[4]{N}$. Then $E[Y] \approx \mu_h$ and $Var[Y] \approx \mu_h^2$, where μ_h means the harmonic mean of $\mu_1, \ldots, \mu_n$.*

Proof

$$\begin{aligned} p\sqrt[4]{N} &= \Big(\sum_{i} p_i - \sum_{i<j} p_i p_j + \sum_{i<j<k} p_i p_j p_k - \cdots \Big)\sqrt[4]{N} \\ &= \sum_{i} \frac{1}{\mu_i} - \sum_{i<j} \frac{1}{\mu_i \mu_j} \frac{1}{\sqrt[4]{N}} + \sum_{i<j<k} \frac{1}{\mu_i \mu_j \mu_k} \frac{1}{(\sqrt[4]{N})^2} - \cdots \\ &=: \frac{1}{\mu(N)}, \end{aligned}$$

where $\mu(N)$ is a value depending on N.

$$\frac{E[W|N]}{\sqrt[4]{N}} = \frac{1}{p\sqrt[4]{N}} = \mu(N)$$

$$\begin{aligned} E[Y] &= E\ E\ \frac{nW}{\sqrt[4]{N}}|N\ = E\ n\frac{E[W|N]}{\sqrt[4]{N}} \\ &= nE[\mu(N)] \approx E[\mu_h] = \mu_h \end{aligned}$$

$$\begin{aligned} Var[Y] &= E[Y^2] - (E[Y])^2 \\ E[Y^2|N] &= E\ E\ \frac{n^2W^2}{\sqrt{N}}|N\ = E\ n^2\frac{E[W^2|N]}{\sqrt{N}} \\ &= \frac{n^2}{\sqrt{N}}(Var[W|N] + E[W|N]^2) \\ &= \frac{n^2}{\sqrt{N}}\ \frac{1}{p^2} - \frac{1}{p} + \frac{1}{p}\ ^2 = \frac{n^2}{\sqrt{N}}\ \frac{2}{p^2} - \frac{1}{p} \\ &= n^2\ \ 2\mu^2(N) - \frac{\mu(N)}{\sqrt[4]{N}} \\ E[Y^2] &= E[E[Y^2|N]] = E\ n^2\ \ 2\mu^2(N) - \frac{\mu(N)}{\sqrt[4]{N}} \\ &= 2n^2E[\mu^2(N)] - n^2E\ \frac{\mu(N)}{\sqrt[4]{N}} \end{aligned}$$

Therefore,

$$\begin{aligned} Var[Y] &= 2n^2E[\mu^2(N)] - n^2E\ \frac{\mu(N)}{\sqrt[4]{N}}\ - n^2E[\mu(N)]^2 \\ &= n^2E[\mu^2(N)] + n^2Var[\mu(N)] - n^2E\ \frac{\mu(N)}{\sqrt[4]{N}}\ \approx \mu_h^2. \end{aligned}$$

■

In the proof of Proposition 3.4.2, we actually assumed that $\mu(N)$ is almost constant such that $n\mu(N) \approx \mu_h$ and $\mu(N)/\sqrt[4]{N}$ is small enough to be negligible.

3.4.2 Probability Distribution of Q

Gower computed the probability that a form will be enqueued in the case of a multiplier in order to compute $E[Q]$ in [13, p. 57 – 61]. We compute it in reverse by $E[Q|N]/E[W|N]$. Then the probability is

$$\hat{p} = \begin{cases} \frac{1}{\sqrt[4]{N}} \Pi_{j=1}^{r} \frac{2q_j+1}{q_j+1} q_j^{-1/4} & \text{if } \Delta(mN) \equiv 1 \bmod 4 \\ \frac{1}{\sqrt[4]{N}} \frac{5}{3\sqrt{2}} \Pi_{j=1}^{r} \frac{2q_j+1}{q_j+1} q_j^{-1/4} & \text{if } \Delta(mN) \equiv 0 \bmod 4 \end{cases}$$

We denote it simply by $\hat{p} = c/\sqrt[4]{N}$, where c is a constant with respect to N.

Now consider the case that we use n multipliers and race them.

Assumption 3.4.3 *Even though c depends on the multipliers, we would like to assume that c is constant no matter what the multipliers are. Taking c as the mean value of them would be reasonable.*

The goal of this assumption is that we can consider that Q follows a binomial distribution $B(nW, \hat{p})$, where W follows the same geometric distribution as in Section 3.4.1.

Next we consider N as a random variable as in Section 3.4.1.

Proposition 3.4.4 *$E[Q] \approx c\mu_h$ and $Var[Q] \approx (c\mu_h)^2 + c\mu_h$*

Proof We have

$$\begin{aligned} E[Q|N] &= E[E[Q|W]|N] = E[nW \cdot \hat{p}|N] \\ &= n\hat{p} \cdot E[W|N] = n \cdot \frac{c}{\sqrt[4]{N}} \cdot E[W|N] = nc\mu(N) \\ &\approx c\mu_h \\ E[Q] &= E[E[Q|N]] \approx E[c\mu_h] = c\mu_h \end{aligned}$$

$$\begin{aligned}
E[Q^2|N] &= E[E[Q^2|W]|N] = E[Var[Q|W] + E[Q|W]^2|N] \\
&= E[nW\hat{p}(1-\hat{p}) + (nW\hat{p})^2|N] \\
&= n\hat{p} \cdot E[W|N] - n\hat{p}^2 \cdot E[W|N] + n^2\hat{p}^2 \cdot E[W^2|N] \\
&\approx c\mu_h - \hat{p} \cdot c\mu_h + n^2\hat{p}^2(2\mu^2(N)\sqrt{N} - \mu(N)\sqrt[4]{N}) \\
&\approx c\mu_h - \hat{p} \cdot c\mu_h + 2(c\mu_h)^2 - n\hat{p} \cdot c\mu_h \\
&= c\mu_h - \hat{p}(n+1) \cdot c\mu_h + 2(c\mu_h)^2
\end{aligned}$$

$$\begin{aligned}
E[Q^2] &= E[E[Q^2|N]] \approx E[c\mu_h - \hat{p}(n+1) \cdot c\mu_h + 2(c\mu_h)^2] \\
&= 2(c\mu_h)^2 + c\mu_h - (n+1) \cdot c\mu_h E[\hat{p}] \\
Var[Q] &\approx (c\mu_h)^2 + c\mu_h - (n+1) \cdot c\mu_h E[\hat{p}] \approx (c\mu_h)^2 + c\mu_h
\end{aligned}$$

■

In the proof of Proposition 3.4.4, we actually assume that $E[\hat{p}]$ is negligible.

3.5 Conclusion with Experimental Data

In his thesis, Gower used experimental data to support his assumptions and propositions. Now we will show that the data also support our propositions which are based on Gower's assumptions and propositions. Eventually, it will fortify Gower's arguments.

Table 3.1 is the experimental data when $k = 2$, $\Delta(mN) \equiv 0 \bmod 4$. Gower generated 10,000 values for N by choosing 100 primes p congruent to 1 mod 4 with $30013 \leq p \leq 32089$ and 100 primes q congruent to 3 mod 4 with $34123 \leq q \leq 36067$, then taking $N = pq$.

The first column is the multiplier ($m = 1$ means no multiplier), the second column is μ in our thesis, and the third column and the fourth column are experimental results for $E[Y]$ and $\sigma[Y]$ respectively, where σ means the standard deviation. Gower denoted these by $\overline{\text{FWRD}}$ and σ (FWRD), respectively.

Table 3.1
Two-prime statistics for FWRD and QUEUE.

m	$\frac{E[W]}{\sqrt[4]{N}}$	$\overline{\text{FWRD}}$	σ (FWRD)	$E[Q]$	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
1	1.7749	1.6917	1.6895	2.0918	2.2934	2.9424	366
3	1.5573	1.4858	1.4576	2.4404	2.2791	2.8100	543
5	1.5925	1.5089	1.5070	2.3009	2.2690	2.8437	411
7	1.6497	1.6021	1.5822	2.2412	2.3414	2.9434	319
11	1.7631	1.6361	1.7075	2.1868	2.2358	2.8973	269
15	1.3972	1.3285	1.3097	2.6844	2.2763	2.7559	362
21	1.4474	1.3463	1.3523	2.6147	2.2288	2.7165	399
33	1.5469	1.4800	1.4530	2.5513	2.2827	2.7500	411
35	1.4802	1.4248	1.4154	2.4653	2.3204	2.8353	235
55	1.5819	1.5134	1.4945	2.4055	2.2922	2.7989	344
77	1.6388	1.5763	1.5819	2.3430	2.3108	2.8277	245
105	1.2987	1.2336	1.2134	2.8762	2.2807	2.7106	349
165	1.3879	1.3299	1.3133	2.8064	2.2988	2.7525	240
231	1.4378	1.3706	1.3696	2.7335	2.2969	2.7777	170
385	1.4703	1.4052	1.4068	2.5773	2.3008	2.8204	224
1155	1.2900	1.2192	1.2012	3.0069	2.2260	2.6422	750

Gower claimed that his assumptions and conclusions are reasonable because the second column and the third column look almost the same. But also, the third column and the fourth column look almost the same. It will support our Proposition 3.3.4 and Propostion 3.4.2 when $n = 1$.

The fifth column is $\hat{\mu}$ (when $m = 1$) or $c\mu$ (when $m = 1$) in our thesis. Note that we denote μ_h simply by μ when $n = 1$. The sixth column and the seventh column are experimental results for $E[Q]$ and $\sigma[Q]$ respectively and Gower denoted these by $\overline{\text{QUEUE}}$ and σ (QUEUE), respectively.

Gower also claimed that his assumptions and conclusions are reasonable because the fifth column and the sixth column look almost the same. Moreover, we can see that (sixth column)^2+(sixth column)$\approx$(seventh column)^2, for example, as $2.2934^2 + 2.2934 = 2.7483^2 \approx 2.9424^2$. It will support our Proposition 3.3.7 and Propostion 3.4.4 when $n = 1$.

Table 3.2 shows the experimental data for racing multipliers when $k = 2, n = 2, m_1 = 1, \Delta(m_i N) \equiv 0 \bmod 4$.

The table shows the similar relation between experimental results for $E[Y]$ and $\sigma[Y]$ and between experimental results for $E[Q]$ and $\sigma[Q]$ with Table 3.1. It confirms our Proposition 3.3.7 and Propostion 3.4.4.

Moreover, we now have theoretical approximations for $E[Y]$ and $E[Q]$ in the case of racing multipliers which contains harmonic mean. For example, If we choose $m_2 = 3$, then $\mu_1 = 1.7749, \mu_2 = 1.5573$. Therefore, $\mu_h = 1.6590 \approx 1.6507$.

Gower already knew some of these results, but did not explain it clearly enough. He put it in the future work section of his thesis.

Table 3.2
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 1$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
3	1.6507	1.6425	2.4674	3.1937	3
5	1.6773	1.6584	2.4698	3.2857	5
7	1.6814	1.6673	2.3961	3.0491	1
11	1.7735	1.7637	2.5019	3.3211	0
$3 \cdot 5$	1.5558	1.5462	2.5187	3.4828	4
$3 \cdot 7$	1.5858	1.5787	2.4410	3.3558	1
$3 \cdot 11$	1.6198	1.6637	2.4077	3.2573	4
$5 \cdot 7$	1.5891	1.5405	2.4164	3.0042	1
$5 \cdot 11$	1.6287	1.6242	2.4059	3.0370	2
$7 \cdot 11$	1.6815	1.6626	2.4511	3.2944	2
$3 \cdot 5 \cdot 7$	1.4871	1.4730	2.5010	3.5409	3
$3 \cdot 5 \cdot 11$	1.5439	1.5412	2.4272	3.0739	4
$3 \cdot 7 \cdot 11$	1.5549	1.5324	2.4275	3.0720	1
$5 \cdot 7 \cdot 11$	1.5881	1.6041	2.4175	3.1048	9
$3 \cdot 5 \cdot 7 \cdot 11$	1.4635	1.4453	2.3796	3.0285	104

4. PRIME FACTORS OF $N_p = (p^p - 1)/(p - 1)$

4.1 Introduction

In this chapter, we investigate how many prime factors N_p has when p is an odd prime. This number will play an important role in supporting a conjecture about the period of the Bell numbers modulo a prime in the following chapter.

The work of this chapter and the next one has been published in [23].

4.2 Heuristic Data for Prime Factors

We start with a basic well known fact about prime factors of N_p.

Theorem 4.2.1 *Every prime factor of N_p has the form $2kp + 1$ when p is an odd prime.*

Proof Suppose q is prime and $q \mid N_p$. The radix-p expansion

$$N_p = 1 + \sum_{i=1}^{p-1} p^i \equiv 1 + \sum_{i=1}^{p-1} p = 1 + p(p-1) \equiv 1 \bmod (p^2 - p)$$

shows that $\gcd(N_p, p^2 - p) = 1$, whence $\gcd(q, p^2 - p) = 1$. In particular q is odd, $q = p$, and $q \nmid (p - 1)$.

We have $p^p \equiv 1 \bmod q$ because $q \mid N_p$. Let d be the smallest positive integer for which $p^d \equiv 1 \bmod q$. We cannot have $d = 1$ because q does not divide $p - 1$. But $d \mid p$, so $d = p$. By Fermat's little theorem, $p^{q-1} \equiv 1 \bmod q$, so $p \mid (q - 1)$. The quotient $(q-1)/p$ must be even because both p and q are odd. Thus, $q = 2kp+1$. ■

According to page 381 of Dickson [11], Euler proved this fact in 1755. On the following page Dickson writes that Legendre proved it again in 1798. A recent proof of a slightly more general result appears on page 642 of Sabia and Tesauri [27].

Now for each $1 \leq k \leq 50$, we counted all the primes $q = 2kp + 1$ that divide N_p for all odd primes $p < 100000$. For example, when $k = 5$ there are 1352 primes $p < 100000$ for which $q = 2kp + 1$ is also prime, and 129 of these q divide N_p, so the fraction of the primes $q = 2kp + 1$ that divide N_p is $129/1352 = 0.095$. We call this fraction "Prob" in Table 4.1 and Table 4.2 because it approximates the probability that q divides N_p, given that p and $q = 2kp + 1$ are prime, for fixed k.

Table 4.1
Probability that $2kp + 1$ divides N_p when k is odd

k	$1/(2k)$	Prob	k	$1/(2k)$	Prob
1	0.500	0.503	3	0.167	0.171
5	0.100	0.095	7	0.071	0.076
9	0.056	0.047	11	0.045	0.042
13	0.038	0.051	15	0.033	0.033
17	0.029	0.032	19	0.026	0.021
21	0.024	0.016	23	0.022	0.021
25	0.020	0.021	27	0.019	0.021
29	0.017	0.022	31	0.016	0.019
33	0.015	0.021	35	0.014	0.015
37	0.014	0.014	39	0.013	0.011
41	0.012	0.010	43	0.012	0.010
45	0.011	0.012	47	0.011	0.011
49	0.010	0.014			

We can see easily that Prob is approximately $1/(2k)$ when k is odd in Table 4.1 and $1/k$ when k is even, except for a few anomalies, in Table 4.2. Note that these exceptional values of k have the form $2m^2$. Prob is about $2/k$ when $k = 2$, 18, 32 and 50, and is about $4/k$ when $k = 8$ in Table 4.2.

Table 4.2
Probability that $2kp+1$ divides N_p when k is even

k	$1/k$	Prob	k	$1/k$	Prob
2	0.500	1.000	4	0.250	0.247
6	0.167	0.173	8	0.125	0.496
10	0.100	0.096	12	0.083	0.082
14	0.071	0.068	16	0.063	0.064
18	0.056	0.111	20	0.050	0.050
22	0.045	0.054	24	0.042	0.042
26	0.038	0.052	28	0.036	0.036
30	0.033	0.031	32	0.031	0.055
34	0.029	0.032	36	0.028	0.030
38	0.026	0.024	40	0.025	0.020
42	0.024	0.023	44	0.023	0.020
46	0.022	0.022	48	0.021	0.025
50	0.020	0.043			

4.3 Interpretation of Data

Before we explain the anomalies in earnest, we explain why usually Prob is approximately $1/k$ when k is even and $1/(2k)$ when k is odd.

Suppose k is a positive integer and that both p and $q = 2kp+1$ are odd primes. Let g be a primitive root modulo q.

If $p \equiv 1 \bmod 4$ or k is even (so $q \equiv 1 \bmod 4$), then by the Law of Quadratic Reciprocity

$$\frac{p}{q} = \frac{q}{p} = \frac{2kp+1}{p} = \frac{1}{p} = +1,$$

so p is a quadratic residue modulo q. In this case $g^{2s} \equiv p \bmod q$ for some s. Now $(2kp+1) \mid (p^p - 1)$ if and only if $p^p \equiv g^{2sp} \equiv 1 \bmod q$, that is, if and only if

$(2k) \mid (2s)$, by Euler's criterion for power residues. It is natural to assume that $k \mid s$ with probability $1/k$ because k is fixed and s is a random integer.

If $p \equiv 3 \bmod 4$ and k is odd (so $q \equiv 3 \bmod 4$), then

$$\frac{p}{q} = -\frac{q}{p} = -\frac{2kp+1}{p} = -\frac{1}{p} = -1,$$

so p is a quadratic nonresidue modulo q. Now $g^{2s+1} \equiv p \bmod q$ for some s. Reasoning as before, $(2kp+1) \mid (p^p - 1)$ if and only if $(2k) \mid (2s+1)$, which is impossible. Therefore q does not divide N_p.

Thus, if we fix k and let p run over all primes, then the probability that $q = 2kp+1$ divides N_p is $1/k$ when k is even and $1/(2k)$ when k is odd because, when k is odd only those $p \equiv 1 \bmod 4$ (that is, half of the primes p) offer a chance for q to divide N_p.

In fact, when $k = 1$ and $p \equiv 1 \bmod 4$, q always divides N_p. This theorem must have been known long ago, but we could not find it in the literature.

Theorem 4.3.1 *If p is odd and $q = 2p+1$ is prime, then q divides N_p if and only if $p \equiv 1 \bmod 4$.*

Proof We have just seen that q does not divide N_p when $p \equiv 3 \bmod 4$. If $p \equiv 1 \bmod 4$, then p is a quadratic residue modulo q, as was mentioned above, so $p^p = p^{(q-1)/2} \equiv +1 \bmod q$ by Euler's criterion. Finally, q is too large to divide $p-1$, so q divides N_p. ■

Now we explain the anomalies, beginning with $k = 2$.

Theorem 4.3.2 *If $q = 4p+1$ is prime, then q divides N_p.*

This result was an old problem posed and solved more than 100 years ago. In [7] it was proposed as Problem 13058 by C. E. Bickmore and solved by him, by Nath Coondoo, and by others. Here is a modern proof.

Proof Since $q \equiv 1 \bmod 4$, there exists an integer I with $I^2 \equiv -1 \bmod q$. Then

$$(1+I)^4 \equiv (2I)^2 \equiv -4 \equiv \frac{1}{p} \bmod q.$$

Hence

$$p^p \equiv \left(\frac{1}{p}\right)^{-p} \equiv (1+I)^{-4p} \equiv (1+I)^{1-q} \equiv 1 \bmod q$$

by Fermat's theorem. Thus, q divides $p^p - 1$. But $q = 4p+1$ is too large to divide $p-1$, so q divides N_p. ■

Lemma 4.3.3 *Suppose q is prime and $q \equiv 1 \bmod 4$. If the integer ℓ divides $(q-1)/4$, then ℓ is a quadratic residue modulo q.*

Proof The hypothesis implies $\gcd(q, \ell) = 1$. In particular $\ell = 0$. Factor

$$\ell = \pm \ell_1 \ldots \ell_\nu \tag{4.1}$$

where each ℓ_j is prime.

The hypotheses that q is prime and $q \equiv 1 \bmod 4$ imply that ± 1 are quadratic residues modulo q.

We claim each ℓ_j is a quadratic residue modulo q, so their product (4.1) (or its negative) is also a quadratic residue.

If $\ell_j = 2$, then ℓ is even and $q \equiv 1 \bmod 8$. Since q is prime, 2 is a quadratic residue modulo q.

If instead ℓ_j is odd, then we can use quadratic reciprocity:

$$\left(\frac{\ell_j}{q}\right) = \left(\frac{q}{\ell_j}\right) = \left(\frac{1}{\ell_j}\right) = +1,$$

which completes the proof. ■

Theorem 4.3.4 *Let p be an odd positive integer and m be a positive integer. If $q = 4m^2p + 1$ is prime, then q divides $p^{m^2p} - 1$.*

Proof As in the proof of Theorem 4.3.2, $q \equiv 1 \bmod 4$, so there is an integer I with $I^2 \equiv -1 \bmod q$ and $(1+I)^4 \equiv -4 \bmod q$. By Lemma 4.3.3, m is a quadratic residue modulo q, so

$$-4m^2 \equiv (1+I)^4 m^2 \bmod q$$

is a fourth power modulo q, say $r^4 \equiv -4m^2 \bmod q$. Then

$$p^{m^2 p} = \left(\frac{q-1}{4m^2}\right)^{(q-1)/4} \equiv ((-4m^2)^{-1})^{(q-1)/4} = r^{1-q} \equiv 1 \bmod q,$$

which proves the theorem. ■

Of course, Theorem 4.3.2 is the case $m = 1$ of Theorem 4.3.4.

We now apply Theorem 4.3.4. As before, let g be a primitive root modulo q and let $a = g^{(q-1)/m^2} \bmod q$. Then a^j, $0 \le j < m^2$, are all the solutions to $x^{m^2} \equiv 1 \bmod q$. Let $b = p^p \bmod q$. By the theorem, $b^{m^2} \equiv 1 \bmod q$, so $b \equiv a^j \bmod q$ for some $0 \le j < m^2$. It is natural to assume that the case $j = 0$, that is, $q \mid N_p$, happens with probability $1/m^2$.

In the case $m = 2$, that is, $k = 8$, we can do even better.

Theorem 4.3.5 *If $q = 16p + 1$ is prime, then q divides $p^{2p} - 1$.*

Proof As in the proof of Theorem 4.3.2, there is an integer I with $I^2 \equiv -1 \bmod q$ and $(1+I)^4 \equiv -4 \bmod q$. Therefore, $(1+I)^8 \equiv 16 \equiv -1/p \bmod q$ and so

$$p^{2p} \equiv \left(\frac{-1}{p}\right)^{-2p} \equiv (1+I)^{-16p} \equiv (1+I)^{1-q} \equiv 1 \bmod q,$$

which proves the theorem. ■

Thus, a prime $q = 2kp + 1$ divides $(p^p - 1)(p^p + 1)$ when $k = 8$. Assuming that q has equal chance to divide either factor, the probability that q divides $p^p - 1$ is $1/2$.

So far, we have explained all the behavior seen in Table 4.2. Further experiments with $q = 2m^2 p + 1$ lead us to the following result, which generalizes Theorems 4.3.4 and 4.3.5.

Theorem 4.3.6 *Suppose p, m, t are positive integers, with t a power of 2 and $t > 1$. Let $k = (2m)^t/2$ and $q = 2kp + 1 = (2m)^t p + 1$. If q is prime, then (a) p is a $(2t)$-th power modulo q, and (b) $p^{kp/t} \equiv 1 \bmod q$.*

Proof To prove part (a), note that since $q \equiv 1 \bmod 2^t$, the cyclic multiplicative group $(\mathbf{Z}/q\mathbf{Z})^*$ of order $q-1$ has an element ω of order 2^t. Then $\omega^{2^{t-1}} \equiv -1 \bmod q$ so $I = \omega^{2^{t-2}}$ satisfies $I^2 \equiv -1 \bmod q$.

Now $m^t = (q-1)/(p2^t)$, so m is a quadratic residue modulo q by Lemma 4.3.3. We will show that $p^{-1} \equiv (1-q)/p = -(2m)^t \bmod q$ is a $(2t)$-th power modulo q.

If $t = 2$, then $-(2m)^t \equiv (2Im)^2 = (1+I)^4 m^2 \bmod q$ is a fourth power modulo q.

If $t > 2$, then $t \geq 4$ because t is a power of 2. Then $(q-1)/4 = 2mp((2m)^{t-1}/4)$ is divisible by $2m$. Hence $2m$ is a quadratic residue modulo q by Lemma 4.3.3. Therefore, $(2m)^t$ is a $(2t)$-th power modulo q. Finally, -1 is a (2^{t-1})-th power modulo q because 2^{t-1} divides $(q-1)/2$. Hence -1 is a $(2t)$-th power modulo q because $2t \leq 2^{t-1}$ when $t \geq 4$.

For part (b), apply part (a) and choose r with $r^{2t} \equiv p \bmod q$. Observe that $2t$ divides 2^t which divides $q - 1 = 2kp$. Hence,

$$1 \equiv r^{q-1} \equiv (r^{2t})^{2kp/2t} \equiv p^{kp/t} \bmod q.$$

This completes the proof. ■

When $t = 2$, Theorem 4.3.6 is just Theorem 4.3.4.

When $t = 4$, Theorem 4.3.6 says that if $q = (2m)^4 p + 1 = 16m^4 p + 1$ is prime, then q divides $p^{2m^4 p} - 1$. Theorem 4.3.5 is the case $m = 1$ of this statement.

When $t = 8$, Theorem 4.3.6 says that if $q = (2m)^8 p + 1 = 256m^8 p + 1$ is prime, then q divides $p^{16m^8 p} - 1$. The first case, $m = 1$, of this statement is for $k = 128$, which is beyond the end of Table 4.2.

4.4 Conclusion

We now apply Theorem 4.3.6. As above, let g be a primitive root modulo q and let $a = g^{(q-1)t/k} \bmod q$. Then a^j, $0 \le j < k/t$, are all the solutions to $x^{k/t} \equiv 1 \bmod q$. Let $b = p^p \bmod q$. By the theorem, $b^{k/t} \equiv 1 \bmod q$, so $b \equiv a^j \bmod q$ for some $0 \le j < k/t$. It is natural to assume that the case $j = 0$, that is, $q \mid N_p$, happens with probability $1/(k/t) = t/k$.

When k is an odd positive integer, define $c(k) = 1/2$. When k is an even positive integer, define $c(k)$ to be the largest power of 2, call it t, for which there exists an integer m so that $k = (2m)^t/2$. Note that $c(k) = 1$ if k is even and not of the form $2m^2$. Also, $c(k) \ge 2$ whenever $k = 2n^2$ because if $k = (2m)^t/2$ with $t \ge 2$, then $k = 2n^2$ with $n = 2^{(t-2)/2}m^{t/2}$. Note that

$$c(k) = \begin{cases} 1/2 & \text{if } k \text{ is odd,} \\ 1 & \text{if } k \text{ is even and not of the form } 2m^2, \\ O(\log k) & \text{if } k = 2m^2 \text{ for some positive integer } m. \end{cases} \tag{4.2}$$

Hence the average value of $c(k)$ is $3/4$ because the numbers $2m^2$ are rare.

We have given heuristic arguments which conclude that, for fixed k, when p and $q = 2kp + 1$ are both prime, the probability that q divides N_p is $c(k)/k$. Empirical evidence in Table 4.1 and Table 4.2 supports this conclusion. We have explained all the behavior shown in Table 4.1 and Table 4.2. We tested many other values of k and found no further anomalies beyond those listed in this chapter.

5. THE PERIOD OF THE BELL NUMBERS MODULO A PRIME

5.1 Introduction

The work of this chapter and the preceeding chapter have been published in [23].

The Bell exponential numbers $B(n)$ are positive integers that arise in combinatorics. They can be defined by the generating function, given by Bell [3] [4],

$$e^{e^x-1} = \sum_{n=0}^{\infty} B(n)\frac{x^n}{n!} \tag{5.1}$$

These numbers have been known for a long time and have a variety of interesting interpretations which include

1. $B(n)$ is the number of pattern sequences for words of n letters, as used in cryptology [19].

2. $B(n)$ is the number of ways n unlike objects can be placed in n like boxes allowing empty boxes [36].

3. $B(n)$ is the number of ways a product of n distinct primes may be factored into factors > 1 [18, p.179].

In conclusion, we can say simply that $B(n)$ is the number of partitions of a set of n members or equivalently, the number of equivalence relations on it.

For computational purposes, various defining relations are known, for example,

$$B(n) = \sum_{r=1}^{n}\sum_{k=0}^{r} \frac{(-1)^k}{r!}\binom{r}{k}(r-k)^n \tag{5.2}$$

given by Bell [3], and Mendelsohn and Riordan [22]. This formula, (5.2), is equivalent to

$$B(n) = \sum_{r=1}^{n} S(n,r) \tag{5.3}$$

where $S(n, r)$ are Stirling numbers of the second kind, and which was obtained by Broggi [8] and Becker and Riordan [5].

The formula

$$B(n+1) = (B+1)^n \tag{5.4}$$

where on the right, B^m is to be replaced by $B(m)$ after expansion of the binomial, was given by d'Ocagne [25].

For a study of arithmetic properties of $B(n)$, the congruence of Touchard [31],

$$B(n+p) \equiv B(n) + B(n+1) \bmod p \tag{5.5}$$

for a prime p, is basic.

In addition, we mention the following congruence given by Hall [15], Touchard [31], and Williams [37],

$$B(n+p^m) \equiv mB(n) + B(n+1) \bmod p \tag{5.6}$$

It was proved by Williams [37] that the minimum period of the sequence (reduced mod p)

$$B(0), B(1), B(2), \ldots, B(n), \ldots \tag{5.7}$$

is a divisor of

$$N_p = \frac{p^p - 1}{p - 1} \tag{5.8}$$

In fact, the minimum period equals N_p for every prime p for which this period is known.

Theorem 5.1.1 *The minimum period of the sequence* $\{B(n) \bmod p\}$ *is* N_p *when* p *is a prime* < 126 *and also when* $p = 137$, 149, 157, 163, 167 *or* 173.

Theorem 5.1.1 improves the first part of Theorem 3 of [33]. The statements about the primes $p = 103$, 107, 109, 137, 149 and 157 are new here and result from calculations we did using the same method as in [33]. These calculations are possible now because new prime factors have been discovered for these N_p. Table 5.1 lists all new prime factors discovered for N_p since [33], even when the factorization remains

incomplete. Table 5.1 uses the same notation and format as Table 1 of [33]. The "L" and "M" in the table represent pieces of algebraic factorizations explained in [33].

Table 5.1
Some new prime factors

p	New prime factors of N_p
103	6637242494411682594040191319 3.
103	167321256949237716863040684441514323749790592645938001.P98
107	847261197784821583381604854855693.P165
109L	708022605183994255434421517741836511379166407220 3.P58
137L	145022309304806896114020754741379 87.P85
149L	1489708492858878967197407256814153782649297 1.P115
149M	24356237167368011037018270166971738740925336580189261.P84
151	760658609581520401030226740176590735 3.C277
157L	26924627624276327689812\ 233716623975855765034528185267934207 73.P99
179	6183119082113155839913145480811 49.C369

Theorem 5.1.1 is proved by showing that the period does not divide N_p/q for any prime divisor q of N_p. (We made this check for each new prime q in Table 5.1, including those written as "Pxxx," and not just those for the p for which N_p is completely factored.) In [33], this condition was checked also for all pairs (p, q) of primes for which $p < 1100$, $q < 2^{31}$ and q divides N_p. It was conjectured there that the minimum period is always N_p. As early as 1979 [21] others wondered whether the minimum period is always N_p. See [10] for a summary of work on this conjecture up to 2008. We present a heuristic argument below supporting the conjecture.

5.2 The Heuristic Argument

We begin this section by stating the conjecture again.

Conjecture 5.2.1 *The minimum period of the sequence (reduced* mod p*)*

$$B(0), B(1), B(2), \ldots, B(n), \ldots$$

is

$$N_p = \frac{p^p - 1}{p - 1}.$$

Touchard's congruence (5.5) shows that any p consecutive values of $B(n) \bmod p$ determine the sequence modulo p after that point. If conjecture fails for p, then there is a prime factor q of N_p such that the period of the Bell numbers modulo p divides $N = N_p/q$. The period will divide N if and only if $B(N + i) \equiv B(i) \bmod p$ for $0 \leq i \leq p - 1$.

Assumption 5.2.2 *The numbers* $B(N + i) \bmod p$ *for all* $0 \leq i \leq p - 1$ *are independent random variables uniformly distributed in the interval* $[0, p - 1]$.

According to Assumption 5.2.2, the probability that the period divides N is p^{-p} because, for each i, there is one chance in p that $B(N + i)$ will have the needed value $B(i) \bmod p$. The probability that the period does not divide N is $1 - p^{-p}$.

Assumption 5.2.3 *The probabilities that the period divides* $N = N_p/q$ *for different prime divisors* q *of* N_p *are independent.*

According to Assumption 5.2.3, the probability that the minimum period is N_p is $(1 - p^{-p})^{d_p}$, where d_p is the number of distinct prime factors of N_p.

Now we try to estimate the expected value of the number d_p of distinct prime factors of N_p. We generally follow the heuristic argument on page 386 of [32].

First, we introduce the Bateman-Horn conjecture [2].

Conjecture 5.2.4 (Bateman-Horn) *Suppose* $f_1, f_2, \ldots, f_m$ *are polynomials in one variable with all coefficients integral and leading coefficients positive, their degrees begin* $h_1, h_2, \ldots, h_m$ *respectively. Suppose each of these polynomials is irreducible over*

the field of rational numbers and no two of them differ by a constant factor. Let $Q(f_1, f_2, \ldots, f_m; N)$ *denote the number of positive integers* n *between* 1 *and* N *inclusive such that* $f_1(n), f_2(n), \ldots, f_m(n)$ *are all primes. (We ignore the finitely many values of* n *for which some* $f_i(n)$ *is negative.) Then heuristically we would expect to have for* N *large*

$$Q(f_1, f_2, \ldots, f_m; N) \sim h_1^{-1} h_2^{-1} \cdots h_m^{-1} C(f_1, \ldots, f_m) \int_2^N (\log u)^{-m}\, du \tag{5.9}$$

where

$$C(f_1, \ldots, f_m) = \prod_{q \text{ prime}} \left\{ \left(1 - \frac{1}{q}\right)^{-m} \left(1 - \frac{\omega(q)}{q}\right) \right\} \tag{5.10}$$

where $\omega(q)$ *is the number of solutions of*

$$f_1(x) f_2(x) \cdots f_m(x) \equiv 0 \pmod{q}.$$

According to the Bateman-Horn conjecture, in order to count the number of primes $p \le x$ for which both p and $2kp + 1$ are prime, where k is a positive integer, we need to set $m = 2$, and $f_1(n) = n, f_2(n) = 2kn + 1$. Then the number is asymptotically

$$C(f_1, f_2) \int_2^x (\log u)^{-2}\, du,$$

where

$$\begin{aligned} C(f_1, f_2) &= \prod_{q \text{ prime}} \left\{ \left(1 - \frac{1}{q}\right)^{-2} \left(1 - \frac{\omega(q)}{q}\right) \right\}, \\ &\quad \text{where } \omega(q) = \begin{cases} 1 & \text{if } q \mid 2k \\ 2 & \text{if } q \nmid 2k \end{cases} \\ &= 2 \prod_{\substack{q \nmid 2k \\ q \text{ odd prime}}} \frac{q(q-2)}{(q-1)^2} \prod_{\substack{q \mid 2k \\ q \text{ odd prime}}} \frac{q}{q-1} \\ &= 2C_2 f(2k), \end{aligned}$$

where

$$C_2 = \prod_{q \text{ odd prime}} \left(1 - (q-1)^{-2}\right), \qquad f(n) = \prod_{\substack{q \mid n \\ q \text{ odd prime}}} \frac{q-1}{q-2}.$$

Moreover, $\int (\log u)^{-2}\, du = u/(\log u)^2 + 2\int (\log u)^{-3}\, du$. So the number of p will be approximately,

$$2C_2 f(2k)\frac{x}{(\log x)\log(2kx)}.$$

Second, we use the following well-known theorem.

Theorem 5.2.5 (Prime Number Theorem) *We define the prime-counting function at real values of x by $\pi(x) =$ the number of primes not exceeding x. Then, as x approaches infinity,*

$$\pi(x) \sim \frac{x}{\log x}$$

Therefore, if p is known to be prime and k is a positive integer, then the probability that $2kp+1$ is prime is $2C_2 f(2k)/\log(2kp)$.

Now we apply the results of the previous chapter. If p is prime and k is a positive integer, then the probability that $2kp+1$ is prime and divides N_p is

$$(2C_2 f(2k)/\log(2kp)) \cdot (c(k)/k)$$

where $c(k)$ is as in (4.2). For a fixed prime p and real numbers $A < B$, let $F_p(A, B)$ denote the expected number of prime factors of N_p between A and B. Then

$$F_p(A,B) \approx \sum_{\substack{k \\ A<2kp+1\le B}} \frac{2C_2 f(2k)c(k)}{k\log(2kp)}.$$

The anomalous values of $c(k)$ occur when k is twice a square, and these numbers are rare. The denominator $k\log(2kp)$ changes slowly with k. If $B - A$ is large, so that there are many k in the sum, then we may ignore the anomalies and replace $c(k)$ by its average value $3/4$. This change makes little difference in the sum. Thus,

$$F_p(A,B) \approx \sum_{\substack{k \\ A<2kp+1\le B}} \frac{3C_2 f(2k)}{2k\log(2kp)}. \tag{5.11}$$

We use the same heuristic argument that appears on page 386 of [32] in order to replace $C_2 f(2k)$ by 1. Suppose that $B - A$ is large. Let q be an odd prime for which $8pq^2 < B - A$. Then q divides about $1/q$ of the k's in the sum in (5.11). For precisely

these k's, the product $f(2k)$ includes the factor $(q-1)/(q-2)$. Thus, the average contribution of q to all $f(2k)$ in (5.11) is

$$\frac{1}{q}\cdot\frac{q-1}{q-2}+\quad 1-\frac{1}{q}\quad\cdot 1=\quad 1-\frac{1}{(q-1)^2}\quad^{-1} \tag{5.12}$$

For each odd prime $q<((B-A)/(8p))^{1/2}$, remove the factor $(q-1)/(q-2)$ from each $f(2k)$ in which appears, and insert the factor (5.12) into each term of (5.11) instead. Since $B-A$ is large, the denominators of (5.11) changes very slowly and little net change is made in (5.11). Now the product of the factor (5.12) over all primes $q<((B-A)/(8p))^{1/2}$ is essentially $1/C_2$, the error being by a factor of about $\exp(-((8p)/(B-A))^{1/2})$, which is very close to 1. In summary, if we change $C_2 f(2k)$ to 1, it makes very little difference.

Then we find

$$F_p(A,B)\approx \sum_{\substack{k\\ A<2kp+1\le B}}\frac{3}{2k\log(2kp)}\approx\frac{3}{2}\log\quad\frac{\log B}{\log A}\quad .$$

Thus, the expected value of d_p is

$$F_p\left(2p,N_p\right)\approx\frac{3}{2}\log\quad\frac{\log N_p}{\log(2p)}\quad=\frac{3}{2}\log\quad\frac{\log_p N_p}{\log_p(2p)}\quad\approx\frac{3}{2}\log p.$$

Using this estimate for d_p, we find that the probability that the minimum period is N_p is $(1-p^{-p})^{3(\log p)/2}$. When p is large, this number is approximately $1-(3\log p)/(2p^p)$ by the binomial theorem. This shows that the heuristic probability that the minimum period of the Bell numbers modulo p is N_p is exceedingly close to 1 when p is a large prime.

Finally, we compute the expected number of primes $p>x$ for which the conjecture fails. When $x>2$, this number is

$$\sum_{p>x}\frac{3\log p}{2p^p}<\sum_{p>x}p^{1-x}\le\int_x^\infty t^{1-x}\,dt=\frac{x^{2-x}}{x-2}.$$

By Theorem 5.1.1, the conjecture holds for all primes $p<126$. Taking $x=126$, the expected number of primes for which the conjecture fails is $<126^{-124}/124<10^{-262}$. Thus, the heuristic argument predicts that the conjecture is almost certainly true.

LIST OF REFERENCES

LIST OF REFERENCES

[1] F. Arslan, S. Sertöz, Genus calculations of complete intersections, *Communications in Algebra*, 26:8, 2463–2471, 1998.

[2] P. T. Bateman, R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 16, 363–367, 1962.

[3] E. T. Bell, Exponential numbers, *Amer. Math. Monthly*, 41, 411–419, 1934.

[4] E. T. Bell, The iterated exponential integers, *Ann. of Math.*, 39, 539–557, 1938.

[5] H. W. Becker, J. Riordan, The arithmetic of Bell and Stirling numbers, *Amer. J. Math.*, 70, 385–394, 1948.

[6] A. Benjamin, C. Bennett, The probability of relatively prime polynomials, *Mathematics Magazine*, 80:3, 196–202, 2007.

[7] C. E. Bickmore, Problem 13058. *Math. Quest. Educ. Times*, 65, 78, 1896.

[8] U. Broggi, Su di qualche applicazione dei numeri di Stirling, *1st. Lombardo Rend.*, II.s., 66, 196–202, 1933.

[9] D. Buell, *Binary Quadratic Forms*, Springer-Verlag, 1989.

[10] M. Car, L. H. Gallardo, O. Rahavandrainy, L. N. Vaserstein, About the period of Bell numbers modulo a prime. *Bull. Korean Math. Soc.*, 45:1, 143–155, 2008.

[11] L. E. Dickson, *History of the Theory of Numbers, Volume 1: Divisibility and Primality*. Chelsea Publishing Company, New York, New York, 1971.

[12] D. Eisenbud, *Commutative Algebra With a View Toward Algebraic Geometry*, Springer-Verlag, New York Inc., 1995.

[13] J. Gower, Square Form Factorization, Ph.D. thesis, Purdue University, December 2004.

[14] J. Gower, S. S. Wagstaff, Jr., Square Form Factorization, *Math. Comp.*, 77:261, 551–588, 2008.

[15] M. Hall, Arithmetic properties of a partition function, (Abstract 200), *Bull. Amer. Math. Soc.*, 40, 1934.

[16] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.

[17] N. Jacobson, *Basic Algebra I*, W. H. Freeman and Company, 1985.

[18] C. Jordan, *Calculus of Finite Differences*, Second Edition, Chelsea Publ. Co., New York, 1950.

[19] J. Levine, A binomial identity related to rhyming sequences, *Math. Mag.*, 32, 71–74, 1958.

[20] J. Levine, R. E. Dalton, Minimum periods, modulo p, of first-order Bell exponential numbers, *Math. Comp.*, 16, 416–423, 1962.

[21] W. F. Lunnon, P. A. B. Pleasants, N. M. Stephens, Arithmetic properties of Bell numbers to a composite modulus I. *Acta Arith.*, 35, 1–16, 1979.

[22] N. S. Mendelsohn, J. Riordan, Problem 4340 and solution, *Amer. Math. Monthly*, 58, 46–48, 1951.

[23] P. L. Montgomery, S. Nahm, S. S. Wagstaff, Jr., The period of the Bell numbers modulo a prime, *Math. Comp.*, 79:271, 1793–1800, 2010.

[24] H. Niederreiter, C. Xing, *Rational Points on Curves over Finite Fields, Theory and Applications*, Cambridge University Press, 2001.

[25] M. d'Ocagne, Sur une classe de nombres remarquables, *Amer. J. Math.*, 9, 353–380, 1887.

[26] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhaüser, Second edition, 1994.

[27] J. Sabia and S. Tesauri, The least prime in certain arithmetic progressions. *Amer. Math. Monthly*, 116, 641–643, 2009.

[28] N. Shang, M. Nabeel, E. Bertino, X. Zou, Broadcast Group Key Management with Access Control Vectors, CERIAS Tech Report 2010-03, Purdue University, 2010.

[29] D. Shanks, *SQUFOF notes*, Unpublished manuscript, 30 handwritten pages, available as 27 printed pages at `http://homes.cerias.purdue.edu/~ssw/gowerthesis804/index.html` .

[30] L. Smith, *Polynomial Invariants of Finite Groups*, A K Peters, Ltd. 1995.

[31] J. Touchard, Propriétés arithmétiques de certains nombres recurrents, *Ann. Soc. Sci. Bruxelles*, 53A, 21–31, 1933.

[32] S. S. Wagstaff, Jr., Divisors of Mersenne numbers. *Math. Comp.*, 40, 385–397, 1983.

[33] S. S. Wagstaff, Jr., Aurifeuillian factorizations and the period of the Bell numbers modulo a prime. *Math. Comp.*, 65, 383–391, 1996.

[34] A. Weil, *Foundations of Algebraic Geometry*, American Mathematical Society, 1946.

[35] A. Weil, *Sur les courbes alébriques et les variétés qui s'en déduisent*, Hermann, Paris, 1948.

[36] W. A. Whitworth, *Choice and Chance*, Hafner Publ. Co., New York, 1951.

[37] G. T. Williams, Numbers generated by the function e^{e^x-1}, *Amer. Math. Monthly*, 52, 323–327, 1945.

[38] X. Zou, Y. Dai, E. Bertino, A practical and flexible key management mechanism for trusted collaborative computing. In INFOCOM 2008. *The 27th conference on Computer Communications*, 538–546, April 2008.

VITA

VITA

Sangil Nahm was born in Pohang, Republic of Korea, on November 16, 1975. After finishing high school in 1994, he studied mathematics at Seoul National University. After graduation, he performed his military service in Republic of Korea Army between December 1998 and February 2001. He received an M.S. in mathematics from Seoul National University in February 2003 and a Ph.D. in mathematics from Purdue University in West Lafayette in May 2011.