CERIAS Tech Report 2004-31

SQUARE FORM FACTORIZATION

by Jason E. Gower

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

SQUARE FORM FACTORIZATION

A Thesis

Submitted to the Faculty

of

Purdue University

by

Jason Eric Gower

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

December 2004

Dedicated to my parents, Ray and Sandy.

ACKNOWLEDGMENTS

Special thanks go to my advisor, Professor Samuel Wagstaff. During the last four years, Sam has been a constant source of encouragement, patience, and guidance, without which I would never have completed this work.

I thank all the members of my committee, Professors Lucier, Moh, Shahidi, and Wagstaff, for their guidance, patience, and careful reading of this thesis.

The love and support shown to me by my friends and family has been incredible. I am especially indebted to my parents, Ray and Sandy, for their unconditional love and support, and to Ben, Bill, Tuli, Martina, Mark, and Cynthia, for being such great friends during some tough times. I also thank my sensei, Jackie Martinez, and everyone I have ever trained with at Challenge Karate, my home away from home.

Finally, I thank both Sam and CERIAS at Purdue University for generous funding and travel funds, and Professor Dasgupta for his helpful comments about probability theory.

TABLE OF CONTENTS

Page

ABSTRACT

Gower, Jason Eric. Ph.D., Purdue University, December, 2004. Square Form Factorization. Major Professor: Samuel S. Wagstaff, Jr.

We present a detailed analysis of SQUFOF, Daniel Shanks' Square Form Factorization algorithm. We give the expected running time and space requirement for SQUFOF. We analyze the effect of multipliers, either used for a single factorization or when racing the algorithm in parallel.

1. Introduction

1.1 Integer Factorization

> The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Further, the dignity of the science itself seems to require solution of a problem so elegant and so celebrated.
>
> Carl Friedrich Gauss *Disquisitiones Arithmeticae* [7]

The Fundamental Theorem of Arithmetic says that the factorization of any positive integer N into primes is unique apart from the order of the prime factors. Once we are certain that such a factorization exists, the question then becomes how to find the factorization. Of course, one can use trial division with primes up to $\sqrt{N}$, though this will be very time consuming for large N. So the real question is how to factor large N in a relatively short amount of time. Since factoring an integer is essentially a recursive problem—if we can find p and q such that $N = pq$, then we continue the process with either p or q, whichever is composite—we are really only interested in a fast algorithm for finding a non-trivial divisor of N.

During the course of the last few hundred years, many people have spent time looking for good factorization algorithms. As a result, today there are several algorithms to choose from if one needs to factor large numbers. On the other hand, most of these algorithms are designed to work quickly only with numbers of a specific type.

For example, Pollard's "$p-1$" method is a very quick algorithm for factoring N, but only if N has a factor p such that $p-1$ is a product of relatively small primes.

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}, say, and the quadratic sieve (QS) is best for numbers between 10^{50} and 10^{120}, etc. As new algorithms are discovered, these ranges change. With present 32-bit computer architecture, Daniel Shanks' Square Form Factorization algorithm (SQUFOF) is the clear champion factoring algorithm for numbers between 10^{10} and 10^{18}, and will likely remain so. The SQUFOF algorithm is extraordinarily simple, beautiful and efficient. Further, it is used in most implementations of NFS and QS to factor small auxiliary numbers arising in factoring large N.

1.2 SQUFOF Briefly

The historically first "sub-exponential" factorization algorithm was the continued fraction algorithm (see [2]), CFRAC for short. Most modern factorization algorithms, including CFRAC, look for a pair of integers x, y such that

$$x^2 \equiv y^2 \bmod N \quad \text{and} \quad x \not\equiv y \bmod N\ .$$

If such a pair can be found, then $\gcd(x \pm y, N)$ will be a non-trivial factor of N. The main difference between the modern algorithms such as CFRAC, the Quadratic Sieve, and the Number Field Sieve is the way in which they go about finding the pair x, y. CFRAC finds this pair by generating the sequences A_n, B_n, q_n, P_n, and Q_n for $n \geq 0$, where

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

is the continued fraction expansion of $\sqrt{N}$, the quantity A_{n+1}/B_{n+1} is n^{th} convergent of the continued fraction, and the P_n, Q_n arise in the computation of the n^{th} complete

quotient of the continued fraction. For the purpose of using CFRAC to factor the number N we need the fundamental equation

$$(-1)^n Q_n = A_n^2 - B_n^2 N \ , \tag{1.1}$$

or modulo N we have

$$(-1)^n Q_n \equiv A_n^2 \bmod N \ .$$

The strategy for finding a congruent pair of squares modulo N is then to find a set of indices Λ such that there is an integer Q with

$$\prod_{n \in \Lambda} (-1)^n Q_n = Q^2 \ .$$

If we let

$$A = \prod_{n \in \Lambda} A_n \ ,$$

then we have the congruence $Q^2 \equiv A^2 \bmod N$.

In order to factor N we also need $Q \not\equiv A \bmod N$. This will be the case at least half of the time for the following reason. If we assume the N is a square-free product of $k \geq 2$ primes, then there are only two ways to trivially split N into the product $(Q-A)(Q+A)$ out of 2^k possible splittings. So the probability that we have $Q \not\equiv A \bmod N$ is

$$\frac{2^k - 2}{2^k} \geq \frac{1}{2} \ .$$

CFRAC can fail if either there is no such set Λ or if all such sets lead only to a trivial factorization. It was during an investigation [19] of these failures of CFRAC that Daniel Shanks observed that one could compute successive Q_n until one finds $Q_n = Q^2$ for the single index n. Furthermore, Shanks discovered that we really only need to compute P_n, Q_n and q_n, which seems surprising in light of Equation (1.1). Obviously we must expect to go further along the continued fraction if we are to find such a square, but it may be worth the extra work since the P_n and Q_n can be

computed very quickly and remain bounded less than $2\sqrt{N}$ for all n, unlike the A_n which grow exponentially. That all of this is possible and more importantly, leads to an extremely fast algorithm, is seen once we switch to the language of binary quadratic forms.

Since the P_n and Q_n satisfy the equation

$$N = P_n^2 + Q_{n-1}Q_n \quad \text{for all } n,$$

the quadratic form in the variables x and y,

$$(-1)^{n-1}Q_{n-1}x^2 + 2P_nxy + (-1)^nQ_ny^2 \ ,$$

which we will write as

$$F_n = \left((-1)^{n-1}Q_{n-1}, 2P_n, (-1)^nQ_n\right) \ ,$$

has discriminant $4N$, where the discriminant of the form (a, b, c) is defined to be $b^2 - 4ac$. Starting with the principal form of discriminant $4N$,

$$\left(1, 2q_0, q_0^2 - N\right) \ ,$$

we proceed along the principal cycle of reduced forms of discriminant $4N$ by $F_{n+1} = \rho\left(F_n\right)$, where ρ is the so-called standard reduction operator. Once we find an even index n such that $F_n = F$ is the square form $(-Q, 2P, S^2)$, we compute the inverse square root

$$F^{-1/2} = G = (-S, 2P, SQ) \ ,$$

and iteratively use the reduction operator on this form to generate the sequence

$$G_m = \rho^m\left(G\right) = \left((-1)^{n-1}S_{m-1}, 2R_m, (-1)^nS_n\right) \ ,$$

where the R_m and S_m are computed using the equations for P_n and Q_n, respectively. Eventually we will find two consecutive forms G_m and G_{m+1} with $R_m = R_{m+1}$. The form G_m must be ambiguous and yield a factor of $4N$. Square forms that lead to a non-trivial factorization of N are called proper square forms.

Shanks did publish works [16], [18] describing some of his other algorithms for factoring integers, computing class numbers and regulators that are similar to SQUFOF. Though he never published any papers about SQUFOF, he did lecture about its virtues and he explained how it works to a few people. Today, there are a few published descriptions of the algorithm, such as [4], [12], [3], and [20], but none contain a detailed analysis. After Shanks' death in 1996, Hugh Williams discovered some of Shanks unpublished hand-written manuscripts [15], [14], [13]. These manuscripts were subsequently typed by Stephen McMath and posted on the web by W. David Joyner [1].

The manuscript [15] is the closest Shanks ever came to a full description and analysis of SQUFOF. In [15], Shanks describes the algorithm and begins a heuristic argument for the following statement. Let N be a product of k distinct odd primes with $N \equiv 3 \bmod 4$. The expected number of forms that SQUFOF must examine before find a proper square form is

$$\frac{3\left(\sqrt{2}+2\right)\log 2}{2\left(2^k-2\right)}\ \sqrt[4]{N}\ .$$

The manuscript also contains a discussion of how to decide whether a square form is proper or not, but there is no proof for why this decision is always correct. Shanks also discusses the use of multipliers as a way to overcome a failure to factor N, and the possibility of racing multipliers.

1.3 Contribution of the Thesis

It is the purpose of this thesis to give a detailed description and analysis of SQUFOF. We complete the heuristic argument started by Shanks in [15] and extend the argument to the cases $N \equiv 1,\ 2 \bmod 4$. We further generalize this argument to the case where multipliers are used to factor N. We give a detailed description of the process for deciding which square forms are proper, show how to modify it when multipliers are used, and prove that it works in all cases. The results of some experiments provide evidence that our simplifying assumptions are reasonable.

1.4 Outline of the Thesis

In Chapter 2 we provide a minimum background for the sequel. We describe the algorithm in Chapter 3. Then in Chapter 4 we give the expected running time and space requirements for the basic algorithm. Chapter 5 presents the running time and space requirements when using multipliers. We present in Chapter 6 the results of some experiments, which provide evidence that our simplifying assumptions are reasonable. Finally, we conclude in Chapter 7 with some questions for future research.

2. Background

2.1 Binary Quadratic Forms

We begin with a brief survey of binary quadratic forms. For a more detailed account of the theory see [3] or [4].

2.1.1 Basic Definitions

Let $f(x,y) = ax^2 + bxy + cy^2$, a *binary quadratic form* in the variables x and y. The constants a, b, and c will be taken in $\mathbb{Z}$. The *discriminant* of f is defined to be $b^2 - 4ac$. A discriminant Δ is called *fundamental* if either Δ is odd and square-free or Δ is even, $\Delta/4$ is square-free, and $\Delta/4 \equiv 2$ or $3 \bmod 4$. The form f is called *primitive* if $\gcd(a,b,c) = 1$.

We will frequently write $f = (a,b,c)$, or just $(a,b,*)$, where c can be computed if we know the discriminant of f. We shall also write $f = (a,*,*)$ whenever b and c are either unknown or irrelevant. Note that if Δ is the discriminant of the form f, then $\Delta \equiv 0$ or $1 \bmod 4$, and $b \equiv \Delta \bmod 2$.

The form f is said to *represent* $m \in \mathbb{Z}$ if there exists $x_0, y_0 \in \mathbb{Z}$ such that $f(x_0,y_0) = ax_0^2 + bx_0y_0 + cy_0^2 = m$. The representation is *primitive* if $\gcd(x_0,y_0) = 1$.

We say that two forms f_1 and f_2 are *properly equivalent*, or just *equivalent*, if we can find $\alpha,\beta,\gamma,\delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1$ and $f_1(x,y) = f_2(\alpha x + \beta y, \gamma x + \delta y)$. We write $f_1 \sim f_2$ when f_1 and f_2 are equivalent. If $\alpha\delta - \beta\gamma = -1$, then we say that f_1 and f_2 are *improperly equivalent*. Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ be the classical modular group and define the action of Γ 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 $f_1 \sim f_2$ if and only if f_1 and f_2 are equivalent modulo the action of Γ. We make special note of the equivalence: $(a, b + 2na, a + nb + c) \sim (a, b, c)$ for any $n \in \mathbb{Z}$, using the matrix $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

The number of classes of forms of discriminant Δ will be written $h^+(\Delta)$ or just h^+. It can be shown that $h^+(\Delta)$ is finite.

Forms with negative discriminant are called *definite*, while forms with positive discriminant are called *indefinite*. We will be concerned only with indefinite forms.

Any form (k, kn, c) is called *ambiguous*. There exists an ambiguous form (k, kn, c) of discriminant Δ for each divisor k of Δ. We also refer to any form (a, b, a) as ambiguous since it is equivalent to $(b + 2a, b + 2a, a)$.

2.1.2 Indefinite Forms

Let Δ be any non-square positive integer. Each class of indefinite forms of discriminant Δ contains a set of canonical representatives, called *reduced* forms. The form $f = (a, b, c)$ is called *reduced* if $\left|\sqrt{\Delta} - 2|a|\right| < b < \sqrt{\Delta}$. It is not hard to see that f is reduced if and only if $\left|\sqrt{\Delta} - 2|c|\right| < b < \sqrt{\Delta}$, and that the number of reduced forms of a given discriminant is finite. For any indefinite form $f = (a, b, c)$ with $ac \neq 0$ we define the *standard reduction operator* by

$$\rho(a, b, c) = \left(c, r(-b, c), \frac{r(-b, c)^2 - \Delta}{4c}\right) , \tag{2.1}$$

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

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

$\rho(f)$ is called the *reduction* of f and the result of n applications of ρ is written $\rho^n(f)$. It will be convenient to define the *inverse reduction operator* by

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

where $r(-b,a)$ is defined as in the definition of ρ. Note that if the discriminant of f is Δ, then the discriminants of both $\rho(f)$ and $\rho^{-1}(f)$ are Δ.

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 of discriminant $\Delta > 0$ 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*. Furthermore, 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 $(1,b,c)$.

If (a,b,c) is a form of discriminant Δ which represents the integer r, then $s^2 \equiv \Delta \mod 4r$ has a solution. Conversely, if a solution to $s^2 \equiv \Delta \mod 4r$ exists, then r is represented by some form of discriminant Δ.

Let $\left(\frac{r}{s}\right)$ be the Jacobi symbol and define the quadratic characters $\chi(r) = \left(\frac{-1}{r}\right)$ and $\psi(r) = \left(\frac{2}{r}\right)$. The *generic characters* of a discriminant Δ are

$$\begin{aligned} &\left(\frac{r}{p}\right) && \text{for all odd primes } p \text{ that divide } \Delta\ , \\ &\chi(r) && \text{if } \Delta \text{ is even and } \Delta/4 \equiv 3,4,7 \bmod 8\ , \end{aligned}$$

$$\begin{aligned} \psi(r) &\quad \text{if } \Delta \text{ is even and } \Delta/4 \equiv 2 \bmod 8 \ , \\ \chi(r) \cdot \psi(r) &\quad \text{if } \Delta \text{ is even and } \Delta/4 \equiv 6 \bmod 8 \ , \\ \chi(r) \text{ and } \psi(r) &\quad \text{if } \Delta \text{ is even and } \Delta/4 \equiv 0 \bmod 8 \ . \end{aligned}$$

These characters are multiplicative functions from $\mathbb{Z}$ to $\{\pm 1\}$. Suppose the discriminant Δ has n generic characters. Then for some arbitrary ordering we have a vector-valued function from $\mathbb{Z}$ to the n-tuples with ± 1 entries. The n-tuple corresponding to an integer r is called the *assigned value* of r. It can be shown that all integers r which are representable by forms of a given equivalence class possess the same assigned values of generic characters. The set of classes of forms possessing the same assigned values of generic characters is called a *genus* of forms. The genus for which the assigned value is $(1, 1, \ldots, 1)$ is called the *principal genus*. The principal genus contains the principal form. An integer r is representable by some class of forms of discriminant Δ if and only if the assigned values of the generic characters of r match the assigned values of characters of some genus of discriminant Δ. This is true if and only if the congruence $s^2 \equiv \Delta \bmod 4r$ is solvable.

The number of ambiguous classes (including the principal class) is equal to one-half the number of possible genera. If Δ is a fundamental discriminant, then we know that the product of the assigned values for the characters for any genus is $+1$ and that exactly half of the possible genera exist.

2.1.3 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

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

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

$$\left(a_1 a_2/n^2, b_1 + 2a_1 z/n, * \right) \ ,$$

where the third coefficient may be determined by the discriminant formula. 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

$$\left(a^2/n^2, b - 2acy/n, *\right) \ .$$

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

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

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 $(a^2, b, -c)$.

Also note that if f is a square form on the principal cycle, then f must have a square root on the principal cycle. To see this, let $f^{1/2}$ be any square root of f. If neither $f^{1/2}$ nor $\rho^n\left(f^{1/2}\right)$ for all $n > 0$ is on the principal cycle, then $f^{1/2}$ must be equivalent to some ambiguous form other than the principal form, say g. Then $f^{1/2} \circ g$ is equivalent to the principal form, and its square is equivalent to f. Finally, we can reduce this form to an equivalent form on the principal cycle.

Observe that

$$(1, b_1, c_1) \circ (a_2, b_2, c_2) \sim (a_2, b_2, c_2) \ ,$$

and that

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

In other words, under composition, the principal class is the identity and the associate is the inverse. Also composition is commutative and associative. Thus the set of equivalence classes of forms of a given discriminant is an abelian group under composition.

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 $[q_0, q_1, \ldots]$. The expansion is ultimately periodic, meaning that for some $j > 0$ we will have $a_i = a_{i+j}$ for all $i > 0$, where j is the period of the continued fraction. In this case, we will write $\sqrt{N} = [q_0, \overline{q_1, \ldots, q_j}]$.

The q_i are called the *partial quotients* of the continued fraction. The rational number $[q_0, q_1, \ldots, q_n]$ is called the n^{th} *convergent* of the continued fraction. Define

$$A_n = \begin{cases} 1 & \text{if } n = 0 \ , \\ q_0 & \text{if } n = 1 \ , \\ q_n A_{n-1} + A_{n-2} & \text{if } n \geq 2 \ , \end{cases}$$

and

$$B_n = \begin{cases} 0 & \text{if } n = 0 \ , \\ 1 & \text{if } n = 1 \ , \\ q_n B_{n-1} + B_{n-2} & \text{if } n \geq 2 \ . \end{cases}$$

Then $[q_0, q_1, \ldots, q_n] = A_{n+1}/B_{n+1}$ for $n \geq 0$.

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

$$P_n = \begin{cases} 0 & \text{if } n = 0 \ , \\ q_0 & \text{if } n = 1 \ , \\ q_{n-1} Q_{n-1} - P_{n-1} & \text{if } n \geq 2 \ , \end{cases} \tag{2.2}$$

and

$$Q_n = \begin{cases} 1 & \text{if } n = 0 \ , \\ N - q_0^2 & \text{if } n = 1 \ , \\ Q_{n-2} + (P_{n-1} - P_n)q_{n-1} & \text{if } n \geq 1 \ . \end{cases} \tag{2.3}$$

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

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

Some important facts that we shall need are as follows.

$$(-1)^n Q_n = A_n^2 - B_n^2 N \ ,$$

$$\frac{A_n + B_n\sqrt{N}}{\sqrt{Q_n}} = \frac{A_{n-1} + B_{n-1}\sqrt{N}}{\sqrt{Q_{n-1}}} \cdot \frac{\sqrt{N} + P_n}{\sqrt{Q_{n-1}Q_n}} \ ,$$

$$N = P_n^2 + Q_n Q_{n-1} \ ,$$

$$0 \leq P_n, \, Q_n < 2\sqrt{N} \ .$$

See [12] for a proof of these facts.

2.3 Real Quadratic Number Fields

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

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

Any finite extension of $\mathbb{Q}$ is called a *number field*. The extension $\mathbb{Q}(\sqrt{N})/\mathbb{Q}$ is called the *quadratic number field* of radicand N and discriminant Δ. We note in passing that $\mathbb{Q}(\sqrt{N}) = \mathbb{Q}(\sqrt{\Delta})$.

Let K be any number field. The ring of integers $\mathcal{O}_K$ of K is the integral closure of $\mathbb{Z}$ in K. When $K = \mathbb{Q}(\sqrt{N})$ we have $\mathcal{O}_K = \mathbb{Z}[\omega]$, where

$$\omega = \begin{cases} \sqrt{N} & \text{if } N \equiv 2, 3 \bmod 4 \ , \\ \dfrac{1+\sqrt{N}}{2} & \text{if } N \equiv 1 \bmod 4 \ . \end{cases}$$

The odd rational primes of $\mathbb{Z}[\omega]$ fall into three categories according to the value of the Jacobi symbol

$$\left(\frac{\Delta}{p}\right) = \begin{cases} 0 & \text{if } p \text{ is a } \textit{ramified} \text{ prime} \ , \\ 1 & \text{if } p \text{ is a } \textit{split} \text{ prime} \ , \\ -1 & \text{if } p \text{ is a } \textit{inert} \text{ prime} \ . \end{cases}$$

When $N \equiv 1 \bmod 4$, the rational prime 2 is split whenever $N \equiv 1 \bmod 8$, and inert whenever $N \equiv 5 \bmod 8$. The ramified primes are precisely those that divide Δ. A consequence of the Chebotarev density theorem (see [10]) is that the density of primes that split in $\mathbb{Q}[\sqrt{\Delta}]$ is $1/2$. Since there are only finitely many ramified primes, it follows that the density of inert primes is also $1/2$.

A *fractional ideal* is a subset $\mathfrak{a}$ of $\mathbb{Q}(\sqrt{\Delta})$ such that

1. for any $\alpha, \beta \in \mathfrak{a}$ and any $\lambda, \mu \in \mathbb{Z}[\omega]$ we have $\lambda\alpha + \mu\beta \in \mathfrak{a}$.

2. there exist a fixed $\nu \in \mathbb{Z}[\omega]$ such that for every $\alpha \in \mathfrak{a}$ we have $\nu\alpha \in \mathbb{Z}[\omega]$.

Two fractional ideals $\mathfrak{a}, \mathfrak{b}$ are said to be *equivalent* if there is some $\alpha \in \mathbb{Z}[\omega]$ such that $\mathfrak{a} = (\alpha)\mathfrak{b}$, and *narrowly equivalent* if there is some $\alpha \in \mathbb{Z}[\omega]$ with positive norm such that $\mathfrak{a} = (\alpha)\mathfrak{b}$. Both types of equivalences are indeed equivalence relations. The first equivalence leads to the *class group* I/P, where I is the set of fractional ideals and P is the set of principal ideals. Narrow equivalence leads to the *narrow class group* I/P^+, where P^+ is the set of principal ideals with positive norm. The *class number* of $\mathbb{Q}(\sqrt{\Delta})$ is the order of I/P, while the *narrow class number* is the order of I/P^+, written $h(\Delta)$ and $h^+(\Delta)$, respectively. It is no coincidence that we use the same symbol to denote both the number of classes of forms of discriminant Δ and

the narrow class number of $\mathbb{Q}(\sqrt{\Delta})$, as it can be shown (see [4]) that they are indeed the same.

2.4 The Infrastructure of the Class Group

The theories of binary quadratic forms, continued fractions, and real quadratic number fields are closely related (see [5] or [4].) First, there is a correspondence between binary quadratic forms of discriminant $N > 0$ and the fractional ideals of $\mathbb{Q}(\sqrt{N})$ defined by

$$(a, b, c) \longleftrightarrow \left(a\mathbb{Z} + \left(\frac{-b + \sqrt{N}}{2} \right) \mathbb{Z} \right) \alpha \ ,$$

where α is any element of $\mathbb{Q}(\sqrt{N})^*$ such that $N(\alpha) = \text{sign}(a)$. We mention that under this correspondence, composition of forms corresponds with ideal multiplication.

There is also a correspondence between binary quadratic forms and continued fractions. The definitions for P_n and Q_n in Section 2.2 satisfy

$$N = P_n^2 + Q_{n-1}Q_n \quad \text{for all } n \ ,$$

and so the binary quadratic form

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

has discriminant $4N$. In fact, the sequence of forms $F_0, F_1, \ldots$ constitutes the principal cycle of forms of discriminant $4N$, where $F_0 = (1, 2q_0, q_0^2 - N)$.

Shanks defined the *infrastructure* of the class group [17] collectively as the inner structure within each cycle of reduced forms determined by ρ, the standard reduction operator. Originally, Shanks defined the infrastructure distance between the form F_n and the principal form by the equation

$$d_n = \log \left(A_n + B_n \sqrt{N} \right) \ ,$$

but this metric did not have all the desirable properties that one would like it to have, so he later [15] changed it to

$$d_n = \log\left(\frac{A_n + B_n\sqrt{N}}{\sqrt{Q_n}}\right).$$

In [9], Lenstra independently proposed this same metric in a slightly different form as follows. Let $f = (a, b, c)$ be a form of discriminant Δ. Then

$$d\left(f, \rho(f)\right) = \frac{1}{2}\log\left|\frac{b + \sqrt{\Delta}}{b - \sqrt{\Delta}}\right|.$$

That these two definitions agree follows from the previously stated facts at the end of Section 2.2.

Now by the laws of Khinchin, Gauss-Kuzmin, and Lévy [8], we can approximate d_n by

$$\log\left(\frac{A_n + B_n\sqrt{N}}{\sqrt{Q_n}}\right) \doteq \frac{\pi^2}{12\log 2}\, n\,, \tag{2.4}$$

where the constant $\pi^2/(12\log 2)$ is approximately 1.19.

More generally, one can define the infrastructure distance $d(f, g)$ between two quadratic forms by the following. Let $\mathfrak{a}, \mathfrak{b}$ be the ideals corresponding to f, g respectively. If f and g are narrowly equivalent, then we can find γ with $N(\gamma) > 0$ such that $\mathfrak{a} = \gamma\mathfrak{b}$. Define the infrastructure distance between f and g by

$$d(f, g) = \frac{1}{2}\log\left|\frac{\gamma}{\sigma(\gamma)}\right|,$$

where σ is the automorphism of $\mathbb{Q}(\sqrt{N})$ taking $\sqrt{N}$ to $-\sqrt{N}$. With this definition, we can see that the distance between f^2 and the principal form is twice the distance between f and the principal form. To see this, let $\mathfrak{a}$ be the fractional ideal corresponding to f and let 1 denote the principal form. Write $\mathfrak{a} = \gamma \cdot 1$, hence $\mathfrak{a}^2 = \gamma^2 \cdot 1$. Then

$$d(f^2, 1) = \frac{1}{2}\log\left|\frac{\gamma^2}{\sigma(\gamma^2)}\right| = \frac{1}{2}\log\left|\frac{\gamma}{\sigma(\gamma)}\right|^2 = 2\, d(f, 1)\,.$$

More generally, let $\mathfrak{b}_1 = \gamma_1\mathfrak{a}_1$ and $\mathfrak{b}_2 = \gamma_2\mathfrak{a}_2$, so that $\mathfrak{b}_1\mathfrak{b}_2 = \gamma_1\gamma_2\mathfrak{a}_1\mathfrak{a}_2$. If f_i, g_i corresponds to $\mathfrak{a}_i, \mathfrak{b}_i$, respectively, then we have

$$d\left(g_1 \circ g_2, f_1 \circ f_2\right) = d\left(g_1, f_1\right) + d\left(g_2, f_2\right) \ . \tag{2.5}$$

Now suppose F_n is a square form on the principal cycle. Then we know that a square root of F_n must also lie on the principal cycle at a distance $d_n/2$ from the principal period. But using the approximation (2.4), this form will be very close to $F_{n/2}$. Also note that Equation (2.5) can be used to show that an inverse square root of F_n is at a distance $d_n/2$ in the reverse direction.

2.5 Asymptotics

We will be interested in finding the asymptotic behavior of many quantities, each of which will ultimately depend on N, the number we are trying to factor. We will say that $f\left(N\right)$ is *asymptotic* to $g\left(N\right)$, written $f\left(N\right) \sim g\left(N\right)$, if $g(N) \neq 0$ for $N > 0$ and

$$\lim_{N\to\infty} \frac{f(N)}{g(N)} = 1 \ .$$

We will also make use of "Big Oh" notation. We say that $f\left(N\right)$ is "Big Oh" of $g\left(N\right)$, written $f\left(N\right) = O\left(g\left(N\right)\right)$, if there is a constant C such that

$$|f\left(N\right)| \leq C|g\left(N\right)| \qquad \text{for all } N > 0 \ .$$

The following two basic lemmas will be useful.

Lemma 2.5.1. *If $f_1\left(N\right) \sim g_1\left(N\right)$, $f_2\left(N\right) \sim g_2\left(N\right)$ and $f_i\left(N\right), g_i\left(N\right) \neq 0$ for $N > 0$, then*

$$f_1\left(N\right)/f_2\left(N\right) \sim g_1\left(N\right)/g_2\left(N\right) \ .$$

Proof.

$$\lim_{N\to\infty} \frac{f_1(N)/f_2(N)}{g_1(N)/g_2(N)} = \lim_{N\to\infty} \frac{f_1(N)}{g_1(N)} \cdot \frac{g_2(N)}{f_2(N)}$$

$$= \lim_{N\to\infty} \frac{f_1(N)}{g_1(N)} \cdot \left[\lim_{N\to\infty} \frac{f_2(N)}{g_2(N)}\right]^{-1}$$
$$= 1 \cdot 1 = 1 \, .$$

□

Lemma 2.5.2. *Suppose that* $1 \leq f(N), g(N)$ *for all* $N > 0$ *and that* $g \to \infty$ *as* $N \to \infty$. *If* $f = g + O(1)$, *then* $f \sim g$.

Proof. By assumption there exists a constant C such that $|f - g| \leq C$ for all $N > 0$. Thus $g - C \leq f \leq g + C$ for all $N > 0$. Hence

$$1 = \lim_{N\to\infty} \frac{g - C}{g} \leq \lim_{N\to\infty} \frac{f}{g} \leq \lim_{N\to\infty} \frac{g + C}{g} = 1 \, ,$$

and therefore $\lim_{N\to\infty} f/g = 1$. □

3. The Description of the Algorithm

We now describe the algorithm in detail. We begin with a description of the fastest and most practical version. A more general version is then described.

3.1 Continued Fractions Description

As usual, we assume that N is a square-free positive integer. In most implementations of SQUFOF, we work with binary quadratic forms of discriminant $\Delta = 4N$. Unfortunately if $N \equiv 1 \bmod 4$, then Δ is not a fundamental discriminant. Although the algorithm works for non-fundamental discriminants, the analysis of SQUFOF presented in subsequent chapters will assume that Δ is fundamental. Therefore, if $N \equiv 1 \bmod 4$ then we replace N with $2N$. We may now assume that $N \equiv 2$ or $3 \bmod 4$ for the remainder of this section. Finally, take $\Delta = 4N$ which is then always a fundamental discriminant.

The principal form is $F_0 = (1, 2q_0, N - q_0^2)$. We compute the forms on the principal cycle by

$$F_n = \rho^n(F_0) = \left((-1)^{n-1}Q_{n-1}, 2P_n, (-1)^n Q_n\right) \ ,$$

where P_n and Q_n are calculated according to (2.2), (2.3), and (2.2). 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. This form may not be reduced so let $G_0 = (-S_{-1}, 2R_0, S_0)$ be its reduction, where

$$R_0 = P + S\left\lfloor \frac{q_0 - P}{S} \right\rfloor \ ,$$
$$S_{-1} = S, \qquad S_0 = \frac{N - R_0^2}{S} \ .$$

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 $t_m = \left\lfloor \frac{q_0 + R_m}{S_m} \right\rfloor$, for $m \geq 1$, which are completely analogous to (2.2), (2.3), and (2.2), we generate a new sequence of forms

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

Now suppose we find m such that $R_m = R_{m+1}$. We expect this to happen at approximately $m \doteq n/2$ for reasons explained at the end of Section 2.4. 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

$$N = S_m \left(S_{m-1} + S_m \frac{t_m^2}{4} \right) \ ,$$

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.

One should note that all computations other than those of F_0 and G_0 are with numbers less than $2\sqrt{N}$ in magnitude. So if N is taken to be no larger than double the word size of the computer, then all computations (except F_0 and G_0) will be with single precision integers.

There are three main issues that arise at this point. First, we will need to test every other form for squareness. This is not a major obstacle since there fast algorithms to test for squareness. A more serious issue is the possibility of ending with the trivial factorization. We could go back 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. Finally, there may be no proper square forms at all on the principal cycle. If this is the case, then we can try factoring mN, for some small m. We shall see later that this is a reasonable thing to do.

3.2 Identifying Proper Square Forms

We begin with a few propositions about square roots of square forms.

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

Proof. This follows directly from the definition of composition of forms, noting that $(a^2, 2b, -c)$ is equivalent to any form $(a^2, 2\beta, *)$, where $\beta \equiv b \bmod a^2$. □

Let $b = \left\lfloor \sqrt{N} \right\rfloor$ and $\mathbf{1} = (1, 2b, c)$ denote the principal form. Let $b' = \left\lfloor \sqrt{N} \right\rfloor$ or $\left\lfloor \sqrt{N} \right\rfloor - 1$, 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. *Suppose that a is a positive odd integer, b is a positive integer,* $\gcd(a,b) = 1$, *and that $F_n = (a^2, 2b, -c)$ is a square form on the principal cycle of discriminant $4N$, with $c > 0$. Some form $(\alpha, 2\beta, *)$ 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 $\pm\mathbf{1}$, $\pm\mathbf{2}$.*

Proof. First suppose that the form $(a, 2\beta, *)$ appears as form F_m on the principal cycle with $m < n$. This form is equivalent to $(a, 2b, -ac)$, and $-\mathbf{1} \sim (a, 2b, -ac) \circ -\mathbf{1} \sim (-a, 2b, ac)$, so we are done. Similarly, if $F_m = (-a, 2\beta, *) \sim (-a, 2b, ac)$, then $(-a, 2b, ac) \sim \mathbf{1}$.

Now suppose that the form $(2a, 2\beta, *)$ appears as F_m. Then $-\mathbf{2} \sim (2a, 2\beta, *) \circ -\mathbf{2} \sim (-a, 2\beta, *) \sim (-a, 2b, ac)$. Finally, if $F_m = (-2a, 2\beta, *)$, then $\mathbf{2} \sim (-2a, 2\beta, *) \circ \mathbf{2} \sim (-a, 2\beta, *) \sim (-a, 2b, ac)$.

Finally, suppose that there is no form $(\alpha, 2\beta, *)$ with $\alpha \in \{\pm a, \pm 2a\}$ with $\beta \equiv b \bmod a$ which appears on the principal cycle as a form F_m with $m < n$. The square root $f = (-a, 2b, ac)$ cannot be equivalent to $\mathbf{1}$, since if it is then we can find a multiple of $2a$ that we can add to $2b$ to get an equivalent reduced form $(a, 2\beta, *)$ on the principal cycle with $\beta \equiv b \bmod a$. But then this form is a square root of F_n

and hence must appear on the principal cycle before F_n, since $d(f, \mathbf{1}) = d(F_n, \mathbf{1})/2$. Therefore f cannot be equivalent to $\mathbf{1}$.

In fact, if $f \sim g$ with $g \in \{\pm\mathbf{1}, \pm\mathbf{2}\}$, then $f \circ g \sim \mathbf{1}$, and $f \circ g = (\alpha, 2\beta', *)$ for $\alpha \in \{\pm a, \pm 2a\}$ and $\beta' \equiv b \bmod a$. But then $f \circ g$ is a square root of F_n, and $f \circ g$ is equivalent to some reduced form $(\alpha, 2\beta, *)$ on the principal cycle with $\beta \equiv \beta' \equiv b \bmod a$. As before this form must appear on the principal cycle before F_n, a contradiction. So it must be that f is not equivalent to any of the forms $\mathbf{1}, \pm\mathbf{2}$.

□

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 $\left(Q_m/2, \overline{P_m}\right)$ 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 $\left(Q_m, \overline{P_m}\right)$ 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 $F_n = (-a, 2b, c^2) \sim (c^2, 2b, -a)^{-1} \sim (-c, 2b, ac)^{-2} \sim (ac, 2b, -c)^2$, then we search the queue in the order that items are put into the queue for the pair $(c, 2b \bmod c)$, taking $c > 0$. Proposition 3.2.2 says that if this pair is in the queue, then the form $(ac, 2b, -c)$ 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 $(c, 2b \bmod c)$ is not in the queue, then Proposition 3.2.2 says that $(ac, 2b, -c)$ is not equivalent to one of the forms $\pm\mathbf{1}, \pm\mathbf{2}$, hence the square form is proper.

Note that these quantities will be one-quarter the precision of N. Hence, the queue entries will be relatively small and easy to work with. Also note that if we have found a square form $F_n = (-a, 2b, c^2)$ and also the pair $(c, 2b \bmod c)$ in the queue, then we may delete this pair along with all other pairs that precede it in the queue. This is possible since if we find another square form F_m with $n < m$, then any of its square roots appearing on the principal cycle must appear after the discovered square root for F_n because of the infrastructure explained in Section 2.4.

3.3 The Algorithm

We now give the algorithm in pseudo-code.

1: Initialize. Read the positive integer N to be factored. If $N \equiv 1 \bmod 4$ then set $N \leftarrow 2N$. In any case, set

$$L \leftarrow 2\sqrt{2\sqrt{N}}\,,$$
$$QA \leftarrow 1\,,$$
$$S \leftarrow \left\lfloor \sqrt{N} \right\rfloor\,,$$
$$PB \leftarrow S\,,$$
$$QB \leftarrow N - PB \cdot PB\,.$$

If $QB = 0$, stop and output the factor PB of N.

2: Cycle forward to find a proper square form. Note that *two* iterations of ρ are done in step 2.

2a: Set $q \leftarrow \lfloor (S + PB)/QB \rfloor$ and $PA \leftarrow q \cdot QB - PB$.

2b: If $QB \leq L$, then:

If QB is even, put the pair $(QB/2, PB \bmod QB/2)$ into the QUEUE; otherwise, if $QB \leq L/2$, then put the pair $(QB, PB \bmod QB)$ into the QUEUE.

2c: Set $QA \leftarrow QA + q \cdot (PB - PA)$. If QA is not the square of an integer, then go to step 2d. Otherwise, set $R \leftarrow \sqrt{QA}$, a positive integer. If there is no pair (R, T) in the QUEUE for which R divides $PA - T$, then go to Step 3. If $R > 1$ and there is a pair (R, T) in the QUEUE for which R divides $PA - T$, then remove all pairs from the beginning of the QUEUE up to and including this pair and go to step 2d. If $R = 1$ and there is a pair $(1, T)$ in the QUEUE, then the algorithm fails.

2d: Set $q \leftarrow \lfloor (S + PA)/QA \rfloor$ and $PB \leftarrow q \cdot QA - PA$.

2e: If $QA \leq L$, then:

If QA is even, then put the pair $(QA/2, PA \bmod QA/2)$ into the QUEUE; otherwise, if $QA \leq L/2$, then put the pair $(QA, PA \bmod QA)$ into the QUEUE.

2f: Set $QB \leftarrow QB + q\,(PA - PB)$ and then go to step 2a.

3: Compute an inverse square root of the square form. Set

$$QA \leftarrow R\,,$$
$$PB \leftarrow PA + R \cdot \lfloor (S - PA)\,/R \rfloor\ ,$$
$$QB \leftarrow (N - PB \cdot PB)\,/QA \quad \text{(This division is exact.)}$$

4: Cycle in the reverse direction to find a factor of N.

4a: Set $q \leftarrow \lfloor (S + PB)\,/QB \rfloor$ and $PA \leftarrow q \cdot QB - PB$.

4b: If $PA = PB$, then go to step 5a.

4c: Set

$$QA \leftarrow QA + q \cdot (PB - PA)\ ,$$
$$q \leftarrow \lfloor (S + PA)\,/QA \rfloor\ ,$$
$$PB \leftarrow q \cdot QA - PA\,.$$

4d: If $PA = PB$, then go to step 5b.

4e: Set $QB \leftarrow QB + q\,(PA - PB)$ and then go to step 4a.

5: Print the factor of N.

5a: Set $QA \leftarrow QB$.

5b: If QA is even, set $QA \leftarrow QA/2$. In any case, print QA, a factor of N.

Some remarks are in order.

1. The algorithm terminates in step 1 if and only if N is a perfect square.

2. We have not discussed the queue structure in depth, but the algorithm will terminate if the QUEUE overflows. For virtually all successful factorizations, a QUEUE size of 50 is adequate.

3. The algorithm always fails if N is of the form $m^2 + 1$. In this case, we compute $QA = QB = 1$ and $PA = PB = m$. In step 2b, the pair $(1, m)$ is placed in the QUEUE. Then $R = 1$ and the algorithm fails in step 2c. Such N are rare, and in any case very little time is wasted so we do not make a special test for $QB = 1$ in step 1.

4. If the algorithm fails in step 2c, then we have gone through the entire principal period of quadratic forms of discriminant $4N$ without finding a proper square form.

5. The arithmetic of steps 2, 4, and 5 involves only positive integers less than $2\sqrt{N}$. Numbers as large as N only occur in steps 1 and 3. The odd numbered steps are executed only once.

6. If N is a prime number, then SQUFOF will fail when the QUEUE overflows. Hence, before running SQUFOF one should be certain that N is composite.

7. Step 4 will be executed approximately half as many times as step 2.

8. In steps 2b and 2c, it almost always happens that QB and QA exceed L. Also, QA is almost never a square in step 2c. Thus, the time spent inserting pairs into the QUEUE and searching for them in it is negligible compared to the total running time for step 2.

9. Once step 3 is reached, the algorithm cannot fail.

3.4 Sufficient List

Some implementations of SQUFOF do not use the previously described queue structure. Instead, when a form $(*, *, c)$ is discovered with $|c| < L$ when c is even, or

with $|c| < L/2$ when c is odd, then $|c|$ is put into an ordered list. Then any square form $(*, *, c^2)$ is skipped if $|c|$ is found to be in the list. This "sufficient list" is simpler, though some proper square forms may be skipped. For the running time analysis we will assume that the queue, and not the list, is used.

3.5 Binary Quadratic Forms Description

In [4], Cohen presents another version of SQUFOF entirely in the language of binary quadratic forms. It reduces to the continued fraction version of SQUFOF whenever $N \equiv 2$ or 3 mod 4. Whenever $N \equiv 1 \bmod 4$ the algorithm defines $\Delta = N$ and works with this fundamental discriminant of binary quadratic forms. Although it is slower than the previous algorithm when $N \equiv 1 \bmod 4$, because each iteration of ρ requires several divisions, the methods that we use to analyze the complexity apply.

4. SQUFOF Running Time Complexity

As we have seen, once SQUFOF finds a square form F_n, it will find an ambiguous form at about $n/2$ forms away from $F_n^{-1/2}$. So we take the number of forms examined before finding a proper square form to be a fair measure of the running time.

We have seen in Chapter 3 that SQUFOF generates several sequences depending on N. It looks for numbers with certain properties (proper squares). The complexity analysis is a heuristic argument based on several assumptions. Most of these assumptions say that these sequences of integers behave like random sequences of numbers of the same approximate size. Our first assumption, however, is not of this type. It simplifies the analysis by permitting the use of theorems about fundamental discriminants. It almost certainly holds in the most common uses of SQUFOF.

Assumption 4.0.1. *We assume that N is a square-free positive integer with k distinct large odd prime divisors.*

Assuming that N is square-free implies that Δ defined by

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

is a fundamental discriminant. This allows us to use many results from the theory of binary quadratic forms. Recall that if we use the continued fraction version of SQUFOF described in Sections 3.1 and 3.3, then any $N \equiv 1 \bmod 4$ will be multiplied by 2 at once. The $N \equiv 1 \bmod 4$ case here implies that we are using Cohen's version of Section 3.5. We will consider non-square-free N in future work.

In any case, SQUFOF is used mainly as an auxiliary algorithm in larger factorization algorithms and hence, SQUFOF will typically be used to factor integers of modest size with no small prime factors. Such integers are typically the product of a small number of distinct primes.

4.1 Counting Reduced Forms

There is an obvious correspondence between forms of discriminant Δ and solutions to the congruence

$$b^2 \equiv \Delta \bmod 4c\,. \tag{4.1}$$

Given an integer c, we will need to know the expected number of reduced forms $(*,*,c)$. It is clear that there will be no such forms if c is divisible by any inert prime, or if c is divisible by the square of a ramified prime. So we may assume that c is divisible by no inert primes and by ramified primes to at most the first power. Under these restrictions, the following three lemmas calculate the number of solutions to (4.1) from which the number of reduced forms will follow.

Lemma 4.1.1. *Let $0 < c < \sqrt{\Delta}/2$ and suppose c is divisible by no inert primes, by ramified primes to at most the first power, and by exactly l distinct split primes. Then there are 2^l reduced forms $(*,*,c)$ of discriminant Δ.*

Proof. Suppose $c = q_1^{e_1} \cdots q_l^{e_l} r_1 \cdots r_t$, where the r_i are ramified primes and the q_j are split primes. For each odd r_i, the congruence $b^2 \equiv \Delta \bmod r_i$ has only the trivial solution. For each odd q_j, the congruence $b^2 \equiv \Delta \bmod q_j$ has exactly two solutions. Since these two solutions are both nonsingular, they each lift to a unique solution of $b^2 \equiv \Delta \bmod q_j^{e_j}$.

If c is odd, then we must count the number of solutions to $b^2 \equiv \Delta \bmod 4$. Since $\Delta \equiv 0$ or $1 \bmod 4$, in either case we have two solutions. Finally, the Chinese Remainder Theorem gives 2^{l+1} solutions to (4.1).

Now suppose c is even. Either 2 is ramified (hence 2 exactly divides c) or 2 is split. If 2 is ramified then we must count the number of solutions to $b^2 \equiv \Delta \bmod 8$. Since $N \equiv 2$ or $3 \bmod 4$, we see that $\Delta \equiv 0$ or $4 \bmod 8$. There are two solutions to $b^2 \equiv 0 \bmod 8$ and two solutions to $b^2 \equiv 4 \bmod 8$, so once again the Chinese Remainder Theorem gives 2^{l+1} solutions to (4.1).

Finally, suppose 2 is a split prime and 2^e exactly divides c, where $e \geq 1$. We must count the number of solutions to $b^2 \equiv \Delta \bmod 2^{e+2}$. In this case $N \equiv 1 \bmod 8$.

The congruence $b^2 \equiv 1 \bmod 8$ has four solutions. It is not hard to show that these four solutions lift to exactly four solutions of $b^2 \equiv \Delta \bmod 2^{e+2}$ for any $e \geq 1$ (c.f Theorem 2.24 of [11].) For any of the other $l-1$ odd split primes, we will have two solutions to $b^2 \equiv \Delta \bmod q_j^{e_j}$ as before. Again, the Chinese Remainder Theorem gives $4 \cdot 2^{l-1} = 2^{l+1}$ solutions to (4.1).

Recall that a form (a,b,c) is reduced iff $\left|\sqrt{\Delta} - 2|c|\right| < b < \sqrt{\Delta}$. By hypothesis $0 < c < \sqrt{\Delta}/2$, hence $\left|\sqrt{\Delta} - 2|c|\right| = \sqrt{\Delta} - 2c$. The condition $\sqrt{\Delta} - 2c < b < \sqrt{\Delta}$ defines an interval of length $2c$. Now suppose $0 < b_1, b_2, \ldots, b_{2^{l+1}} < 4c$ are the 2^{l+1} solutions of (4.1) in the interval $(0, 4c)$. Note that half of these solutions must be in $(0, 2c)$ and half must be in $(2c, 4c)$. By translating these solutions to the interval $(\sqrt{\Delta} - 4c, \sqrt{\Delta})$, we see that the 2^l solutions in $(\sqrt{\Delta} - 2c, \sqrt{\Delta})$ lead to 2^l reduced forms $(*, *, c)$ of discriminant Δ. Finally, if (a,b,c) is a reduced form of discriminant Δ, then clearly b must be one of the translated b_i. This finishes the proof of the lemma. □

Lemma 4.1.2. *Let $\sqrt{\Delta} < c$. There are no reduced forms $(*, *, c)$ of discriminant Δ.*

Proof. A form (a,b,c) is reduced iff $\left|\sqrt{\Delta} - 2|c|\right| < b < \sqrt{\Delta}$. No b can satisfy this condition since $\sqrt{\Delta} < c$ implies that $\sqrt{\Delta} < 2c - \sqrt{\Delta} = \left|\sqrt{\Delta} - 2|c|\right|$. □

The previous two lemmas give us the exact number of reduced forms $(*, *, c)$ of discriminant Δ whenever $0 < c < \sqrt{\Delta}/2$ or $\sqrt{\Delta} < c$. We must settle for a probabilistic answer whenever $\sqrt{\Delta}/2 < c < \sqrt{\Delta}$. To this end, we make the following assumption regarding the distribution of quadratic residues in a complete system of residues modulo $4c$.

Assumption 4.1.3. *For each c such that $\sqrt{\Delta}/2 < c < \sqrt{\Delta}$, we assume that the 2^l solutions b to (4.1) in each half of the interval $(0, 4c)$ are randomly distributed.*

Lemma 4.1.4. *Let $\sqrt{\Delta}/2 < c < \sqrt{\Delta}$ and suppose c is divisible by no inert primes, by ramified primes to at most the first power, and by exactly l distinct split primes. Then the expected number of reduced forms $(*, *, c)$ of discriminant Δ is*

$$\frac{2^l\left(\sqrt{\Delta} - c\right)}{c}.$$

Proof. Since $\sqrt{\Delta}/2 < c < \sqrt{\Delta}$, the condition $\left|\sqrt{\Delta} - 2|c|\right| < b < \sqrt{\Delta}$ is equivalent to $2c - \sqrt{\Delta} < b < \sqrt{\Delta}$. This defines the interval $(2c - \sqrt{\Delta}, \sqrt{\Delta})$ of length $2\left(\sqrt{\Delta} - c\right)$. We translate the 2^{l+1} solutions of the congruence (4.1) in $(0, 4c)$ to the interval $(2c - \sqrt{\Delta}, 6c - \sqrt{\Delta})$. Half of these solutions will be in the interval $(2c - \sqrt{\Delta}, 4c - \sqrt{\Delta})$. By Assumption 4.1.3, the probability that a given solution in $(2c - \sqrt{\Delta}, 4c - \sqrt{\Delta})$ is actually in $(2c - \sqrt{\Delta}, \sqrt{\Delta})$ is assumed to be $2(\sqrt{\Delta} - c)/2c = (\sqrt{\Delta} - c)/c$. Thus the expected number of solutions that lie in $(2c - \sqrt{\Delta}, \sqrt{\Delta})$ is $2^l\left(\sqrt{\Delta} - c\right)/c$. As before, the number of reduced forms $(*, *, c)$ of discriminant Δ is equal to the number of solutions b to the congruence (4.1) such that $\left|\sqrt{\Delta} - 2c\right| < b < \sqrt{\Delta}$, and the lemma is proved. □

Note that if (a, b, c) is a reduced form of discriminant Δ, then so is $(-a, b, -c)$, so the previous three lemmas tell us how many forms $(*, *, -c)$ to expect for $c > 0$. For $c > 0$ we let Y_c be the number of forms (a', b', c') of discriminant Δ with $|c'| = c$. We will not compute this quantity for every possible value of c. Instead we compute $E[Y_c]$, the *expected* value of Y_c. The previous three lemmas can be used to compute this quantity once we make the following assumption.

Assumption 4.1.5. *Let p be a prime that is not ramified and suppose that $p|c$ for some $0 < c < \sqrt{\Delta}$. Then probability that p is split is $1/2$.*

This assumption is reasonable in light of the fact that the density of split primes is $1/2$ by the Chebotarev Density Theorem.

Lemma 4.1.6. *Suppose $c > 0$ is an integer divisible by ramified primes to at most the first power, and let Y_c be the number of reduced forms $(*, *, c')$ of discriminant Δ with $|c'| = c$. Then*

$$E[Y_c] = \begin{cases} 2 & \text{if } 0 < c < \sqrt{\Delta}/2 \ , \\ \frac{2\left(\sqrt{\Delta}-c\right)}{c} & \text{if } \sqrt{\Delta}/2 < c < \sqrt{\Delta} \ , \\ 0 & \text{if } \sqrt{\Delta} < c \ . \end{cases} \tag{4.2}$$

Proof. First suppose $0 < c < \sqrt{\Delta}/2$ and that c is divisible by l non-ramified primes. By assumption we take the probability that c is divisible by no inert prime to be 2^{-l}. Lemma 4.1.1 says that if c is divisible by no inert primes, by ramified primes to at most the first power, and by exactly l split primes, then there will be 2^l reduced forms $(*, *, c)$ of discriminant Δ. So we have

$$E[Y_c] = 2\left(2^{-l} \cdot 2^l + (1 - 2^{-l}) \cdot 0\right) = 2 \ ,$$

where we multiply by two since (a, b, c) is a reduced form of discriminant Δ iff $(-a, b, -c)$ is a reduced form of discriminant Δ.

Now suppose that $\sqrt{\Delta}/2 < c < \sqrt{\Delta}$, and that c is divisible by l non-ramified primes. Again, the probability that no inert prime divides c is taken to be 2^{-l}. Lemma 4.1.4 implies that if c is divisible by no inert primes, by ramified primes to at most the first power, and by exactly l split primes, then we expect $2^l(\sqrt{\Delta} - c)/c$ reduced forms $(*, *, c)$ of discriminant Δ. So we have

$$E[Y_c] = 2\left(2^{-l} \cdot \frac{2^l\left(\sqrt{\Delta} - c\right)}{c} + (1 - 2^{-l}) \cdot 0\right) = \frac{2\left(\sqrt{\Delta} - c\right)}{c} \ .$$

Finally, suppose $\sqrt{\Delta} < c$. Lemma 4.1.2 implies that there are no reduced forms $(*, *, c)$ of discriminant Δ, hence $E[Y_c] = 0$. □

4.2 Successive Square Forms

We now use the results of the previous section to compute the expected index-difference between successive square forms. Using similar techniques, we will count

both the expected number of reduced forms and reduced square forms on the principal cycle. Thinking of SQUFOF's search for a square form as a random walk on the principal cycle, the probability that SQUFOF finds a square at any given step is the ratio of these two counts. Finally, the expected number of steps between successive square forms is the reciprocal of this ratio.

Let C be the group of equivalence classes of binary quadratic forms of discriminant Δ. Recall that this group is isomorphic to the narrow class group of $\mathbb{Q}(\sqrt{\Delta})$, hence $|C| = h^+$, the narrow class number of $\mathbb{Q}(\sqrt{\Delta})$. Let G be the group of genera of forms of discriminant Δ. There is a surjective group homomorphism $\phi : C \to G$ taking an equivalence class to its genus, which we identify with its corresponding assigned value. The kernel of this homomorphism is the set of classes in the principal genus. The first group isomorphism theorem implies that $C/\ker\phi \cong G$, hence $|\ker\phi| = h^+/|G|$. It remains to compute the value of $|G|$.

When $N \equiv 1 \bmod 4$, $\Delta = N$ has k generic characters, one for each prime dividing N. If $N \equiv 2$ or $3 \bmod 4$, then $\Delta = 4N$ and there are $k+1$ generic characters. Let κ be the number of generic characters associated with the discriminant Δ. Since the number of genera is equal to one half the possible assigned values, we see that $|G| = 2^{\kappa-1}$. Finally we see that the number of classes in the principal genus is $h^+/2^{\kappa-1}$.

4.2.1 Number of Reduced Forms on the Principal Cycle

Let $c > 0$, X_c be the number of reduced forms $(*, *, c')$ of discriminant Δ with $|c'| = c$ on the principal cycle, and X be the total number of reduced forms with discriminant Δ on the principal cycle. Then $X = \sum_{0<c} X_c$. We have seen (Lemma 4.1.2) that if $(*, *, c)$ is a reduced form, then $0 < |c| < \sqrt{\Delta}$, so

$$X = \sum_{c=1}^{\sqrt{\Delta}} X_c \, . \tag{4.3}$$

We will compute $E[X]$, the expected number of reduced forms on the principal cycle,

$$E[X] = \sum_{c=1}^{\sqrt{\Delta}} E[X_c] \ . \tag{4.4}$$

We must now make a few observations about the distribution of forms among the the h^+ cycles. First observe that since the principal cycle is ambiguous, a reduced form (a, b, c) (non-ambiguous) will be on the principal cycle iff its associate (c, b, a) is on the principal cycle. But this means that (a, b, c) is on the principal cycle iff $\rho^{-1}(c, b, a) = (a', b', c)$ is on the principal cycle. Existence of the reduced forms (a, b, c), (a', b', c) implies the existence of the reduced forms $(-a, b, -c)$, $(-a', b', -c)$. These four forms will be collectively referred to as the quartet of forms associated with the form (a, b, c).

Suppose that one of the κ generic characters χ associated to Δ is such that $\chi(-1) = -1$. Then the forms (a, b, c), (a', b', c) are on the principal cycle iff the forms $(-a, b, -c)$, $(-a', b', -c)$ are *not* on the principal cycle. This means that for a given $c > 0$, at most two forms from each quartet can be on the principal cycle. This leads us to make the following assumption.

Assumption 4.2.1. *Suppose that there is some generic character χ associated with Δ such that $\chi(-1) = -1$. For each quartet of forms $(*, *, c')$ with $|c'| = c$, at most two forms may be on the principal cycle, and we assume that the probability that these two forms are on the principal cycle is $1/h^+$.*

Let Z be the random variable defined by

$$Z = \begin{cases} 1 & \text{with probability } \frac{1}{h^+} \ , \\ 0 & \text{with probability } 1 - \frac{1}{h^+} \ . \end{cases} \tag{4.5}$$

Then we have

$$X_c = \sum_{i=1}^{Y_c/4} 2Z \ . \tag{4.6}$$

Note that whether or not a given reduced form $(*,*,c)$ of discriminant Δ is on the principal cycle is independent of the number of forms $(*,*,c)$ of discriminant Δ. Hence Wald's equation (see [6]) implies that

$$E[X_c] = E\left[\sum_{i=1}^{Y_c/4} 2Z\right] = E[Y_c/4]\,E[2Z] = E[Y_c]/2h^+ \,. \tag{4.7}$$

Since Lemma 4.1.6 gives us an expression for $E[Y_c]$ when $0 < c < \sqrt{\Delta}$, we can now compute $E[X]$.

Now suppose that $\chi(-1) = 1$ for all generic characters χ associated to Δ. Then (a,b,c) is on the principal cycle iff its entire quartet is on the principal cycle. We now make the following assumption.

Assumption 4.2.2. *Suppose that $\chi(-1) = 1$ for all generic characters χ associated with Δ. Then either the quartet associated with (a,b,c) is on the principal cycle or not, and we assume that the quartet is on the principal cycle with probability $1/h^+$.*

In this case we have

$$X_c = \sum_{i=1}^{Y_c/4} 4Z \,, \tag{4.8}$$

and Wald's equation implies that

$$E[X_c] = E\left[\sum_{i=1}^{Y_c/4} 4Z\right] = E[Y_c/4]\,E[4Z] = E[Y_c]/h^+ \,.$$

In summary $E[X_c] = \nu E[Y_c]/h^+$, where

$$\nu = \begin{cases} \frac{1}{2} & \text{if } \chi(-1) = -1 \text{ for some } \chi \,, \\ 1 & \text{if } \chi(-1) = 1 \text{ for all } \chi \,. \end{cases} \tag{4.9}$$

If $N \equiv 1$ or $2 \bmod 4$ then we cannot know which value to use for ν, so we make the following assumption and calculate the expected value of ν.

Assumption 4.2.3. *Let χ be any generic character associated with Δ. We assume that $\chi(-1) = 1$ with probability $1/2$.*

Since there are κ generic characters, the probability that all take the value 1 at -1 is $2^{-\kappa}$. Hence

$$E[\nu] = \frac{1}{2}\left(1 - 2^{-\kappa}\right) + 2^{-\kappa} = \frac{2^{\kappa}+1}{2^{\kappa+1}}\ , \tag{4.10}$$

In this case we take $E[X_c]$ to be

$$E[X_c] = E[\nu]E[Y_c]/h^+ = \frac{(2^{\kappa}+1)E[Y_c]}{2^{\kappa+1}h^+}\ . \tag{4.11}$$

If $N \equiv 3 \bmod 4$, then some prime dividing N must be congruent to 3 modulo 4. In this case we take $\nu = 1/2$ and so

$$E[X_c] = E[Y_c]/2h^+. \tag{4.12}$$

In any case, we can now calculate $E[X]$.

Proposition 4.2.4. *The expected number of reduced forms of discriminant Δ on the principal cycle is*

$$E[X] \sim \begin{cases} \dfrac{\left(2^k+1\right)\sqrt{N}\log 2}{2^k h^+} & \text{if } N \equiv 1 \bmod 4\ , \\ \dfrac{3\left(2^{k+1}+1\right)\sqrt{N}\log 2}{2^{k+2}h^+} & \text{if } N \equiv 2 \bmod 4\ , \\ \dfrac{3\sqrt{N}\log 2}{2h^+} & \text{if } N \equiv 3 \bmod 4\ . \end{cases} \tag{4.13}$$

Proof. We assume that the odd prime divisors p_i of N (all of which are ramified) are so large that the probability that c is divisible by p_i^2 is negligibly small. This means that we shall use the results of Lemma 4.1.6 for all values of c, except when 2 is ramified ($N \equiv 2$ or $3 \bmod 4$.) When 2 is ramified, we will use $E[X_c] = 0$ for any c divisible by 4.

Note that to get the result in the case of $N \equiv 2 \bmod 4$, we may multiply the result in the case of $N \equiv 3 \bmod 4$ by $\left(2^{\kappa}+1\right)/2^{\kappa} = \left(2^{k+1}+1\right)/2^{k+1}$, since the only difference is that we replace $1/2$ with $E[\nu]$.

Case 1: ($N \equiv 1 \bmod 4$) In this case $\Delta = N$.

$$\begin{aligned}
E[X] &= \sum_{c=1}^{\sqrt{\Delta}} E[X_c] \\
&= \sum_{c=1}^{\sqrt{N}} \frac{\left(2^k+1\right) E[Y_c]}{2^{k+1}h^+} \\
&\qquad \text{(using Equation (4.11))} \\
&= \frac{2^k+1}{2^{k+1}h^+} \sum_{c=1}^{\sqrt{N}} E[Y_c] \\
&= \frac{2^k+1}{2^{k+1}h^+} \left[\sum_{c=1}^{\sqrt{N}/2} 2 \; + \sum_{c=\sqrt{N}/2}^{\sqrt{N}} \frac{2\left(\sqrt{N}-c\right)}{c} \right] \\
&\qquad \text{(by Lemma 4.1.6)} \\
&= \frac{\left(2^k+1\right)\sqrt{N}}{2^k h^+} \sum_{c=\sqrt{N}/2}^{\sqrt{N}} \frac{1}{c} \\
&= \frac{\left(2^k+1\right)\sqrt{N}}{2^k h^+} \left[\log\sqrt{N} - \log\left(\sqrt{N}/2\right)\right] \\
&\quad + O(1/h^+) \\
&\qquad \text{(using Lemma 5.1.2)} \\
&= \frac{\left(2^k+1\right)\sqrt{N}\log 2}{2^k h^+} + O(1)\,,
\end{aligned}$$

hence

$$E[X] \sim \frac{\left(2^k+1\right)\sqrt{N}\log 2}{2^k h^+}\,.$$

Case 2: ($N \equiv 3 \bmod 4$) In this case $\Delta = 4N$, and 2 is a ramified prime.

$$\begin{aligned}
E[X] &= \sum_{c=1}^{\sqrt{\Delta}} E[X_c] \\
&= \sum_{c=1}^{2\sqrt{N}} E[Y_c]/2h^+ \; - \sum_{c=1}^{\sqrt{N}/2} E[Y_{4c}]/2h^+ \\
&\qquad \text{(using Equation (4.7))}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2h^+}\left[\sum_{c=1}^{2\sqrt{N}} E[Y_c] \;-\; \sum_{c=1}^{\sqrt{N}/2} E[Y_{4c}]\right] \\
&= \frac{1}{2h^+}\left[\sum_{c=1}^{\sqrt{N}} 2 \;+\; \sum_{c=\sqrt{N}}^{2\sqrt{N}} \frac{2\left(2\sqrt{N}-c\right)}{c}\right. \\
&\qquad\qquad \left. -\sum_{c=1}^{\sqrt{N}/4} 2 \;-\; \sum_{c=\sqrt{N}/4}^{\sqrt{N}/2} \frac{2\left(2\sqrt{N}-4c\right)}{4c}\right] \\
&\qquad\qquad \text{(by Lemma 4.1.6)} \\
&= \frac{1}{2h^+}\left[4\sqrt{N}\sum_{c=\sqrt{N}}^{2\sqrt{N}} \frac{1}{c} \;-\sqrt{N}\sum_{c=\sqrt{N}/4}^{\sqrt{N}/2} \frac{1}{c}\right] \\
&= \frac{\sqrt{N}}{2h^+}\left[4\left(\log 2\sqrt{N} - \log\sqrt{N}\right)\right. \\
&\qquad\qquad \left. -\;\left(\log\left(\sqrt{N}/2\right) - \log\left(\sqrt{N}/4\right)\right)\right] \;+\; O(1/h^+) \\
&\qquad\qquad \text{(using Lemma 5.1.2)} \\
&= \frac{3\sqrt{N}\log 2}{2h^+} \;+\; O(1)\,,
\end{aligned}
$$

hence

$$E[X] \sim \frac{3\sqrt{N}\log 2}{2h^+}\,.$$

□

4.2.2 Number of Square Forms on the Principal Cycle

We can use the same methods used in the previous section to count X_{sq}, the number of reduced square forms $(*, *, c^2)$ on the principal cycle. As before, we will actually compute $E[X_{sq}]$, the expected number of reduced square forms on the principal cycle. Here we begin with $X_{sq} = \sum X_{c^2}/2$, where we divide by two since square

forms must have a positive right-end coefficient and exactly half of the X_{c^2} forms will satisfy this condition. Lemma 4.1.2 implies that

$$X_{sq} = \sum_{c=1}^{\Delta^{1/4}} X_{c^2}/2 \ , \tag{4.14}$$

hence,

$$E[X_{sq}] = \sum_{c=1}^{\Delta^{1/4}} E[X_{c^2}]/2 \ . \tag{4.15}$$

As before, for a given $c > 0$ there are Y_{c^2} reduced forms (a, b, c') of discriminant Δ with $|c'| = c^2$. Also, for each non-ambiguous form (a, b, c^2) we have the associated quartet of forms: (a, b, c^2), $\rho^{-1}(c^2, b, a) = (a', b', c^2)$, $(-a, b, -c^2)$, and $(-a', b', -c^2)$. Let Z_{sq} be the random variable defined by

$$Z_{sq} = \begin{cases} 1 & \text{with probability } \frac{2^{\kappa-1}}{h^+} \ , \\ 0 & \text{with probability } 1 - \frac{2^{\kappa-1}}{h^+} \ , \end{cases} \tag{4.16}$$

where κ is the number of generic characters of Δ. We make the following assumption.

Assumption 4.2.5. *We assume that a square form lies on the principal cycle (one of the $h^+/2^{\kappa-1}$ cycles in the principal genus) with probability $2^{\kappa-1}/h^+$.*

Replacing c with c^2 and Z with Z_{sq} in the calculation of $E[X_c]$ gives us the calculation for $E[X_{c^2}]$.

$$E[X_{c^2}] = \begin{cases} \dfrac{2^\kappa + 1}{4h^+} \, E[Y_{c^2}] & \text{if } N \equiv 1 \text{ or } 2 \bmod 4, \\ \\ \dfrac{2^{\kappa-2}}{h^+} \, E[Y_{c^2}] & \text{if } N \equiv 3 \bmod 4. \end{cases}$$

Since Lemma 4.1.6 gives us an expression for $E[Y_{c^2}]$ when $0 < c < \Delta^{1/4}$, we can now compute $E[X_{sq}]$.

Proposition 4.2.6. *The expected number of reduced square forms of discriminant Δ on the principal cycle is*

$$E[X_{sq}] \sim \begin{cases} \dfrac{\left(2^k+1\right)\left(\sqrt{2}-1\right)\sqrt[4]{N}}{2h^+} & \text{if } N \equiv 1 \bmod 4\ , \\ \dfrac{\left(2^{k+1}+1\right)\left(2-\sqrt{2}\right)\sqrt[4]{N}}{4h^+} & \text{if } N \equiv 2 \bmod 4\ , \\ \dfrac{2^k\left(2-\sqrt{2}\right)\sqrt[4]{N}}{2h^+} & \text{if } N \equiv 3 \bmod 4\ . \end{cases} \tag{4.17}$$

Proof. As in the proof of Proposition 4.2.4, we assume that the odd prime divisors p_i of N are so large that the probability that c^2 is divisible by p_i^2 is negligibly small. So we shall once again use the results of Lemma 4.1.6 for all values of c^2, except when 2 is ramified. When 2 is ramified, $2|c^2$ implies that $4|c^2$, and hence $E[X_{c^2}] = 0$. Also we can easily obtain the result for $N \equiv 2 \bmod 4$ once we have the result for $N \equiv 3 \bmod 4$ as in Proposition 4.2.4.

Case 1: ($N \equiv 1 \bmod 4$) In this case $\Delta = N$.

$$\begin{aligned} E[X_{sq}] &= \sum_{c=1}^{\sqrt[4]{\Delta}} E[X_{c^2}]/2 \\ &= \sum_{c=1}^{\sqrt[4]{N}} \frac{\left(2^\kappa+1\right) E[Y_{c^2}]}{8h^+} \\ &\qquad \text{(by Equation 4.2.2)} \\ &= \frac{2^\kappa+1}{8h^+} \sum_{c=1}^{\sqrt[4]{N}} E[Y_{c^2}] \\ &= \frac{2^\kappa+1}{8h^+} \left[\sum_{c=1}^{\sqrt[4]{N}/\sqrt{2}} 2 \ + \sum_{c=\sqrt[4]{N}/\sqrt{2}}^{\sqrt[4]{N}} \frac{2\left(\sqrt{N}-c^2\right)}{c^2} \right] \\ &\qquad \text{(by Lemma 4.1.6)} \\ &= \frac{2^\kappa+1}{4h^+} \left[\left(\sqrt{2}-1\right)\sqrt[4]{N} \ + \ \sqrt{N} \sum_{c=\sqrt[4]{N}/\sqrt{2}}^{\sqrt[4]{N}} \frac{1}{c^2} \right] \end{aligned}$$

$$\sim \frac{2^\kappa+1}{4h^+}\left[\left(\sqrt{2}-1\right)\sqrt[4]{N} + \sqrt{N}\left(\frac{\sqrt{2}}{\sqrt[4]{N}}-\frac{1}{\sqrt[4]{N}}\right)\right]$$

(by Lemma (5.1.3))

$$= \frac{\left(2^\kappa+1\right)\left(\sqrt{2}-1\right)\sqrt[4]{N}}{2h^+}$$

When $N \equiv 1 \bmod 4$, we have $\kappa = k$ generic characters, one for each prime divisor of N. Thus

$$E[X_{sq}] \sim \frac{\left(2^k+1\right)\left(\sqrt{2}-1\right)\sqrt[4]{N}}{2h^+}\,. \tag{4.18}$$

Case 2: ($N \equiv 3 \bmod 4$) In this case $\Delta = 4N$.

$$E[X_{sq}] = \sum_{c=1}^{\sqrt[4]{\Delta}} E[X_{c^2}]/2$$

$$= \sum_{c=1}^{\sqrt{2}\sqrt[4]{N}} \frac{2^{\kappa-2}E[Y_{c^2}]}{2h^+} - \sum_{c=1}^{\sqrt[4]{N}/\sqrt{2}} \frac{2^{\kappa-2}E[Y_{4c^2}]}{2h^+}$$

(by Equation 4.2.2)

$$= \frac{2^\kappa}{8h^+}\left[\sum_{c=1}^{\sqrt{2}\sqrt[4]{N}} E[Y_{c^2}] \;-\; \sum_{c=1}^{\sqrt[4]{N}/\sqrt{2}} E[Y_{4c^2}]\right]$$

$$= \frac{2^\kappa}{8h^+}\left[\sum_{c=1}^{\sqrt[4]{N}} 2 \;+ \sum_{c=\sqrt[4]{N}}^{\sqrt{2}\sqrt[4]{N}} \frac{2\left(2\sqrt{N}-c^2\right)}{c^2} - \sum_{c=1}^{\sqrt[4]{N}/2} 2 \;- \sum_{c=\sqrt[4]{N}/2}^{\sqrt[4]{N}/\sqrt{2}} \frac{2\left(2\sqrt{N}-4c^2\right)}{4c^2}\right]$$

(by Lemma 4.1.6)

$$= \frac{2^\kappa}{4h^+}\left[\left(2-\sqrt{2}\right)\sqrt[4]{N} \;+\; 2\sqrt{N}\sum_{c=N^{1/4}}^{\sqrt{2}\sqrt[4]{N}} \frac{1}{c^2}\right.$$

$$
\begin{aligned}
&\quad - \frac{2-\sqrt{2}}{2}\sqrt[4]{N} \; - \; \frac{\sqrt{N}}{2} \sum_{c=\sqrt[4]{N}/2}^{\sqrt[4]{N}/\sqrt{2}} \frac{1}{c^2} \Bigg] \\
&\sim \frac{2^\kappa}{4h^+} \left[\frac{2-\sqrt{2}}{2}\sqrt[4]{N} \right. \\
&\qquad + \; 2\sqrt{N}\left(\frac{1}{\sqrt[4]{N}} - \frac{1}{\sqrt{2}\sqrt[4]{N}}\right) \\
&\qquad \left. - \frac{\sqrt{N}}{2}\left(\frac{2}{\sqrt[4]{N}} - \frac{\sqrt{2}}{\sqrt[4]{N}}\right)\right] \\
&\qquad\qquad \text{(by Lemma 5.1.3)} \\
&= \frac{2^\kappa \left(2-\sqrt{2}\right)\sqrt[4]{N}}{4h^+}
\end{aligned}
$$

In this case $\kappa = k+1$, thus

$$E[X_{sq}] \sim \frac{2^k \left(2-\sqrt{2}\right)\sqrt[4]{N}}{2h^+} \; . \tag{4.19}$$

□

4.2.3 Expected Index-Difference between Successive Square Forms

We can use Propositions 4.2.4 and 4.2.6 to derived a formula for the expected index-difference between successive square forms if we make the following assumptions.

Assumption 4.2.7. *We model SQUFOF's search for a square form on the principal cycle as a random walk between the non-square forms and square forms of the principal cycle.*

We must now calculate the probability that a given form on the principal cycle is actually a square form. There are X_{sq} square forms among the X forms on the principal cycle, so we would like to compute $E[X_{sq}/X]$. To do this, we make the following assumption.

Assumption 4.2.8. *The probability that a given form on the principal cycle is a square form is taken to be $E[X_{sq}]/E[X]$.*

Thus $E[X]/E[X_{sq}]$ is the expected number of forms between any two successive square forms. The following Corollary gives the asymptotic behavior of $E[D]$.

Corollary 4.2.9. *Let D be the index-difference between successive square forms on the principal cycle. Then*

$$E[D] \sim \begin{cases} \dfrac{\left(\sqrt{2}+1\right)\sqrt[4]{N}\log 2}{2^{k-1}} & \text{if } N \equiv 1 \bmod 4\ , \\ \\ \dfrac{3\left(\sqrt{2}+2\right)\sqrt[4]{N}\log 2}{2^{k+1}} & \text{if } N \equiv 2 \text{ or } 3 \bmod 4\ . \end{cases} \tag{4.20}$$

Proof. We prove the case $N \equiv 1 \bmod 4$. The cases $N \equiv 2$ and $3 \bmod 4$ are proved in the same way.

Case 1: ($N \equiv 1 \bmod 4$) Proposition 4.2.4 implies that

$$E[X] \sim \frac{\left(2^k+1\right)\sqrt{N}\log 2}{2^k h^+}\ ,$$

and Proposition 4.2.6 implies that

$$E[X_{sq}] \sim \frac{\left(2^k+1\right)\left(\sqrt{2}-1\right)\sqrt[4]{N}}{2h^+}\ .$$

Thus

$$E[D] \sim \frac{\left(\left(2^k+1\right)\sqrt{N}\log 2\right)\Big/ 2^k h^+}{\left(\left(2^k+1\right)\left(\sqrt{2}-1\right)\sqrt[4]{N}\right)\Big/ 2h^+} = \frac{\left(\sqrt{2}+1\right)\sqrt[4]{N}\log 2}{2^{k-1}}\ .$$

□

4.3 Proper Square Forms

In this section we will derive the probability that a square form is a proper square form. The reciprocal of this probability gives the expected number of square forms we must examine before we successfully factor N. Recall that an proper square form is one that leads to an ambiguous form, which in turn leads to a nontrivial divisor of N. We make the following assumption about the appearance of proper squares.

Assumption 4.3.1. *Suppose SQUFOF has found a square form and let* (a, ab, c) *be one of the* 2^κ *reduced ambiguous forms of discriminant* Δ*. The square form will lead to* (a, ab, c) *with probability* $2^{-\kappa}$*.*

Proposition 4.3.2. *The probability that a square form is a proper square form is*

$$\frac{2^k - 2}{2^k} \,. \tag{4.21}$$

Proof. As we have seen, a square form leads to an ambiguous from (a, ab, c), hence a factor of Δ. There are as many ambiguous classes as there are genera, and this latter quantity is known to be $2^{\kappa-1}$. There are two ambiguous forms per ambiguous class, hence there are 2^κ ambiguous forms. These forms are in bijective correspondence with the square-free divisors d of Δ with $|d| < \sqrt{\Delta}$.

Now suppose Δ has n small ramified primes (primes which we already know divide Δ) and k large ramified primes. Then $\kappa = k + n$ and there will be 2^{n+1} improper squares (one for each of the possible 2^{n+1} square-free divisors d of Δ divisible only by the small ramified primes and $|d| < \sqrt{\Delta}$.) Thus the probability that a given square for is proper is

$$\frac{2^{n+k} - 2^{n+1}}{2^{n+k}} = \frac{2^k - 2}{2^k} \,.$$

□

Corollary 4.3.3. *The expected number of square forms that SQUFOF must examine before finding a proper square form is*

$$\frac{2^k}{2^k - 2} \,. \tag{4.22}$$

4.4 The Running Time Complexity of SQUFOF

We now have everything we need to compute the asymptotic behavior of the expected number of forms SQUFOF must examine before finding a proper square form.

k	$E[W]/\sqrt[4]{N},\ N \equiv 1 \bmod 4$	$E[W]/\sqrt[4]{N},\ N \equiv 2 \text{ or } 3 \bmod 4$
2	1.6734	1.7749
3	0.5578	0.5916
4	0.2391	0.2536

Table 4.1
Estimates of $E[W]/\sqrt[4]{N}$ for $k = 2, 3, 4$.

Proposition 4.4.1. *Let W be the number of forms that SQUFOF must examine before finding a proper square form. Then*

$$E[W] \sim \begin{cases} \dfrac{2\left(\sqrt{2}+1\right)\sqrt[4]{N}\log 2}{2^k-2} & \text{if } N \equiv 1 \bmod 4\ , \\ \\ \dfrac{3\left(\sqrt{2}+2\right)\sqrt[4]{N}\log 2}{2\left(2^k-2\right)} & \text{if } N \equiv 2 \text{ or } 3 \bmod 4\ . \end{cases} \tag{4.23}$$

Proof. This is simply the product of (4.20) and (4.22). □

Table 4.1 lists the predicted values for $E[W]/\sqrt[4]{N}$ when N is a product of two, three, and four primes.

4.5 Expected Queue Size

Now that we have the expected number of forms that SQUFOF will examine before finding a proper square form, it is a simple matter to calculate the expected queue size. If $N \equiv 1 \bmod 4$, then $(*, *, c)$ will be enqueued if $|c| < \sqrt[4]{\Delta}$. There are $2\sqrt[4]{\Delta}$ integers c such that $|c| < \sqrt[4]{\Delta}$, of which only $3\sqrt[4]{\Delta}/2$ are such that $4 \nmid c$. There are $3\sqrt{\Delta}/2$ integers c such that $|c| < \sqrt{\Delta}$. Thus the probability is $1/\sqrt[4]{\Delta}$ that an integer c not divisible by 4 in $(-\sqrt{\Delta}, \sqrt{\Delta})$ such that c is in $(-\sqrt[4]{\Delta}, \sqrt[4]{\Delta})$.

Now assume that $N \equiv 2$ or $3 \bmod 4$. If a form $(*, *, c)$ is such that $|c| < \sqrt[4]{\Delta}$ when c is odd, or $|c/2| < \sqrt[4]{\Delta}$ when c is even, then SQUFOF will enqueue this

form, increasing the size of the queue by one. There are $2\sqrt[4]{\Delta}$ integers c such that $|c| < \sqrt[4]{\Delta}$, and only $3\sqrt[4]{\Delta}/2$ such that $4 \nmid c$ as well. Of this latter quantity, $\sqrt[4]{\Delta}$ of these c are odd, and so $2c$ satisfies $|c| = |2c/2| < \sqrt[4]{\Delta}$. So there are $5\sqrt[4]{\Delta}/2$ integers c such that $|c| < \sqrt[4]{\Delta}$ when c is odd, and $|c/2| < \sqrt[4]{\Delta}$ when c is even. Finally, there are $3\sqrt{\Delta}/2$ integers c with $|c| < \sqrt{\Delta}$ and $4 \nmid c$. Thus the probability that an integer c not divisible by 4 in $(-\sqrt{\Delta}, \sqrt{\Delta})$ such that c or $c/2$ is in $(-\sqrt[4]{\Delta}, \sqrt[4]{\Delta})$ is $\left(5\sqrt[4]{\Delta}/2\right) / \left(3\sqrt{\Delta}/2\right) = 5/\left(3\sqrt[4]{\Delta}\right)$. This leads us to the following assumption.

Assumption 4.5.1. *Suppose that the form $(*, *, c)$ is examined at the n^{th} step of SQUFOF's search for a proper square form. The probability that the form is enqueued is either $1/\sqrt[4]{\Delta}$ or $5/\left(3\sqrt[4]{\Delta}\right)$, depending on whether $N \equiv 1 \bmod 4$ or $N \equiv 2$ or $3 \bmod 4$, respectively.*

Proposition 4.5.2. *Let Q be the number of forms enqueued during the factorization of N. Then*

$$E[Q] \sim \begin{cases} \dfrac{2\left(\sqrt{2}+1\right)\log 2}{2^k - 2} & \text{if } N \equiv 1 \bmod 4\,, \\ \\ \dfrac{5\left(\sqrt{2}+1\right)\log 2}{2\left(2^k - 2\right)} & \text{if } N \equiv 2 \text{ or } 3 \bmod 4\,, \end{cases} \tag{4.24}$$

Proof. **Case 1:** ($N \equiv 1 \bmod 4$.) Since $\Delta = N$, we have

$$\begin{aligned} E[Q] &= E[W]/\sqrt[4]{N} \\ &= \left(\frac{2\left(\sqrt{2}+1\right)\sqrt[4]{N}\log 2}{2^k - 2}\right) \Big/ \sqrt[4]{N} \\ &= \frac{2\left(\sqrt{2}+1\right)\log 2}{2^k - 2}\,. \end{aligned}$$

Case 2: ($N \equiv 2$ or $3 \bmod 4$.) Since $\Delta = 4N$, we have

$$\begin{aligned} E[Q] &= (5E[W]) \,/\, (3\sqrt[4]{4N}) \\ &= \left(\frac{5 \cdot 3\left(\sqrt{2}+2\right)\sqrt[4]{N}\log 2}{2\left(2^k - 2\right)}\right) \Big/ \left(3\sqrt[4]{4N}\right) \\ &= \frac{5\left(\sqrt{2}+1\right)\log 2}{2\left(2^k - 2\right)} \end{aligned}$$

k	$E[Q],\ N \equiv 1 \bmod 4$	$E[Q],\ N \equiv 2$ or $3 \bmod 4$
2	1.6734	2.0918
3	0.5578	0.6973
4	0.2391	0.2988

Table 4.2
Estimates of $E[Q]$ for $k = 2, 3, 4$.

□

Table 4.2 lists the predicted values for $E[Q]$ when N is a product of two, three, and four primes.

5. The Effect of Multipliers

We now consider how multiplying N by small odd primes changes the running time of SQUFOF and the queue length. Our strategy will be similar to that of Chapter 4 in that we will compute $E[X]$ and $E[X_{sq}]$ for $p_1 p_2 \cdots p_n N$ for distinct small odd primes p_i.

5.1 Helpful Lemmas

The following three lemmas will be helpful in computing $E[X]$ and $E[X_{sq}]$. The notation $a \ll b$ will mean that b is much larger than a.

Lemma 5.1.1. *Let $0 \ll \Delta$ be a positive integer and suppose $p_1, \ldots, p_n$, for $n \geq 0$, are distinct small primes with $p_i \ll \Delta$. Then for $e \geq 1$ we have*

$$\sum_{\substack{c=1 \\ p_i^e \nmid c,\ i=1,\ldots,n}}^{\sqrt{\Delta}} 1 \quad \sim \quad \sqrt{\Delta} \prod_{i=1}^{n} \frac{p_i^e - 1}{p_i^e} \, .$$

Proof. When $n = 0$ the claim obviously holds. If $n = 1$ then

$$\begin{aligned} \sum_{\substack{c=1 \\ p_1^e \nmid c}}^{\sqrt{\Delta}} 1 &= \sum_{c=1}^{\sqrt{\Delta}} 1 \; - \sum_{c=1}^{\sqrt{\Delta}/p_1^e} 1 \\ &= \sqrt{\Delta} \; - \; \frac{\sqrt{\Delta}}{p_1^e} \\ &= \sqrt{\Delta} \prod_{i=1}^{1} \frac{p_i^e - 1}{p_i^e} \, . \end{aligned}$$

Now suppose the claim holds for $n-1$ primes $p_1, \ldots, p_{n-1}$ and consider

$$\sum_{\substack{c=1 \\ p_i^e \nmid c,\ i=1,\ldots,n}}^{\sqrt{\Delta}} 1 = \sum_{\substack{c=1 \\ p_i^e \nmid c,\ i=1,\ldots,n-1}}^{\sqrt{\Delta}} 1 \; - \sum_{\substack{c=1 \\ p_i^e \nmid c,\ i=1,\ldots,n-1}}^{\sqrt{\Delta}/p_n^e} 1$$

$$\sim \sqrt{\Delta} \prod_{i=1}^{n-1} \frac{p_i^e - 1}{p_i^e} \; - \; \frac{\sqrt{\Delta}}{p_n^e} \prod_{i=1}^{n-1} \frac{p_i^e - 1}{p_i^e}$$
$$= \sqrt{\Delta} \prod_{i=1}^{n} \frac{p_i^e - 1}{p_i^e} \, .$$

Thus the claim hold for all $n \geq 0$.

□

Lemma 5.1.2. *Let $0 \ll \Delta$ be a positive integer and suppose $p_1, \ldots, p_n$, for $n \geq 0$, are distinct small primes with $p_i \ll \Delta$. Then*

$$\sum_{\substack{c=\sqrt{\Delta}/2 \\ p_i^2 \nmid c,\, i=1,\ldots,n}}^{\sqrt{\Delta}} \frac{1}{c} \quad \sim \quad \log 2 \prod_{i=1}^{n} \frac{p_i^2 - 1}{p_i^2} \, .$$

Proof. We prove the lemma by induction on n. First suppose that $n = 0$. Then

$$\sum_{c=\sqrt{\Delta}/2}^{\sqrt{\Delta}} \frac{1}{c} \; = \; H_{\sqrt{\Delta}} - H_{\sqrt{\Delta}/2} \; \sim \; \log 2 \, .$$

For $n = 1$ we have

$$\sum_{\substack{c=\sqrt{\Delta}/2 \\ p_1^2 \nmid c}}^{\sqrt{\Delta}} \frac{1}{c} = \sum_{c=\sqrt{\Delta}/2}^{\sqrt{\Delta}} \frac{1}{c} \; - \sum_{c=\sqrt{\Delta}/2p_1^2}^{\sqrt{\Delta}/p_1^2} \frac{1}{p_1^2}$$
$$\sim \log 2 - \frac{1}{p_1^2} \sum_{\sqrt{\Delta}/2p_1^2}^{\sqrt{\Delta}/p_1^2} \frac{1}{c}$$
$$\sim \log 2 - \frac{1}{p_1^2} \; \log 2$$
$$= \log 2 \prod_{i=1}^{1} \frac{p_i^2 - 1}{p_i^2} \, .$$

Now suppose the claim holds for $n - 1$ primes $p_1, \ldots, p_{n-1}$ and consider

$$\sum_{\substack{c=\sqrt{\Delta}/2 \\ p_i^2 \nmid c,\, i=1,\ldots,n}}^{\sqrt{\Delta}} \frac{1}{c} = \sum_{\substack{c=\sqrt{\Delta}/2 \\ p_i^2 \nmid c,\, i=1,\ldots,n-1}}^{\sqrt{\Delta}} \frac{1}{c} \; - \sum_{\substack{c=\sqrt{\Delta}/2p_n^2 \\ p_i^2 \nmid c,\, i=1,\ldots,n-1}}^{\sqrt{\Delta}/p_n^2} \frac{1}{p_n^2 c}$$

$$\sim \log 2 \prod_{i=1}^{n-1} \frac{p_i^2-1}{p_i^2} \; - \; \frac{1}{p_n^2} \sum_{\substack{c=\sqrt{\Delta}/2p_n^2 \\ p_i^2 \nmid c,\ i=1,\ldots,n-1}}^{\sqrt{\Delta}/p_n^2} \frac{1}{c}$$

$$\sim \log 2 \prod_{i=1}^{n-1} \frac{p_i^2-1}{p_i^2} \; - \; \frac{1}{p_n^2} \; \log 2 \prod_{i=1}^{n-1} \frac{p_i^2-1}{p_i^2}$$

$$= \log 2 \prod_{i=1}^{n} \frac{p_i^2-1}{p_i^2} \, .$$

Thus the claim hold for all $n \geq 0$. □

Lemma 5.1.3. *Let $0 \ll \Delta$ be a positive integer and suppose $p_1, \ldots, p_n$, for $n \geq 0$, are distinct small primes with $p_i \ll \Delta$. Then*

$$\sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ p_i \nmid c,\ i=1,\ldots,n}}^{\sqrt[4]{\Delta}} \frac{1}{c^2} \quad \sim \quad \frac{\sqrt{2}-1}{\sqrt[4]{\Delta}} \prod_{i=1}^{n} \frac{p_i-1}{p_i} \, .$$

Proof. We prove the lemma by induction on n. First suppose that $n = 0$. Then

$$\sum_{c=\sqrt[4]{\Delta}/\sqrt{2}}^{\sqrt[4]{\Delta}} \frac{1}{c^2} \; \sim \; \frac{\sqrt{2}}{\sqrt[4]{\Delta}} - \frac{1}{\sqrt[4]{\Delta}} \; = \; \frac{\sqrt{2}-1}{\sqrt[4]{\Delta}} \, .$$

For $n = 1$ we have

$$\sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ p_1 \nmid c}}^{\sqrt[4]{\Delta}} \frac{1}{c^2} = \sum_{c=\sqrt[4]{\Delta}/\sqrt{2}}^{\sqrt[4]{\Delta}} \frac{1}{c^2} \; - \sum_{c=\sqrt[4]{\Delta}/p_1\sqrt{2}}^{\sqrt[4]{\Delta}/p_1} \frac{1}{p_1^2 c^2}$$

$$\sim \frac{\sqrt{2}-1}{\sqrt[4]{\Delta}} \; - \frac{1}{p_1^2} \sum_{c=\sqrt[4]{\Delta}/p_1\sqrt{2}}^{\sqrt[4]{\Delta}/p_1} \frac{1}{c^2}$$

$$\sim \frac{\sqrt{2}-1}{\sqrt[4]{\Delta}} \; - \frac{1}{p_1^2} \left(\frac{\sqrt{2}}{\sqrt[4]{\Delta}/p_1} - \frac{1}{\sqrt[4]{\Delta}/p_1} \right)$$

$$= \frac{\sqrt{2}-1}{\sqrt[4]{\Delta}} \; - \frac{1}{p_1} \; \frac{\sqrt{2}-1}{\sqrt[4]{\Delta}}$$

$$= \frac{\sqrt{2}-1}{\sqrt[4]{\Delta}} \; \prod_{i=1}^{1} \frac{p_i-1}{p_i} \, .$$

Now suppose the claim holds for $n-1$ primes $p_1, \ldots, p_{n-1}$ and consider

$$\sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ p_i \nmid c,\ i=1,\ldots,n}}^{\sqrt[4]{\Delta}} \frac{1}{c^2} = \sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ p_i \nmid c,\ i=1,\ldots,n-1}}^{\sqrt[4]{\Delta}} \frac{1}{c^2} \; - \sum_{\substack{c=\sqrt[4]{\Delta}/p_n\sqrt{2} \\ p_i \nmid c,\ i=1,\ldots,n-1}}^{\sqrt[4]{\Delta}/p_n} \frac{1}{p_n^2 c^2}$$

$$\sim \frac{\sqrt{2}-1}{\sqrt[4]{\Delta}} \prod_{i=1}^{n-1} \frac{p_i-1}{p_i} - \frac{1}{p_n^2} \sum_{\substack{c=\sqrt[4]{\Delta}/p_n\sqrt{2} \\ p_i\nmid c,\ i=1,\ldots,n-1}}^{\sqrt[4]{\Delta}/p_n} \frac{1}{c^2}$$

$$\sim \frac{\sqrt{2}-1}{\sqrt[4]{\Delta}} \prod_{i=1}^{n-1} \frac{p_i-1}{p_i} - \frac{1}{p_n^2} \frac{\sqrt{2}-1}{\sqrt[4]{\Delta}/p_n} \prod_{i=1}^{n-1} \frac{p_i-1}{p_i}$$

$$= \frac{\sqrt{2}-1}{\sqrt[4]{\Delta}} \prod_{i=1}^{n} \frac{p_i-1}{p_i} .$$

Thus the claim holds for all $n \geq 0$. □

Lemma 5.1.4. *Let $0 \ll \Delta$ be a positive integer and suppose $p_1, \ldots, p_n$, for $n \geq 0$, are distinct small primes with $p_i \ll \Delta$. Then*

$$\sum_{\substack{c=1 \\ p_i\nmid c,\ i=1,\ldots,n}}^{\sqrt[4]{\Delta}/\sqrt{2}} 1 - \sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ p_i\nmid c,\ i=1,\ldots,n}}^{\sqrt[4]{\Delta}} 1 \quad \sim \quad \sqrt[4]{\Delta}\left(\sqrt{2}-1\right) \prod_{i=1}^{n} \frac{p_i-1}{p_i} .$$

Proof. We prove the lemma by induction on n. First suppose that $n = 0$. Then

$$\sum_{c=1}^{\sqrt[4]{\Delta}/\sqrt{2}} 1 - \sum_{\sqrt[4]{\Delta}/\sqrt{2}}^{\sqrt[4]{\Delta}} 1 = \frac{\sqrt[4]{\Delta}}{\sqrt{2}} - \left(\sqrt[4]{\Delta} - \frac{\sqrt[4]{\Delta}}{\sqrt{2}}\right) = \sqrt[4]{\Delta}\left(\sqrt{2}-1\right) .$$

For $n = 1$ we have

$$\sum_{\substack{c=1 \\ p_1\nmid c}}^{\sqrt[4]{\Delta}/\sqrt{2}} 1 - \sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ p_1\nmid c}}^{\sqrt[4]{\Delta}} 1 = \left(\sum_{c=1}^{\sqrt[4]{\Delta}/\sqrt{2}} 1 - \sum_{c=1}^{\sqrt[4]{\Delta}/p_1\sqrt{2}} 1\right) - \left(\sum_{\sqrt[4]{\Delta}/\sqrt{2}}^{\sqrt[4]{\Delta}} 1 - \sum_{\sqrt[4]{\Delta}/p_1\sqrt{2}}^{\sqrt[4]{\Delta}/p_1} 1\right)$$

$$= \left(\sum_{c=1}^{\sqrt[4]{\Delta}/\sqrt{2}} 1 - \sum_{\sqrt[4]{\Delta}/\sqrt{2}}^{\sqrt[4]{\Delta}} 1\right) - \left(\sum_{c=1}^{\sqrt[4]{\Delta}/p_1\sqrt{2}} 1 - \sum_{\sqrt[4]{\Delta}/p_1\sqrt{2}}^{\sqrt[4]{\Delta}/p_1} 1\right)$$

$$= \sqrt[4]{\Delta}\left(\sqrt{2}-1\right) - \left[\frac{\sqrt[4]{\Delta}}{p_1\sqrt{2}} - \left(\frac{\sqrt[4]{\Delta}}{p_1} - \frac{\sqrt[4]{\Delta}}{p_1\sqrt{2}}\right)\right]$$

$$= \sqrt[4]{\Delta}\left(\sqrt{2}-1\right) \prod_{i=1}^{1} \frac{p_1-1}{p_1} .$$

Now suppose the claim holds for $n-1$ primes $p_1, \ldots, p_{n-1}$ and consider

$$\sum_{\substack{c=1 \\ p_i\nmid c,\ i=1,\ldots,n}}^{\sqrt[4]{\Delta}/\sqrt{2}} 1 - \sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ p_i\nmid c,\ i=1,\ldots,n}}^{\sqrt[4]{\Delta}} 1$$

$$
\begin{aligned}
&= \left(\sum_{\substack{c=1 \\ p_i \nmid c,\ i=1,\ldots,n-1}}^{\sqrt[4]{\Delta}/\sqrt{2}} 1 \; - \sum_{\substack{c=1 \\ p_i \nmid c,\ i=1,\ldots,n-1}}^{\sqrt[4]{\Delta}/p_n\sqrt{2}} 1 \right) - \left(\sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ p_i \nmid c,\ i=1,\ldots,n-1}}^{\sqrt[4]{\Delta}} 1 \; - \sum_{\substack{c=\sqrt[4]{\Delta}/p_n\sqrt{2} \\ p_i \nmid c,\ i=1,\ldots,n-1}}^{\sqrt[4]{\Delta}/p_n} 1 \right) \\
&= \left(\sum_{\substack{c=1 \\ p_i \nmid c,\ i=1,\ldots,n-1}}^{\sqrt[4]{\Delta}/\sqrt{2}} 1 \; - \sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ p_i \nmid c,\ i=1,\ldots,n-1}}^{\sqrt[4]{\Delta}} 1 \right) - \left(\sum_{\substack{c=1 \\ p_i \nmid c,\ i=1,\ldots,n-1}}^{\sqrt[4]{\Delta}/p_n\sqrt{2}} 1 \; - \sum_{\substack{c=\sqrt[4]{\Delta}/p_n\sqrt{2} \\ p_i \nmid c,\ i=1,\ldots,n-1}}^{\sqrt[4]{\Delta}/p_n} 1 \right) \\
&\sim \left[\sqrt[4]{\Delta} \left(\sqrt{2} - 1 \right) \prod_{i=1}^{n-1} \frac{p_i - 1}{p_i} \right] - \left[\frac{\sqrt[4]{\Delta}}{p_n} \left(\sqrt{2} - 1 \right) \prod_{i=1}^{n-1} \frac{p_i - 1}{p_i} \right] \\
&= \sqrt[4]{\Delta} \left(\sqrt{2} - 1 \right) \prod_{i=1}^{n} \frac{p_i - 1}{p_i} \, .
\end{aligned}
$$

Thus the claim holds for all $n \geq 0$. □

5.2 The Running Time with Multipliers

Proposition 5.2.1. *Let N be a square-free positive integer with k distinct large odd prime divisors and let $p_1, \ldots, p_n$ be n distinct small odd primes ($n \geq 0$) with $p_i \nmid N$ for all i. Define Δ by*

$$
\Delta = \begin{cases} p_1 \cdots p_n N & \text{if} \quad p_1 \cdots p_n N \equiv 1 \bmod 4 \, , \\ 4 p_1 \cdots p_n N & \text{if} \quad p_1 \cdots p_n N \equiv 2 \text{ or } 3 \bmod 4 \, . \end{cases}
$$

If X is the number of reduced forms on the principal cycle of discriminant Δ then

$$E[X] \sim \begin{cases} \dfrac{\left(2^{k+n}+1\right)\sqrt{N}\log 2}{2^{k+n}h^+}\ \prod_{i=1}^{n}\dfrac{p_i^2-1}{p_i^{3/2}} & \text{if } \Delta \equiv 1 \bmod 4 \text{ and } p_i \equiv 1 \bmod 4\ \forall i\ , \\ \dfrac{\sqrt{N}\log 2}{h^+}\ \prod_{i=1}^{n}\dfrac{p_i^2-1}{p_i^{3/2}} & \text{if } \Delta \equiv 1 \bmod 4 \text{ and } \exists p_i \equiv 3 \bmod 4\ , \\ \dfrac{3\left(2^{k+n+1}+1\right)\sqrt{N}\log 2}{2^{k+n+2}h^+}\ \prod_{i=1}^{n}\dfrac{p_i^2-1}{p_i^{3/2}} & \text{if } N \equiv 2 \bmod 4 \text{ and } p_i \equiv 1 \bmod 4\ \forall i\ , \\ \dfrac{3\sqrt{N}\log 2}{2h^+}\ \prod_{i=1}^{n}\dfrac{p_i^2-1}{p_i^{3/2}} & \text{otherwise.} \end{cases}$$

Proof. The proof of each case is similar to the corresponding proof in Proposition 4.2.4. The main difference is that we will need Lemma 5.1.2 to handle several small ramified primes.

Case 1: (Δ and $p_i \equiv 1 \bmod 4$ for $i = 1, 2, \ldots, n$.) Here $\Delta = p_1 \cdots p_n N$ and so the small ramified primes are $p_1, \ldots, p_n$.

$$\begin{aligned} E[X] &= \sum_{\substack{c=1 \\ p_i^2 \nmid c}}^{\sqrt{\Delta}} E[X_c] \\ &= \sum_{\substack{c=1 \\ p_i^2 \nmid c}}^{\sqrt{\Delta}} \frac{\left(2^\kappa+1\right)E[Y_c]}{2^{\kappa+1}h^+} \\ &= \frac{2^\kappa+1}{2^{\kappa+1}h^+} \sum_{\substack{c=1 \\ p_i^2 \nmid c}}^{\sqrt{\Delta}} E[Y_c] \\ &= \frac{2^\kappa+1}{2^{\kappa+1}h^+} \left[\sum_{\substack{c=1 \\ p_i^2 \nmid c}}^{\sqrt{\Delta}/2} 2 \ + \sum_{\substack{c=\sqrt{\Delta}/2 \\ p_i^2 \nmid c}}^{\sqrt{\Delta}} \frac{2\left(\sqrt{\Delta}-c\right)}{c} \right] \\ &= \frac{\left(2^\kappa+1\right)\sqrt{\Delta}}{2^\kappa h^+} \sum_{\substack{c=\sqrt{\Delta}/2 \\ p_i^2 \nmid c}}^{\sqrt{\Delta}} \frac{1}{c} \end{aligned}$$

$$\sim \frac{(2^\kappa+1)\sqrt{\Delta}\log 2}{2^\kappa h^+}\ \prod_{i=1}^{n}\frac{p_i^2-1}{p_i^2}\ .$$

Now $\kappa = k+n$ and $\Delta = p_1\cdots p_n N$, hence

$$E[X] \sim \frac{\left(2^{k+n}+1\right)\sqrt{N}\log 2}{2^{k+n}h^+}\ \prod_{i=1}^{n}\frac{p_i^2-1}{p_i^{3/2}}\ .$$

Case 2: ($\Delta \equiv 1 \bmod 4, \exists p_i \equiv 3 \bmod 4$.) In this case we multiply the result for the previous case by $2^\kappa/\left(2^\kappa+1\right)$, since we know that some prime equivalent to 3 mod 4 divides Δ. As in the previous case, $\Delta = p_1\cdots p_n$ and $\kappa = k+n$ so

$$\begin{aligned} E[X] &\sim \left(\frac{\left(2^{k+n}+1\right)\sqrt{N}\log 2}{2^{k+n}h^+}\ \prod_{i=1}^{n}\frac{p_i^2-1}{p_i^{3/2}}\right)\left(\frac{2^{k+n}}{2^{k+n}+1}\right) \\ &= \frac{\sqrt{N}\log 2}{h^+}\ \prod_{i=1}^{n}\frac{p_i^2-1}{p_i^{3/2}}\ . \end{aligned}$$

Case 3: ($N \equiv 2 \bmod 4, p_1 \equiv 1 \bmod 4$ for $i = 1, 2, \ldots, n$.) Here $\Delta = 4p_1\cdots p_n N$ and $\kappa = k+n+1$. So the small ramified primes are $2, p_1, \ldots, p_n$.

$$\begin{aligned} E[X] &= \sum_{\substack{c=1 \\ 4,p_i^2\nmid c}}^{\sqrt{\Delta}} E[X_c] \\ &= \sum_{\substack{c=1 \\ 4,p_i^2\nmid c}}^{\sqrt{\Delta}} \frac{(2^\kappa+1)\,E[Y_c]}{2^{\kappa+1}h^+} \\ &= \frac{2^\kappa+1}{2^{\kappa+1}h^+}\sum_{\substack{c=1 \\ 4,p_i^2\nmid c}}^{\sqrt{\Delta}} E[Y_c] \\ &= \frac{2^\kappa+1}{2^{\kappa+1}h^+}\left[\sum_{\substack{c=1 \\ 4,p_i^2\nmid c}}^{\sqrt{\Delta}/2} 2\ +\ \sum_{\substack{c=\sqrt{\Delta}/2 \\ p_i^2\nmid c}}^{\sqrt{\Delta}} \frac{2\left(\sqrt{\Delta}-c\right)}{c}\right] \\ &= \frac{(2^\kappa+1)\sqrt{\Delta}}{2^\kappa h^+}\ \sum_{\substack{c=\sqrt{\Delta}/2 \\ 4,p_i^2\nmid c}}^{\sqrt{\Delta}} \frac{1}{c} \\ &\sim \frac{(2^\kappa+1)\sqrt{\Delta}\log 2}{2^\kappa h^+}\ \left(\frac{2^2-1}{2^2}\right)\ \prod_{i=1}^{n}\frac{p_i^2-1}{p_i^2} \end{aligned}$$

$$= \frac{3\left(2^{k+n+1}+1\right)\sqrt{N}\log 2}{2^{k+n+2}h^+} \prod_{i=1}^{n} \frac{p_i^2-1}{p_i^{3/2}} .$$

Case 4: In all other cases $\Delta = 4p_1\cdots p_nN$ and $\kappa = k+n+1$. We can obtain the result in this case by multiplying the result for Case 3 by $2^\kappa/\left(2^\kappa+1\right) = 2^{k+n+1}/\left(2^{k+n+1}+1\right)$, which gives the desired result.

□

Proposition 5.2.2. *Let N be a square-free positive integer with k distinct large odd prime divisors and let $p_1,\ldots,p_n$ be n distinct small odd primes ($n \geq 0$) with $p_i \nmid N$ for all i. Define Δ as in Proposition 5.2.1. If X_{sq} is the number of reduced square forms on the principal cycle of discriminant Δ then*

$$E[X_{sq}] = \begin{cases} \dfrac{\left(2^{k+n}+1\right)\left(\sqrt{2}-1\right)\sqrt[4]{N}}{2h^+} \prod_{i=1}^{n} \dfrac{p_i-1}{p_i^{3/4}} & \text{if } \Delta \equiv 1 \bmod 4 \text{ and } p_i \equiv 1 \bmod 4\ \forall i\ , \\ \dfrac{2^{k+n}\left(\sqrt{2}-1\right)\sqrt[4]{N}}{2h^+} \prod_{i=1}^{n} \dfrac{p_i-1}{p_i^{3/4}} & \text{if } \Delta \equiv 1 \bmod 4 \text{ and } \exists p_i \equiv 3 \bmod 4\ , \\ \dfrac{\left(2^{k+n+1}+1\right)\left(2-\sqrt{2}\right)\sqrt[4]{N}}{4h^+} \prod_{i=1}^{n} \dfrac{p_i-1}{p_i^{3/4}} & \text{if } N \equiv 2 \bmod 4 \text{ and } p_i \equiv 1 \bmod 4\ \forall i\ , \\ \dfrac{2^{k+n}\left(2-\sqrt{2}\right)\sqrt[4]{N}}{2h^+} \prod_{i=1}^{n} \dfrac{p_i-1}{p_i^{3/4}} & \text{otherwise.} \end{cases}$$

Proof. The proof of each case is similar to the corresponding proof in Proposition 4.2.6. The main difference is that we will need Lemmas 5.1.3 and 5.1.4 to handle several small ramified primes.

Case 1: (Δ and $p_i \equiv 1 \bmod 4$ for $i = 1,2,\ldots,n$.) Here $\Delta = p_1\cdots p_nN$ and so the small ramified primes are $p_1,\ldots,p_n$.

$$E[X_{sq}] = \sum_{\substack{c=1 \\ p_i \nmid c}}^{\sqrt[4]{\Delta}} E[X_{c^2}]/2$$

$$
\begin{aligned}
&= \sum_{\substack{c=1 \\ p_i \nmid c}}^{\sqrt[4]{\Delta}} \frac{(2^\kappa + 1)\, E[Y_{c^2}]}{8h^+} \\
&= \frac{2^\kappa + 1}{8h^+} \sum_{\substack{c=1 \\ p_i \nmid c}}^{\sqrt[4]{\Delta}} E[Y_{c^2}] \\
&= \frac{2^\kappa + 1}{8h^+} \left[\sum_{\substack{c=1 \\ p_i \nmid c}}^{\sqrt[4]{\Delta}/\sqrt{2}} 2 \; + \sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ p_i \nmid c}}^{\sqrt[4]{\Delta}} \frac{2\left(\sqrt{\Delta} - c^2\right)}{c^2} \right] \\
&= \frac{2^\kappa + 1}{4h^+} \left[\left(\sum_{\substack{c=1 \\ p_i \nmid c}}^{\sqrt[4]{\Delta}/\sqrt{2}} 1 \; - \sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ p_i \nmid c}}^{\sqrt[4]{\Delta}} 1 \right) + \sqrt{\Delta} \sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ p_i \nmid c}}^{\sqrt[4]{\Delta}} \frac{1}{c^2} \right] \\
&\sim \frac{2^\kappa + 1}{4h^+} \left[\sqrt[4]{\Delta}\left(\sqrt{2} - 1\right) \prod_{i=1}^{n} \frac{p_i - 1}{p_i} \; + \; \sqrt{\Delta} \left(\frac{\sqrt{2} - 1}{\sqrt[4]{\Delta}} \right) \prod_{i=1}^{n} \frac{p_i - 1}{p_i} \right] \\
&= \frac{(2^\kappa + 1)\left(\sqrt{2} - 1\right)\sqrt[4]{\Delta}}{2h^+} \prod_{i=1}^{n} \frac{p_i - 1}{p_i} \, .
\end{aligned}
$$

Now $\kappa = k + n$, hence

$$
E[X_{sq}] \sim \frac{\left(2^{k+n} + 1\right)\left(\sqrt{2} - 1\right)\sqrt[4]{N}}{2h^+} \prod_{i=1}^{n} \frac{p_i - 1}{p_i^{3/4}} \, .
$$

Case 2: ($\Delta \equiv 1 \bmod 4, \exists p_i \equiv 3 \bmod 4.$) In this case we multiply the result for the previous case by $2^\kappa / \left(2^\kappa + 1\right)$, since we know that some prime equivalent to 3 mod 4 divides Δ. As in the previous case, $\Delta = p_1 \cdots p_n N$ and $\kappa = k + n$ so

$$
\begin{aligned}
E[X] &\sim \left(\frac{\left(2^{k+n} + 1\right)\left(\sqrt{2} - 1\right)\sqrt[4]{N}}{2h^+} \prod_{i=1}^{n} \frac{p_i - 1}{p_i^{3/4}} \right) \left(\frac{2^{k+n}}{2^{k+n} + 1} \right) \\
&= \frac{2^{k+n}\left(\sqrt{2} - 1\right)\sqrt[4]{N}}{2h^+} \prod_{i=1}^{n} \frac{p_i - 1}{p_i^{3/4}} \, .
\end{aligned}
$$

Case 3: ($N \equiv 2 \bmod 4, p_1 \equiv 1 \bmod 4$ for $i = 1, 2, \ldots, n.$) Here $\Delta = 4p_1 \cdots p_n N$ and $\kappa = k + n + 1$. So the small ramified primes are $2, p_1, \ldots, p_n$.

$$
E[X_{sq}] = \sum_{\substack{c=1 \\ 2, p_i \nmid c}}^{\sqrt[4]{\Delta}} E[X_{c^2}]/2
$$

$$
\begin{aligned}
&= \sum_{\substack{c=1 \\ 2,p_i \nmid c}}^{\sqrt[4]{\Delta}} \frac{(2^\kappa+1)\,E[Y_{c^2}]}{8h^+} \\
&= \frac{2^\kappa+1}{8h^+} \sum_{\substack{c=1 \\ 2,p_i \nmid c}}^{\sqrt[4]{\Delta}} E[Y_{c^2}] \\
&= \frac{2^\kappa+1}{8h^+} \left[\sum_{\substack{c=1 \\ 2,p_i \nmid c}}^{\sqrt[4]{\Delta}/\sqrt{2}} 2 \;-\; \sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ 2,p_i \nmid c}}^{\sqrt[4]{\Delta}} \frac{2\left(\sqrt{\Delta}-c^2\right)}{c^2} \right] \\
&= \frac{2^\kappa+1}{4h^+} \left[\left(\sum_{\substack{c=1 \\ 2,p_i \nmid c}}^{\sqrt[4]{\Delta}/\sqrt{2}} 1 \;-\; \sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ 2,p_i \nmid c}}^{\sqrt[4]{\Delta}} 1 \right) + \sqrt{\Delta} \sum_{\substack{c=\sqrt[4]{\Delta}/\sqrt{2} \\ 2,p_i \nmid c}}^{\sqrt[4]{\Delta}} \frac{1}{c^2} \right] \\
&\sim \frac{2^\kappa+1}{4h^+} \left[\sqrt[4]{\Delta}\left(\sqrt{2}-1\right) \left(\frac{2-1}{2}\right) \prod_{i=1}^{n} \frac{p_i-1}{p_i} \right. \\
&\qquad\qquad \left. + \sqrt{\Delta} \left(\frac{\sqrt{2}-1}{\sqrt[4]{\Delta}}\right) \left(\frac{2-1}{2}\right) \prod_{i=1}^{n} \frac{p_i-1}{p_i} \right] \\
&= \frac{(2^\kappa+1)\left(\sqrt{2}-1\right)\sqrt[4]{\Delta}}{4h^+} \prod_{i=1}^{n} \frac{p_i-1}{p_i} \\
&= \frac{\left(2^{k+n+1}+1\right)\left(2-\sqrt{2}\right)\sqrt[4]{N}}{4h^+} \prod_{i=1}^{n} \frac{p_i-1}{p_i^{3/4}} \,.
\end{aligned}
$$

Case 4: In all other cases $\Delta = 4p_1 \cdots p_n N$ and $\kappa = k+n+1$. We can obtain the result in this case by multiplying the result for Case 3 by $2^\kappa/\left(2^\kappa+1\right) = 2^{k+n+1}/\left(2^{k+n+1}+1\right)$, which gives the desired result.

□

Corollary 5.2.3. *Let N be a square-free positive integer with k distinct large odd prime divisors and let $p_1, \ldots, p_n$ be n distinct small odd primes ($n \geq 0$) with $p_i \nmid N$*

for all i. Define Δ as in Proposition 5.2.1. If D is the index-difference between successive square forms on the principal cycle, then

$$E[D] = \begin{cases} \dfrac{\left(\sqrt{2}+1\right)\sqrt[4]{N}\log 2}{2^{k-1}} \prod_{i=1}^{n} \dfrac{p_i+1}{2p_i^{3/4}} & \text{if} \quad \Delta \equiv 1 \bmod 4\ , \\ \\ \dfrac{3\left(\sqrt{2}+2\right)\sqrt[4]{N}\log 2}{2^{k+1}} \prod_{i=1}^{n} \dfrac{p_i+1}{2p_i^{3/4}} & \text{if} \quad \Delta \equiv 0 \bmod 4\ . \end{cases}$$

Proof. Just as with the proof of Corollary 4.2.9, we obtain the result by computing $E[X]/E[X_{sq}]$. □

Proposition 5.2.4. *Let N be a square-free positive integer with k distinct large odd prime divisors and let $p_1, \ldots, p_n$ be n distinct small odd primes ($n \geq 0$) with $p_i \nmid N$ for all i. Define Δ as in Proposition 5.2.1. If W is the number of forms that SQUFOF must examine before finding a proper square form, then*

$$E[W] = \begin{cases} \dfrac{2\left(\sqrt{2}+1\right)\sqrt[4]{N}\log 2}{2^{k}-2} \prod_{i=1}^{n} \dfrac{p_i+1}{2p_i^{3/4}} & \text{if} \quad \Delta \equiv 1 \bmod 4\ , \\ \\ \dfrac{3\left(\sqrt{2}+2\right)\sqrt[4]{N}\log 2}{2\left(2^{k}-2\right)} \prod_{i=1}^{n} \dfrac{p_i+1}{2p_i^{3/4}} & \text{if} \quad \Delta \equiv 0 \bmod 4\ . \end{cases}$$

Proof. As in the proof of Proposition 4.4.1, this is the product of the results from Corollaries 4.3.3 and 5.2.3. □

5.3 Using the Queue with Multipliers

We begin with Propositions analogous to Propositions 3.2.1 and 3.2.2.

Proposition 5.3.1. *Let N be a square-free positive integer with k distinct large odd prime divisors and let $p_1, \ldots, p_n$ be n distinct small odd primes ($n \geq 0$) with $p_i \nmid N$ for all i. Define Δ as in Proposition 5.2.1. Suppose that a is a positive odd integer, b is a positive integer, $\gcd(a,b) = 1$, and that $(a^2, b, -c)$ is a square form on the principal cycle of discriminant Δ with $c > 0$. Then $(-a, b, ac)^2 \sim (a^2, b, -c)$.*

Proof. This follows directly from the definition of composition. □

There are 2^{κ} reduced ambiguous forms of discriminant Δ. The forms $(\pm d, *, *)$, where d is a square-free divisor of Δ relatively prime to N with $|d| < \sqrt{\Delta}$, lead to trivial factorizations of N. Let $\pm\mathbf{d}$ denote the reduced ambiguous form $(\pm d, *, *)$.

Proposition 5.3.2. *Let N be a square-free positive integer with k distinct large odd prime divisors and let $p_1, \ldots, p_n$ be n distinct small odd primes ($n \geq 0$) with $p_i \nmid N$ for all i. Define Δ as in Proposition 5.2.1. Suppose that a is a positive odd integer, b is a positive integer,* $\gcd(a, b) = 1$, *and that $F_n = (a^2, b, -c)$ is a square form on the principal cycle of discriminant Δ, with $c > 0$. Some form $(\alpha, \beta, *)$ appears on the principal cycle at position $m < n$ with $\alpha \in \{\pm da\}$, where d is a square-free divisor of Δ that is relatively prime to N with $|d| < \sqrt{\Delta}$, and $\beta \equiv b \bmod a$ if and only if $(-a, b, ac)$ is equivalent to one of the ambiguous forms $\pm\mathbf{d}$.*

Proof. Suppose some form $(\alpha, \beta, *)$ appears on the principal cycle at position $m < n$ with $\alpha = da$, where d is a square-free divisor of Δ that is relatively prime to N with $|d| < \sqrt{\Delta}$, and $\beta \equiv b \bmod a$. Then we can write the form as $(\alpha, \beta, *) \sim (da, \beta, *)$. It is easy to see that $-\mathbf{d} \sim (da, \beta, *) \circ -\mathbf{d} \sim (-a, \beta, *) \sim (-a, b, ac)$.

Conversely, suppose there is no form $(\alpha, \beta, *)$ appearing on the principal cycle before F_n with $\alpha \in \{\pm da\}$ and $\beta \equiv b \bmod a$. Let $f = (-a, b, ac)$. If f is equivalent to some $g \in \{\pm\mathbf{d}\}$, then $f \circ g \sim \mathbf{1}$ and $f \circ g$ is equivalent to some form $(\alpha, \beta', *)$ with $\alpha \in \{\pm da\}$ and $\beta' \equiv b \bmod a$. But this square root is equivalent to a reduced square root $(\alpha, \beta, *)$, with $\alpha \in \{\pm da\}$ and $\beta \equiv \beta' \equiv b \bmod a$, that must be on the principal cycle. But then this reduced square root must appear before the form F_n, a contradiction. Therefore, f is not equivalent to any of the ambiguous forms $\pm\mathbf{d}$. □

Proposition 5.3.2 says that when we have several small ramified primes, the test for whether a form is enqueued or not is the following. First suppose $N \equiv 1 \bmod 4$. If a form $(*, b, c)$ is found such that $|c'| < \sqrt[4]{\Delta}$, where $c' = c/\gcd(c, p_1 \cdots p_n)$, then SQUFOF will enqueue the pair $(c', b \bmod c')$. If $N \equiv 2$ or $3 \bmod 4$, then the additional ramified prime 2 means that we should take $c' = c/\gcd(c, 2p_1 \cdots p_n)$. We now turn

to the task of computing the expected number of forms enqueued in terms of N and p_i.

Proposition 5.3.3. *Let $0 \ll \Delta$ be a positive integer and suppose $p_1, \ldots, p_n$, for $n \geq 0$, are distinct small primes with $p_i \ll \Delta$. Let $\mathcal{S}$ be the set of integers c such that*

1. *$p_i^2 \nmid c$ for $i = 1, 2, \ldots, n$, and*
2. *$|c| < \sqrt[4]{\Delta}$, or*
3. *if $|c| > \sqrt[4]{\Delta}$, then $|c'| < \sqrt[4]{\Delta}$, where $c' = c/\gcd(p_1 \cdots p_n, c)$.*

Then

$$|\mathcal{S}| \sim |\mathcal{T}| \prod_{i=1}^{n} \frac{2p_i + 1}{p_i + 1},$$

where

$$|\mathcal{T}| \sim 2\sqrt[4]{\Delta} \prod_{i=1}^{n} \frac{p_i^2 + 1}{p_i^2},$$

and $\mathcal{T}$ is the set of integers satisfying only 1. and 2. above.

Proof. The asymptotics behavior of the cardinality of the set $\mathcal{T}$ is clear, as is the behavior of the cardinality of the set $\mathcal{S}$ when $n = 0$. We prove the asymptotic behavior of the cardinality of the set $\mathcal{S}$ for $n > 0$ by induction on n.

Suppose $n = 1$. Of the integers in $\mathcal{T}$, the subset of integers c divisible by p_1 (given that c is not divisible by p_1^2) has size $|\mathcal{T}|/(p_1 + 1)$, using the fundamental equation for conditional probabilities. None of these numbers can also appear as a c' for some $c > \sqrt[4]{\Delta}$. The rest of the integers in the set $\mathcal{T}$ are not divisible by p_1, so if we multiply each of these by p_1, we get a new set of integers that must satisfy 1. and 3. Thus

$$|\mathcal{S}| \sim |\mathcal{T}| \frac{1}{p_1 + 1} + 2\,|\mathcal{T}| \frac{p_1}{p_1 + 1} = |\mathcal{T}| \prod_{i=1}^{1} \frac{2p_i + 1}{p_i + 1}.$$

Now suppose that the claim holds for any choice of $n - 1$ primes and consider the case of n primes $p_1, \ldots, p_n$. Again, it is easy to see that

$$|\mathcal{T}| \sim 2\sqrt[4]{\Delta} \prod_{i=1}^{n} \frac{p_i^2 + 1}{p_i^2}.$$

The subset of these numbers divisible by p_n has cardinality $|\mathcal{T}|/(p_n+1)$. Each of these can be multiplied by some square-free product (perhaps trivial) of only the $p_1, \ldots, p_{n-1}$. By the induction hypothesis, this subset leads to

$$|\mathcal{T}| \, \frac{1}{p_n+1} \, \prod_{i=1}^{n-1} \frac{2p_i+1}{p_i+1}$$

integers that satisfy either 1. and 2., or 1. and 3. The rest of the integers in $\mathcal{T}$ are not divisible by p_n. Again, by the induction hypothesis, this subset leads to

$$2\,|\mathcal{T}| \, \frac{p_n}{p_n+1} \, \prod_{i=1}^{n-1} \frac{2p_i+1}{p_i+1} \, ,$$

where we first count those numbers that we get by multiplying by some square-free product (perhaps trivial) of the $p_1, \ldots, p_{n-1}$, then we double our count since for each of these we may multiply by either 1 or p_n. Finally, $|\mathcal{S}|$, the total number of integers that satisfy either 1. and 2., or 1. and 3. is

$$\begin{aligned} |\mathcal{S}| \;&\sim\; |\mathcal{T}| \, \frac{1}{p_n+1} \, \prod_{i=1}^{n-1} \frac{2p_i+1}{p_i+1} \;+ 2\,|\mathcal{T}| \, \frac{p_n}{p_n+1} \, \prod_{i=1}^{n-1} \frac{2p_i+1}{p_i+1} \\ &= |\mathcal{T}| \, \prod_{i=1}^{n} \frac{2p_i+1}{p_i+1} \, . \end{aligned}$$

Thus the claim holds for all $n \geq 0$. □

Proposition 5.3.4. *Let N be a square-free positive integer with k distinct large odd prime divisors and let $p_1, \ldots, p_n$ be n distinct small odd primes ($n \geq 0$) with $p_i \nmid N$ for all i. Define Δ as in Proposition 5.2.1. If Q is the number of forms that SQUFOF enqueues before finding a proper square form, then*

$$E[Q] = \begin{cases} \dfrac{2\left(\sqrt{2}+1\right)\log 2}{2^k-2} \, \prod_{i=1}^{n} \dfrac{2p_i+1}{2p_i} & \text{if} \quad \Delta \equiv 1 \bmod 4 \, , \\[2ex] \dfrac{5\left(\sqrt{2}+1\right)\log 2}{2\left(2^k-2\right)} \, \prod_{i=1}^{n} \dfrac{2p_i+1}{2p_i} & \text{if} \quad \Delta \equiv 0 \bmod 4 \, . \end{cases}$$

Proof. Proposition 5.3.3 counts the number of end coefficients that will lead to a form being enqueued, where we must include the small prime 2 if it is ramified. The

number of end coefficients c with $|c| < \sqrt{\Delta}$ and c not divisible by the square of any ramified prime is given by $|\mathcal{T}|$ of Proposition 5.3.3, where again we include the small prime 2 whenever it is ramified, and we replace $\sqrt[4]{\Delta}$ with $\sqrt{\Delta}$. We take the ratio of these two numbers to be the probability that a form will be enqueued. Finally, we take the product of this number with $E[W]$ to get $E[Q]$, as in the proof of Proposition 4.5.2. □

5.4 Optimal Multipliers for SQUFOF

When SQUFOF is implemented using the continued fraction description, the case of $p_1 \cdots p_n N \equiv 1 \bmod 4$ is never encountered, since we assume multiplication of such numbers by 8 before a factorization is attempted. So we will choose the p_i so as to minimize the quantity

$$E[W] = \frac{3\left(\sqrt{2}+2\right)\sqrt[4]{N}\log 2}{2\left(2^k-2\right)} \prod_{i=1}^{n} \frac{p_i+1}{2p_i^{3/4}} ,$$

which is the factor by which factorization of $p_1 \cdots p_n N$ is faster or slower than that of N.

Proposition 5.4.1. *Let Ω be the set of all finite sets of odd primes and define the mapping $F : \Omega \to \mathbb{Z}$ by $F(\emptyset) = 1$ and*

$$F\left(\{p_1, \ldots, p_n\}\right) = \prod_{i=1}^{n} \frac{p_i+1}{2p_i^{3/4}} .$$

Then F is minimized at the set $\{3,5,7,11\}$ and

$$F\left(\{3,5,7,11\}\right) \doteq 0.7268 .$$

Proof. It is easy to check that $F\left(\{3,5,7,11\}\right) \doteq 0.7268$. We will show that for any other finite set of odd primes $\{p_1, \ldots, p_n\}$, we will have

$$F\left(\{p_1, \ldots, p_n\}\right) > F\left(\{3,5,7,11\}\right) ,$$

which will prove the claim. So suppose by way of contradiction that there exists a finite set of odd primes $\{p_1, \ldots, p_n\}$ such that $F(\{p_1, \ldots, p_n\}) < F(\{3, 5, 7, 11\})$. Since $F(\emptyset) = 1$, F is not minimized at $\emptyset$ and so $n > 0$.

It is easy to check that the function $f(x) = (x+1)/2x^{3/4}$ is strictly increasing on $[3, \infty)$ and so for a given n, among all sets of n primes, F is minimized at $\{3, 5, 7, \ldots, p_n\}$, where p_n is the n^{th} odd prime. Straightforward computation shows that for sets of n primes with $n = 1, 2, 3, 4$, F is minimized at $\{3, 5, 7, 11\}$. Finally, one easily sees that $(x+1)/2x^{3/4} > 1$ for $x \geq 13$. This means that adding any additional primes to the set $\{3, 5, 7, 11\}$ will increase the value of F at this new set. Therefore, F is minimized at the set $\{3, 5, 7, 11\}$. □

Proposition 5.4.1 shows that the optimal multiplier is $3 \cdot 5 \cdot 7 \cdot 11 = 1155$, and that in fact we can expect SQUFOF to find a non-trivial factor of N using $1155N$ in about 73% of the time that it would take using N. However, for practical reasons associated with the size of single precision numbers, SQUFOF may actually run faster for smaller multipliers.

Let F be defined as in Proposition 5.4.1 and let $G(\{p_1, \ldots, p_n) = \prod_{i=1}^{n} \frac{2p_i+1}{2p_i}$ be the factor by which the number of forms enqueued is larger when factoring $p_1 \cdots p_n N$ than when factoring N. Table 5.1 lists some good candidate multipliers, along with the associated values of F and G. Note that for the values of $p_1 \cdots p_n$ considered in Table 5.1, the value of G is no larger than 1.5. In other words, at worst we can expect a 50% increase in the number of forms enqueued when using one of these multipliers. However, the number of forms enqueued without using a multiplier is very small—about 2.1 forms. So even though the rules for enqueuing a form are more complicated (hence more time consuming) when using multipliers, this expected running time cost is negligible compared with the expected running time savings.

$p_1 \cdots p_n$	$F(\{p_1, \ldots, p_n\})$	$G(\{p_1, \ldots, p_n\})$
3	0.8774	1.1667
5	0.8972	1.1000
7	0.9295	1.0714
11	0.9934	1.0455
$3 \cdot 5$	0.7872	1.2833
$3 \cdot 7$	0.8155	1.2500
$3 \cdot 11$	0.8716	1.2197
$5 \cdot 7$	0.8339	1.1786
$5 \cdot 11$	0.8913	1.1500
$7 \cdot 11$	0.9233	1.1201
$3 \cdot 5 \cdot 7$	0.7317	1.3750
$3 \cdot 5 \cdot 11$	0.7820	1.3417
$3 \cdot 7 \cdot 11$	0.8101	1.3068
$5 \cdot 7 \cdot 11$	0.8284	1.2321
$3 \cdot 5 \cdot 7 \cdot 11$	0.7268	1.4375

Table 5.1
Good candidate multipliers for $N \equiv 2$ or 3 mod 4.

5.5 Racing SQUFOF with multipliers

Originally, the main reason for using multipliers was to exploit the great variation in W, the actual number of forms that SQUFOF must examine before finding a proper square form. Racing several multipliers succeeds when the first proper square form is found, which is very likely to be where we expect for at least one of the multiples of N. The results of the previous section suggest that if we choose the multipliers wisely, we can expect the proper square form to come even sooner.

6. Experimental Results

6.1 Factoring with and without Multipliers

In this section we describe our experiments with factoring integers with two, three, or four large prime divisors, with and without the use of multipliers. We present the results of these experiments and compare them with the expected running time and expected number of forms enqueued for $p_1 \cdots p_n N \equiv 2$ or $3 \bmod 4$.

6.1.1 Factoring Products of Two Primes

We began by generating $40,000$ values for N by taking N to be the product of two primes p and q where $30011 \leq p \leq 32099$ and $36097 \leq q \leq 38239$. Whenever $pq \equiv 1 \bmod 4$ we take $N = 2pq$, otherwise $N = pq$. SQUFOF then attempted to factor each of these 10-digit numbers, failing to find a non-trivial factor only when the principal period contains no proper square forms, or if there was a queue overflow. We found the failure rate to be no more than 2% for a maximum queue length of 55. We repeated the factorization for each value of N and each multiplier m from Table 5.1.

Let FWRD be the number of forms of discriminant Δ that SQUFOF examines before finding a proper square form divided by the fourth root of N. Let QUEUE be the number of forms that SQUFOF enqueues during the search for a proper square form. We computed FWRD and QUEUE for each successful factorization. We then computed the average values $\overline{\text{FWRD}}$ and $\overline{\text{QUEUE}}$, along with the standard deviations σ (FWRD) and σ (QUEUE). We also the computed the maximum and minimum value for FWRD and QUEUE, which gives the inequalities: $0.0053 \leq \text{FWRD} \leq 32.8856$ and $0 \leq \text{QUEUE} \leq 78$. Table 6.1 gives a comparison between the predicted and

calculated values for FWRD and QUEUE. Note that we have not given the multipliers in their factored form due to space constraints.

6.1.2 Factoring Products of Three Primes

Next we generated $10,000$ products of three primes by choosing 50 primes p congruent to 1 modulo 4 with $30013 \leq p \leq 30941$, 50 primes q congruent to 3 modulo 4 with $32971 \leq q \leq 33923$, and a third prime $r \in \{9803, 9871, 9923, 9973\}$. As before, if $pqr \equiv 1 \bmod 4$, then we take $N = 2pqr$, otherwise $N = pqr$. SQUFOF then attempted to factor each of these 12-13 digit numbers. We repeated the factorization for each value of N and each multiplier m from Table 5.1. The ranges for FWRD and QUEUE are $0.0006 \leq \text{FWRD} \leq 7.6516$ and $0 \leq \text{QUEUE} \leq 21$. Table 6.2 gives a summary of the results.

6.1.3 Factoring Products of Four Primes

We then generated $10,000$ products of four primes by choosing 50 primes p congruent to 1 modulo 4 with $30013 \leq p \leq 30941$, 50 primes q congruent to 3 modulo 4 with $32971 \leq q \leq 33923$, and a third and fourth prime by taking $rs \in \{109 \cdot 1423, 109 \cdot 1429, 127 \cdot 1423, 127 \cdot 1429\}$. As before, if $pqrs \equiv 1 \bmod 4$, then we take $N = 2pqrs$, otherwise $N = pqrs$. SQUFOF then attempted to factor each of these 14 digit numbers. We repeated the factorization for each value of N and each multiplier m from Table 5.1. The ranges for FWRD and QUEUE are $0.0003 \leq \text{FWRD} \leq 2.6333$ and $0 \leq \text{QUEUE} \leq 12$. Table 6.3 gives a summary of the results.

6.2 Racing with Multipliers

In this section we describe our experiments with racing multipliers to factor integers with two, three, or four large prime divisors. As in the previous section, we

worked only with integers $p_1 \cdots p_n N \equiv 2$ or $3 \bmod 4$. We used multipliers m_1, m_2 taken from Table 5.1, where $m_1 < m_2$.

6.2.1 Factoring Products of Two Primes by Racing Two Multipliers

We began the racing experiments by generating $10,000$ values for N by choosing 100 primes p congruent to 1 modulo 4 with $30013 \leq p \leq 32089$ and 100 primes q congruent to 3 modulo 4 with $34123 \leq q \leq 36067$, then taking $N = 2pq$ whenever $pq \equiv 1 \bmod 4$ and otherwise $N = pq$. For each pair m_1, m_2 with $m_1 < m_2$ SQUFOF attempted to factor each of these 10-digit numbers by racing the factorizations of $m_1 N$ and $m_2 N$.

Let FWRD be the total number of forms that SQUFOF examines during the race before finding a proper square form divided by the fourth root of N. Let QUEUE be the total number of forms that SQUFOF enqueues during the race. We computed FWRD and QUEUE for each successful factorization. We then computed the average values $\overline{\text{FWRD}}$ and $\overline{\text{QUEUE}}$, along with the standard deviations $\sigma\,(\text{FWRD})$ and $\sigma\,(\text{QUEUE})$. We also the computed the maximum and minimum value for FWRD and QUEUE, which gives the inequalities: $0.0109 \leq \text{FWRD} \leq 32.3333$ and $0 \leq \text{QUEUE} \leq 115$. Tables A.1 - A.15 in Appendix A give a summary of our findings.

6.2.2 Factoring Products of Three Primes by Racing Two Multipliers

Next we generated $10,000$ products of three primes by choosing 50 primes p congruent to 1 modulo 4 with $30013 \leq p \leq 30941$, 50 primes q congruent to 3 modulo 4 with $32971 \leq q \leq 33923$, and a third prime $r \in \{101, 103, 107, 109\}$. As before, if $pqr \equiv 1 \bmod 4$, then we take $N = 2pqr$, otherwise $N = pqr$. For each pair m_1, m_2 with $m_1 < m_2$ SQUFOF attempted to factor each of these 10-11 digit numbers by racing the factorizations of $m_1 N$ and $m_2 N$. The ranges for FWRD and QUEUE are $0.0034 \leq \text{FWRD} \leq 9.4782$ and $0 \leq \text{QUEUE} \leq 97$. Tables A.16 - A.30 in Appendix A give a summary of our findings.

6.2.3 Factoring Products of Four Primes by Racing Two Multipliers

We then generated $10,000$ products of four primes by choosing 50 primes p congruent to 1 modulo 4 with $30013 \leq p \leq 30941$, 50 primes q congruent to 3 modulo 4 with $32971 \leq q \leq 33923$, and a third and fourth prime by taking $rs \in \{109 \cdot 1423, 109 \cdot 1429, 127 \cdot 1423, 127 \cdot 1429\}$. As before, if $pqrs \equiv 1 \bmod 4$, then we take $N = 2pqrs$, otherwise $N = pqrs$. SQUFOF attempted to factor each of these 14 digit numbers by racing the factorizations of m_1N and m_2N. The ranges for FWRD and QUEUE are $0.0005 \leq \text{FWRD} \leq 12.6129$ and $0 \leq \text{QUEUE} \leq 82$. Tables A.31 - A.45 in Appendix A give a summary of our findings.

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

Table 6.1
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	0.5916	0.5821	0.5771	0.6973	0.7710	1.1989	0
3	0.5191	0.5209	0.5176	0.8135	0.7940	1.2030	7
5	0.5308	0.5129	0.5076	0.7670	0.7726	1.1940	44
7	0.5499	0.5360	0.5356	0.7471	0.7719	1.1904	6
11	0.5877	0.5666	0.5607	0.7289	0.7864	1.1961	2
15	0.4657	0.4544	0.4534	0.8948	0.7678	1.1705	4
21	0.4825	0.4798	0.4757	0.8716	0.8073	1.2363	5
33	0.5157	0.5156	0.5120	0.8504	0.8085	1.2300	2
35	0.4934	0.4923	0.4915	0.8218	0.8073	1.2363	2
55	0.5273	0.5158	0.5041	0.8018	0.7872	1.1722	2
77	0.5463	0.5472	0.5434	0.7810	0.8168	1.2270	2
105	0.4329	0.4274	0.4285	0.9587	0.8044	1.2303	4
165	0.4627	0.4592	0.4552	0.9355	0.8173	1.2156	0
231	0.4793	0.4768	0.4773	0.9112	0.7833	1.1851	5
385	0.4901	0.4946	0.4918	0.8591	0.7875	1.1697	3
1155	0.4300	0.4283	0.4271	1.0023	0.7881	1.1901	3

Table 6.2
Three-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	0.2536	0.2539	0.2554	0.2988	0.3403	0.6958	1
3	0.2225	0.2189	0.2232	0.3486	0.3347	0.6762	2
5	0.2275	0.2323	0.2297	0.3287	0.3398	0.6787	1
7	0.2357	0.2367	0.2324	0.3202	0.3368	0.6766	3
11	0.2519	0.2522	0.2477	0.3124	0.3321	0.6818	0
15	0.1996	0.2012	0.2011	0.3835	0.3444	0.6954	1
21	0.2068	0.2072	0.2049	0.3735	0.3328	0.6667	2
33	0.2210	0.2195	0.2158	0.3645	0.3406	0.6589	0
35	0.2114	0.2121	0.2095	0.3522	0.3298	0.6646	2
55	0.2260	0.2283	0.2300	0.3436	0.3432	0.6857	1
77	0.2341	0.2343	0.2340	0.3347	0.3409	0.6764	0
105	0.1855	0.1847	0.1806	0.4109	0.3215	0.6565	0
165	0.1983	0.2006	0.1978	0.4009	0.3430	0.6747	0
231	0.2054	0.2046	0.2045	0.3905	0.3449	0.6772	1
385	0.2100	0.2100	0.2120	0.3682	0.3465	0.6821	2
1155	0.1843	0.1858	0.1850	0.4296	0.3540	0.6964	1

Table 6.3
Four-prime statistics for FWRD and QUEUE.

This page deliberately left blank.

7. Conclusions and Further Work

We end this thesis with a conclusion and some questions for future work.

7.1 Conclusions

We have shown that given a square-free positive integer N, SQUFOF can be expected to examine

$$E[W] \sim \begin{cases} \dfrac{2\left(\sqrt{2}+1\right)\sqrt[4]{N}\log 2}{2^k-2} & \text{if } N \equiv 1 \bmod 4\ , \\ \\ \dfrac{3\left(\sqrt{2}+2\right)\sqrt[4]{N}\log 2}{2\left(2^k-2\right)} & \text{if } N \equiv 2 \text{ or } 3 \bmod 4\ , \end{cases}$$

reduced forms on the principal cycle of discriminant Δ before finding a proper square form, where Δ is defined by

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

Since a proper square form quickly leads to a proper factorization of N, this gives a good measure of the running time. Regarding the space requirement for SQUFOF, we have shown that we can expect SQUFOF to enqueue

$$E[Q] \sim \begin{cases} \dfrac{2\left(\sqrt{2}+1\right)\log 2}{2^k-2} & \text{if } N \equiv 1 \bmod 4\ , \\ \\ \dfrac{5\left(\sqrt{2}+1\right)\log 2}{2\left(2^k-2\right)} & \text{if } N \equiv 3 \bmod 4\ , \end{cases}$$

reduced forms on the principal cycle of discriminant Δ before finding a proper square form.

If we use the multiplier $p_1 \cdots p_n$ to factor N, where the p_i are distinct small odd primes, then we can expect SQUFOF to examine

$$E[W] \prod_{i=1}^{n} \frac{p_i + 1}{2p_i^{3/4}}$$

reduced forms on the principal cycle of discriminant Δ before finding a proper square form, where now Δ is defined by

$$\Delta = \begin{cases} p_1 \cdots p_n N & \text{if } p_1 \cdots p_n N \equiv 1 \bmod 4 \ , \\ 4p_1 \cdots p_n N & \text{if } p_1 \cdots p_n N \equiv 2 \text{ or } 3 \bmod 4 \ . \end{cases}$$

Furthermore, we can expect SQUFOF to enqueue

$$E[Q] \prod_{i=1}^{n} \frac{2p_i + 1}{2p_i}$$

reduced forms on the principal cycle of discriminant Δ before finding a proper square form. We performed many experiments to test our claims. We believe that the results of our experiments indicate that our simplifying assumptions are reasonable and that these expectations are useful.

7.2 Future Work

Some questions for further study:

1.) Non-square-free N: SQUFOF will work for non-fundamental discriminants Δ, and we believe that a similar analysis to that contained in this thesis will yield the running time and expected number of forms enqueued for such Δ. Towards this end, in future work we will re-examine the points where we assume Δ to be a fundamental discriminant.

2.) SQUFOF Failures: From our experiments, we have seen that SQUFOF does not fail whenever N is a product of two primes, each of which is congruent to 3 modulo 4. It would be interesting to prove why this is so. Also, we will

investigate why there are so many more failures when N is a product of two primes than when N is a product of three or four primes, and when racing with the multipliers $5 \cdot 7 \cdot 11$ or $3 \cdot 5 \cdot 7 \cdot 11$.

3.) Distributions of $E[W]$ and $E[Q]$: Our experiments suggest that $E[W]$ may be closely approximated by an exponentially distributed random variable, since we find the mean and variance to be approximately the same. In future work, we will investigate this possibility, along with the implications it holds for the distribution of $E[Q]$.

4.) Racing Multipliers: First, we would like to find results analogous to $E[W]$ and $E[Q]$ for the case of racing multipliers. If we can prove that the $E[W]$ are approximately exponentially distributed, then we will be able to give a good estimate for $E[W_r]$, the expected number of forms examined during a race between several multiples of N. We also hope to discover the distribution of $E[Q_r]$, the expected number of forms enqueued during a race between several multiples of N. Also, given that there are several multipliers m such that we can expect to factor mN faster than we can expect to factor N, it may be worthwhile to race several multiples of N.

This page deliberately left blank.

LIST OF REFERENCES

[1] http://cadigweb.ew.usna.edu/%7ewdj/mcmath/.

[2] J. Brillhart and M. A. Morrison. A Method of Factoring and the Factorization of F_7. *Mathematics of Computation*, 29:183–205, 1975.

[3] Duncan A. Buell. *Binary Quadratic Forms: Classical Theory and Modern Computations*. Springer-Verlag, 1989.

[4] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1996.

[5] Harvey Cohn. *A Second Course in Number Theory*. John Wiley & Sons, Inc., 1962.

[6] William Feller. *An Introduction to Probability Theory and Its Applications*, volume I. John Wiley & Sons, Inc., third edition, 1968.

[7] Carl F. Gauss. *Disquistitiones Arithmeticae*. Yale University Press, 1966. translated into English by Arthur A. Clarke, S. J.

[8] A. Y. Khinchin. *Continued Fractions*. The University of Chicago Press, third edition, 1964.

[9] H. W. Lenstra, Jr. On the Calculation of Regulators and Class Numbers of Quadratic Fields. In J. V. Armitage, editor, *Journées Arithmétiques, 1980*, volume 56 of *Lecture Notes Series*, pages 123–150. London Mathematical Society, 1982.

[10] J. S. Milne. Algebraic Number Theory, 1998. available at http://www.math.lsa.umich.edu/~jmilne.

[11] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, Inc., fifth edition, 1991.

[12] Hans Riesel. *Prime Numbers and Computer Methods for Factorization*. Birkhaüser, second edition, 1994.

[13] Daniel Shanks. An Attempt to Factor $N = 1002742628021$. manuscript, 3 pages.

[14] Daniel Shanks. notes for *Analysis and Improvement of the Continued Fraction Method of Factorization*. manuscript, 15 pages.

[15] Daniel Shanks. SQUFOF Notes. manuscript, 30 pages.

[16] Daniel Shanks. Class Number, a Theory of Factorization, and Genera. In *Proceedings of Symposia in Pure Mathematics*, volume 20, pages 415–440. American Mathematical Society, 1971.

[17] Daniel Shanks. The Infrastructure of a Real Quadratic Field and its Applications. In *Proceedings of the 1972 Number Theory Conference*, pages 217–224, Boulder, Colorado, 1972.

[18] Daniel Shanks. Five Number-Theoretic Algorithms. In *Proceedings of the Second Manitoba Conference on Numerical Mathematics*, pages 51–70. Utilitas Mathematica, 1973. number VII in Congressus Numerantium.

[19] Daniel Shanks. Analysis and Improvement of the Continued Fraction Method of Factorization. *American Mathematical Society Notices, 22:A–68*, 1975. Abstract 720-10-43.

[20] Samuel S. Wagstaff, Jr. *Cryptanalysis of Number Theoretic Ciphers*. CRC Press, 2003.

A. Racing with Multipliers Data

We present the data for racing multipliers m_1, m_2 from Table 5.1, for N a product of two, three, and four primes. Each table summarizes the result for racing a fixed m_1 against each multiplier m_2 with $m_1 < m_2$.

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

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

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
5	1.5446	1.5351	2.4633	3.6090	1
7	1.5807	1.5689	2.4275	3.1903	2
11	1.6205	1.5936	2.4466	3.2071	2
$3 \cdot 5$	1.4717	1.4960	2.5115	3.5144	3
$3 \cdot 7$	1.4782	1.4863	2.4345	3.3837	6
$3 \cdot 11$	1.4999	1.5229	2.3940	3.2385	6
$5 \cdot 7$	1.4905	1.4621	2.4330	3.2702	1
$5 \cdot 11$	1.5160	1.5134	2.4035	3.4065	3
$7 \cdot 11$	1.5710	1.5605	2.4188	3.0889	3
$3 \cdot 5 \cdot 7$	1.3906	1.3792	2.4768	3.4607	5
$3 \cdot 5 \cdot 11$	1.4347	1.4256	2.4320	3.4426	2
$3 \cdot 7 \cdot 11$	1.4791	1.5024	2.4591	3.3089	1
$5 \cdot 7 \cdot 11$	1.4778	1.5349	2.4436	3.6460	11
$3 \cdot 5 \cdot 7 \cdot 11$	1.3768	1.3479	2.3769	3.0663	115

Table A.2
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 3$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
7	1.5885	1.5664	2.4000	3.1011	2
11	1.6501	1.6411	2.4290	3.0286	1
$3 \cdot 5$	1.4686	1.4587	2.4817	3.2797	2
$3 \cdot 7$	1.4846	1.4707	2.3919	3.1280	1
$3 \cdot 11$	1.5415	1.5767	2.4106	3.4158	1
$5 \cdot 7$	1.5082	1.4641	2.4310	3.2208	0
$5 \cdot 11$	1.5576	1.5618	2.4499	3.3855	0
$7 \cdot 11$	1.5791	1.5521	2.4106	3.2454	2
$3 \cdot 5 \cdot 7$	1.3969	1.3643	2.4423	3.2732	5
$3 \cdot 5 \cdot 11$	1.4574	1.4493	2.4147	3.2079	1
$3 \cdot 7 \cdot 11$	1.4852	1.4766	2.4212	3.0642	2
$5 \cdot 7 \cdot 11$	1.4803	1.5067	2.3691	3.0737	12
$3 \cdot 5 \cdot 7 \cdot 11$	1.4032	1.3848	2.3968	3.2105	112

Table A.3
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 5$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
11	1.6750	1.6476	2.3905	2.9841	0
$3 \cdot 5$	1.5024	1.5194	2.4632	3.4718	2
$3 \cdot 7$	1.5308	1.5413	2.3837	3.0183	3
$3 \cdot 11$	1.5617	1.5928	2.3936	3.3862	3
$5 \cdot 7$	1.5386	1.5235	2.3910	2.9911	2
$5 \cdot 11$	1.5766	1.6233	2.3957	3.1254	0
$7 \cdot 11$	1.6267	1.6443	2.4294	3.3299	0
$3 \cdot 5 \cdot 7$	1.4268	1.4449	2.4324	3.3131	5
$3 \cdot 5 \cdot 11$	1.4758	1.4785	2.3814	3.1792	0
$3 \cdot 7 \cdot 11$	1.4985	1.5039	2.3912	3.0388	1
$5 \cdot 7 \cdot 11$	1.5130	1.5739	2.3688	3.2185	9
$3 \cdot 5 \cdot 7 \cdot 11$	1.4215	1.4371	2.3672	3.1334	106

Table A.4
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 7$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 5$	1.5373	1.5369	2.4641	3.3038	4
$3 \cdot 7$	1.5635	1.5687	2.4049	3.2795	1
$3 \cdot 11$	1.5883	1.6120	2.3527	3.2305	2
$5 \cdot 7$	1.5975	1.5757	2.4138	3.0327	0
$5 \cdot 11$	1.6260	1.6432	2.4310	3.4626	0
$7 \cdot 11$	1.6598	1.6392	2.4035	3.0978	1
$3 \cdot 5 \cdot 7$	1.4687	1.4690	2.4526	3.3900	5
$3 \cdot 5 \cdot 11$	1.5211	1.5115	2.3940	2.9792	1
$3 \cdot 7 \cdot 11$	1.5470	1.5380	2.4049	3.1102	0
$5 \cdot 7 \cdot 11$	1.5443	1.5558	2.3350	2.9135	11
$3 \cdot 5 \cdot 7 \cdot 11$	1.4510	1.4508	2.3379	2.9284	105

Table A.5
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 7$	1.3924	1.3797	2.3977	3.0994	7
$3 \cdot 11$	1.4221	1.4320	2.4048	3.3277	0
$5 \cdot 7$	1.4203	1.4256	2.4940	3.6652	0
$5 \cdot 11$	1.4618	1.4996	2.4505	3.3353	2
$7 \cdot 11$	1.4860	1.4929	2.4653	3.2708	0
$3 \cdot 5 \cdot 7$	1.3416	1.3572	2.4954	3.5007	5
$3 \cdot 5 \cdot 11$	1.3701	1.3783	2.4378	3.2650	1
$3 \cdot 7 \cdot 11$	1.3938	1.4082	2.4573	3.2494	2
$5 \cdot 7 \cdot 11$	1.3915	1.4280	2.4247	3.4237	13
$3 \cdot 5 \cdot 7 \cdot 11$	1.3148	1.3103	2.4008	3.1489	91

Table A.6
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 5$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 11$	1.4419	1.4453	2.3497	3.2228	3
$5 \cdot 7$	1.4298	1.4046	2.3791	3.0752	2
$5 \cdot 11$	1.4678	1.4694	2.3733	3.1562	4
$7 \cdot 11$	1.5031	1.4912	2.3530	2.9123	5
$3 \cdot 5 \cdot 7$	1.3373	1.3174	2.4230	3.3711	4
$3 \cdot 5 \cdot 11$	1.3891	1.3758	2.3912	3.1544	2
$3 \cdot 7 \cdot 11$	1.4029	1.3874	2.3691	2.9938	1
$5 \cdot 7 \cdot 11$	1.4167	1.4262	2.3515	2.9957	9
$3 \cdot 5 \cdot 7 \cdot 11$	1.3343	1.3055	2.3404	2.8637	99

Table A.7
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 7$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$5 \cdot 7$	1.4724	1.4671	2.3793	3.2583	2
$5 \cdot 11$	1.4983	1.5308	2.3535	3.1854	4
$7 \cdot 11$	1.5561	1.6212	2.4155	3.5726	3
$3 \cdot 5 \cdot 7$	1.3582	1.4059	2.4055	3.6592	8
$3 \cdot 5 \cdot 11$	1.4051	1.4479	2.3475	3.2072	6
$3 \cdot 7 \cdot 11$	1.4503	1.4812	2.4099	3.2776	1
$5 \cdot 7 \cdot 11$	1.4353	1.4891	2.3371	3.1884	13
$3 \cdot 5 \cdot 7 \cdot 11$	1.3503	1.3626	2.3287	3.0222	91

Table A.8
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$5 \cdot 11$	1.4778	1.4519	2.3791	3.1818	1
$7 \cdot 11$	1.5323	1.5488	2.4064	3.1386	1
$3 \cdot 5 \cdot 7$	1.3694	1.3858	2.4501	3.2297	3
$3 \cdot 5 \cdot 11$	1.4182	1.4100	2.4068	3.0855	1
$3 \cdot 7 \cdot 11$	1.4477	1.4484	2.4552	3.2765	1
$5 \cdot 7 \cdot 11$	1.4417	1.4658	2.3822	3.0932	11
$3 \cdot 5 \cdot 7 \cdot 11$	1.3501	1.3460	2.3581	2.9290	96

Table A.9
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 5 \cdot 7$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$7 \cdot 11$	1.5656	1.5896	2.4069	3.2974	3
$3 \cdot 5 \cdot 7$	1.3793	1.3812	2.4169	3.2944	4
$3 \cdot 5 \cdot 11$	1.4316	1.4426	2.3933	3.2371	5
$3 \cdot 7 \cdot 11$	1.4538	1.4741	2.3935	3.0984	4
$5 \cdot 7 \cdot 11$	1.4472	1.5032	2.3075	3.0246	12
$3 \cdot 5 \cdot 7 \cdot 11$	1.3822	1.3934	2.3694	3.1920	100

Table A.10
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 5 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 5 \cdot 7$	1.4215	1.4218	2.4441	3.3959	3
$3 \cdot 5 \cdot 11$	1.4636	1.4673	2.3988	3.2373	4
$3 \cdot 7 \cdot 11$	1.4947	1.5099	2.4230	3.2435	4
$5 \cdot 7 \cdot 11$	1.4993	1.5289	2.3737	3.1859	11
$3 \cdot 5 \cdot 7 \cdot 11$	1.3887	1.3594	2.3450	2.9337	102

Table A.11
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 7 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 5 \cdot 11$	1.3108	1.3185	2.4280	3.3120	3
$3 \cdot 7 \cdot 11$	1.3274	1.3304	2.4325	3.3615	3
$5 \cdot 7 \cdot 11$	1.3381	1.3403	2.3951	3.1983	9
$3 \cdot 5 \cdot 7 \cdot 11$	1.2664	1.2633	2.4249	3.5217	100

Table A.12
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 5 \cdot 7$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 7 \cdot 11$	1.3274	1.3304	2.4266	3.2476	3
$5 \cdot 7 \cdot 11$	1.3381	1.3403	2.3638	2.8799	9
$3 \cdot 5 \cdot 7 \cdot 11$	1.2664	1.2633	2.3395	3.1553	100

Table A.13
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 5 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$5 \cdot 7 \cdot 11$	1.3992	1.4263	2.3838	3.1727	10
$3 \cdot 5 \cdot 7 \cdot 11$	1.3139	1.3006	2.3449	2.9594	96

Table A.14
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 7 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 5 \cdot 7 \cdot 11$	1.3170	1.3531	2.3011	2.9217	108

Table A.15
Two-prime racing statistics for FWRD and QUEUE, $m_1 = 5 \cdot 7 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
3	0.5707	0.5569	0.8139	1.2288	0
5	0.5723	0.5562	0.8038	1.2441	0
7	0.5770	0.5630	0.8122	1.2200	0
11	0.6001	0.5943	0.7805	1.2042	0
$3 \cdot 5$	0.5344	0.5328	0.8032	1.2106	0
$3 \cdot 7$	0.5374	0.5169	0.7992	1.1927	0
$3 \cdot 11$	0.5518	0.5514	0.7851	1.3589	0
$5 \cdot 7$	0.5439	0.5320	0.7804	1.1790	0
$5 \cdot 11$	0.5764	0.5659	0.8054	1.2074	0
$7 \cdot 11$	0.5793	0.5606	0.7868	1.1814	0
$3 \cdot 5 \cdot 7$	0.5041	0.4921	0.7934	1.2004	1
$3 \cdot 5 \cdot 11$	0.5288	0.5302	0.7951	1.2533	0
$3 \cdot 7 \cdot 11$	0.5417	0.5346	0.7888	1.1905	0
$5 \cdot 7 \cdot 11$	0.5474	0.5367	0.8114	1.2266	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.5071	0.5010	0.7860	1.1897	0

Table A.16
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 1$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
5	0.5373	0.5161	0.8319	1.2832	0
7	0.5361	0.5156	0.8071	1.1811	0
11	0.5526	0.5276	0.7999	1.1933	0
$3 \cdot 5$	0.4969	0.4851	0.8063	1.2397	0
$3 \cdot 7$	0.5056	0.4855	0.8119	1.2310	0
$3 \cdot 11$	0.5200	0.5069	0.8113	1.2959	0
$5 \cdot 7$	0.5124	0.4954	0.8033	1.2086	0
$5 \cdot 11$	0.5358	0.5209	0.8106	1.2109	0
$7 \cdot 11$	0.5432	0.5322	0.7985	1.1944	0
$3 \cdot 5 \cdot 7$	0.4773	0.4662	0.8165	1.2189	0
$3 \cdot 5 \cdot 11$	0.4958	0.4866	0.8091	1.2103	0
$3 \cdot 7 \cdot 11$	0.5015	0.4846	0.7966	1.1739	0
$5 \cdot 7 \cdot 11$	0.5118	0.4991	0.8283	1.2242	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.4753	0.4592	0.8070	1.1908	0

Table A.17
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 3$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
7	0.5465	0.5267	0.8246	1.3735	0
11	0.5648	0.5553	0.8124	1.3185	0
$3 \cdot 5$	0.5034	0.4881	0.8174	1.2577	0
$3 \cdot 7$	0.5135	0.4911	0.8087	1.4319	0
$3 \cdot 11$	0.5276	0.5222	0.7947	1.2798	1
$5 \cdot 7$	0.5208	0.5082	0.8167	1.2874	0
$5 \cdot 11$	0.5438	0.5315	0.8206	1.5030	0
$7 \cdot 11$	0.5577	0.5479	0.8131	1.2858	0
$3 \cdot 5 \cdot 7$	0.4867	0.4755	0.8196	1.3004	0
$3 \cdot 5 \cdot 11$	0.4987	0.4868	0.8088	1.2633	0
$3 \cdot 7 \cdot 11$	0.5114	0.4990	0.8095	1.3043	0
$5 \cdot 7 \cdot 11$	0.5213	0.5085	0.8309	1.2895	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.4861	0.4789	0.8119	1.2213	0

Table A.18
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 5$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
11	0.5704	0.5678	0.8162	1.2430	0
$3 \cdot 5$	0.5033	0.4890	0.8127	1.2416	0
$3 \cdot 7$	0.5163	0.4977	0.8214	1.2826	0
$3 \cdot 11$	0.5261	0.5211	0.8044	1.3011	0
$5 \cdot 7$	0.5196	0.5092	0.8004	1.2220	0
$5 \cdot 11$	0.5451	0.5322	0.8192	1.2054	0
$7 \cdot 11$	0.5578	0.5514	0.8138	1.2369	0
$3 \cdot 5 \cdot 7$	0.4855	0.4699	0.8269	1.2797	0
$3 \cdot 5 \cdot 11$	0.4974	0.4847	0.7950	1.2071	0
$3 \cdot 7 \cdot 11$	0.5159	0.5124	0.8147	1.2260	0
$5 \cdot 7 \cdot 11$	0.5221	0.5105	0.8268	1.2377	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.4863	0.4748	0.7984	1.1863	0

Table A.19
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 7$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 5$	0.5162	0.5008	0.7919	1.2020	0
$3 \cdot 7$	0.5329	0.5225	0.7983	1.2251	0
$3 \cdot 11$	0.5403	0.5410	0.7668	1.1827	1
$5 \cdot 7$	0.5432	0.5409	0.7899	1.1956	0
$5 \cdot 11$	0.5629	0.5536	0.7974	1.2233	0
$7 \cdot 11$	0.5699	0.5615	0.7824	1.2047	0
$3 \cdot 5 \cdot 7$	0.4983	0.4992	0.7964	1.2345	0
$3 \cdot 5 \cdot 11$	0.5172	0.5165	0.7900	1.2194	0
$3 \cdot 7 \cdot 11$	0.5234	0.5162	0.7831	1.2003	0
$5 \cdot 7 \cdot 11$	0.5366	0.5335	0.8104	1.2332	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.4974	0.4891	0.7848	1.1875	0

Table A.20
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 7$	0.4793	0.4697	0.7973	1.2128	0
$3 \cdot 11$	0.4838	0.4715	0.7879	1.4110	0
$5 \cdot 7$	0.4763	0.4639	0.7883	1.2130	0
$5 \cdot 11$	0.5030	0.4866	0.8074	1.1953	0
$7 \cdot 11$	0.5080	0.4985	0.7948	1.2165	0
$3 \cdot 5 \cdot 7$	0.4516	0.4526	0.8172	1.2650	0
$3 \cdot 5 \cdot 11$	0.4605	0.4502	0.7878	1.2211	0
$3 \cdot 7 \cdot 11$	0.4707	0.4662	0.8001	1.2658	0
$5 \cdot 7 \cdot 11$	0.4834	0.4741	0.8200	1.2242	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.4511	0.4399	0.7923	1.1842	0

Table A.21
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 5$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 11$	0.4939	0.4892	0.7864	1.2395	1
$5 \cdot 7$	0.4934	0.4845	0.7914	1.2238	0
$5 \cdot 11$	0.5074	0.4927	0.7911	1.2167	0
$7 \cdot 11$	0.5164	0.4931	0.7901	1.2710	0
$3 \cdot 5 \cdot 7$	0.4577	0.4441	0.8046	1.2552	0
$3 \cdot 5 \cdot 11$	0.4733	0.4604	0.8038	1.2362	0
$3 \cdot 7 \cdot 11$	0.4829	0.4709	0.7987	1.2223	0
$5 \cdot 7 \cdot 11$	0.4927	0.4754	0.8161	1.2270	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.4594	0.4397	0.7939	1.1975	0

Table A.22
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 7$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$5 \cdot 7$	0.5010	0.5042	0.7772	1.2082	1
$5 \cdot 11$	0.5277	0.5259	0.7885	1.1978	1
$7 \cdot 11$	0.5291	0.5259	0.7868	1.3127	0
$3 \cdot 5 \cdot 7$	0.4624	0.4620	0.7793	1.2879	0
$3 \cdot 5 \cdot 11$	0.4834	0.4857	0.7823	1.2668	0
$3 \cdot 7 \cdot 11$	0.4944	0.4862	0.7787	1.2314	0
$5 \cdot 7 \cdot 11$	0.5043	0.5004	0.7969	1.2328	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.4659	0.4635	0.7808	1.1674	0

Table A.23
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$5 \cdot 11$	0.5129	0.4933	0.7847	1.1976	0
$7 \cdot 11$	0.5224	0.5193	0.7822	1.2329	0
$3 \cdot 5 \cdot 7$	0.4586	0.4474	0.8017	1.6729	0
$3 \cdot 5 \cdot 11$	0.4776	0.4754	0.7823	1.3303	0
$3 \cdot 7 \cdot 11$	0.4833	0.4770	0.7883	1.3527	0
$5 \cdot 7 \cdot 11$	0.4938	0.4841	0.7999	1.2082	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.4647	0.4585	0.7882	1.1796	0

Table A.24
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 5 \cdot 7$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$7 \cdot 11$	0.5451	0.5333	0.7972	1.2139	0
$3 \cdot 5 \cdot 7$	0.4821	0.4786	0.8118	1.2195	0
$3 \cdot 5 \cdot 11$	0.4972	0.4848	0.7902	1.2017	0
$3 \cdot 7 \cdot 11$	0.5054	0.4926	0.8010	1.2023	0
$5 \cdot 7 \cdot 11$	0.5228	0.5132	0.8227	1.2247	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.4761	0.4554	0.7808	1.1628	0

Table A.25
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 5 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 5 \cdot 7$	0.4850	0.4782	0.7948	1.2361	0
$3 \cdot 5 \cdot 11$	0.5020	0.4901	0.7848	1.2108	0
$3 \cdot 7 \cdot 11$	0.5108	0.5001	0.7929	1.2224	0
$5 \cdot 7 \cdot 11$	0.5275	0.5202	0.8270	1.2497	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.4926	0.4893	0.7907	1.1836	0

Table A.26
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 7 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 5 \cdot 11$	0.4441	0.4349	0.7981	1.1935	0
$3 \cdot 7 \cdot 11$	0.4505	0.4516	0.7886	1.2196	0
$5 \cdot 7 \cdot 11$	0.4558	0.4426	0.8139	1.3828	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.4354	0.4300	0.8009	1.989	0

Table A.27
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 5 \cdot 7$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 7 \cdot 11$	0.4609	0.4489	0.7763	1.1799	0
$5 \cdot 7 \cdot 11$	0.4792	0.4674	0.8109	1.2388	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.4470	0.4405	0.7864	1.2571	0

Table A.28
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 5 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$5 \cdot 7 \cdot 11$	0.4871	0.4812	0.8016	1.2017	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.4543	0.4471	0.7926	1.1936	0

Table A.29
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 7 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 5 \cdot 7 \cdot 11$	0.4626	0.4602	0.8066	1.1922	0

Table A.30
Three-prime racing statistics for FWRD and QUEUE, $m_1 = 5 \cdot 7 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
3	0.2520	0.4363	0.5667	1.2000	0
5	0.2524	0.4654	0.5769	1.2700	0
7	0.2472	0.4271	0.5569	1.1945	0
11	0.2664	0.4929	0.5661	1.2731	0
$3 \cdot 5$	0.2394	0.4106	0.5828	1.2310	0
$3 \cdot 7$	0.2447	0.4087	0.5793	1.2262	1
$3 \cdot 11$	0.2539	0.4332	0.5968	1.2875	0
$5 \cdot 7$	0.2387	0.4169	0.5626	1.1983	0
$5 \cdot 11$	0.2526	0.4465	0.5733	1.2229	0
$7 \cdot 11$	0.2589	0.4547	0.5772	1.2353	0
$3 \cdot 5 \cdot 7$	0.2372	0.4009	0.5990	1.2655	0
$3 \cdot 5 \cdot 11$	0.2417	0.4245	0.5942	1.2577	0
$3 \cdot 7 \cdot 11$	0.2444	0.4214	0.5882	1.2241	0
$5 \cdot 7 \cdot 11$	0.2463	0.4251	0.5864	1.2578	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2372	0.4045	0.6038	1.2900	0

Table A.31
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 1$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
5	0.2378	0.4208	0.5718	1.2298	0
7	0.2398	0.4010	0.5735	1.3844	0
11	0.2535	0.4368	0.5749	1.2436	0
$3 \cdot 5$	0.2327	0.3887	0.5941	1.2236	0
$3 \cdot 7$	0.2397	0.4059	0.6002	1.2382	1
$3 \cdot 11$	0.2489	0.4243	0.6032	1.2376	0
$5 \cdot 7$	0.2340	0.4085	0.5801	1.2387	0
$5 \cdot 11$	0.2396	0.4039	0.5759	1.1971	0
$7 \cdot 11$	0.2493	0.4378	0.5913	1.2535	0
$3 \cdot 5 \cdot 7$	0.2307	0.3854	0.6128	1.2405	0
$3 \cdot 5 \cdot 11$	0.2336	0.3886	0.5965	1.2048	0
$3 \cdot 7 \cdot 11$	0.2397	0.4092	0.6077	1.2527	0
$5 \cdot 7 \cdot 11$	0.2339	0.3845	0.5872	1.2111	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2309	0.3878	0.6133	1.2776	0

Table A.32
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 3$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
7	0.2375	0.4175	0.5612	1.2389	0
11	0.2533	0.4634	0.5776	1.3061	0
$3 \cdot 5$	0.2307	0.4007	0.5928	1.2594	0
$3 \cdot 7$	0.2331	0.4022	0.5925	1.3859	0
$3 \cdot 11$	0.2422	0.4106	0.5922	1.2252	0
$5 \cdot 7$	0.2326	0.4091	0.5800	1.2274	0
$5 \cdot 11$	0.2407	0.4165	0.5801	1.2164	0
$7 \cdot 11$	0.2446	0.4282	0.5845	1.2377	0
$3 \cdot 5 \cdot 7$	0.2279	0.3871	0.7105	1.2593	0
$3 \cdot 5 \cdot 11$	0.2318	0.3947	0.6029	1.2472	0
$3 \cdot 7 \cdot 11$	0.2336	0.3942	0.5855	1.2039	0
$5 \cdot 7 \cdot 11$	0.2346	0.3983	0.5904	1.2568	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2277	0.3907	0.6142	1.2923	0

Table A.33
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 5$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
11	0.2493	0.4290	0.5603	1.2321	0
$3 \cdot 5$	0.2302	0.3685	0.5728	1.2226	0
$3 \cdot 7$	0.2367	0.3951	0.5885	1.2467	1
$3 \cdot 11$	0.2471	0.4280	0.5928	1.2753	0
$5 \cdot 7$	0.2350	0.4041	0.5869	1.3980	0
$5 \cdot 11$	0.2375	0.4047	0.5552	1.1867	0
$7 \cdot 11$	0.2444	0.4221	0.5763	1.2276	0
$3 \cdot 5 \cdot 7$	0.2307	0.3956	0.5962	1.2729	0
$3 \cdot 5 \cdot 11$	0.2316	0.3863	0.5964	1.2411	0
$3 \cdot 7 \cdot 11$	0.2354	0.3904	0.5834	1.2261	0
$5 \cdot 7 \cdot 11$	0.2323	0.3813	0.5728	1.2135	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2307	0.3791	0.6086	1.3035	0

Table A.34
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 7$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 5$	0.2434	0.4250	0.5852	1.2471	0
$3 \cdot 7$	0.2428	0.4084	0.5911	1.3410	0
$3 \cdot 11$	0.2605	0.4569	0.6058	1.3307	0
$5 \cdot 7$	0.2415	0.4293	0.5765	1.2687	0
$5 \cdot 11$	0.2501	0.4225	0.5655	1.1931	0
$7 \cdot 11$	0.2556	0.4541	0.5793	1.2608	0
$3 \cdot 5 \cdot 7$	0.2389	0.4132	0.6054	1.3088	0
$3 \cdot 5 \cdot 11$	0.2446	0.4294	0.6068	1.3324	0
$3 \cdot 7 \cdot 11$	0.2446	0.4199	0.5778	1.1838	0
$5 \cdot 7 \cdot 11$	0.2454	0.4240	0.5880	1.2803	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2400	0.4003	0.6054	1.2820	0

Table A.35
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 7$	0.2272	0.3781	0.6028	1.2680	0
$3 \cdot 11$	0.2330	0.3882	0.6070	1.2359	0
$5 \cdot 7$	0.2213	0.3713	0.5993	1.3066	0
$5 \cdot 11$	0.2323	0.3898	0.5832	1.2033	0
$7 \cdot 11$	0.2329	0.3896	0.5943	1.2201	0
$3 \cdot 5 \cdot 7$	0.2209	0.3712	0.6117	1.2850	0
$3 \cdot 5 \cdot 11$	0.2259	0.3719	0.6195	1.2504	0
$3 \cdot 7 \cdot 11$	0.2255	0.3698	0.6065	1.2281	0
$5 \cdot 7 \cdot 11$	0.2233	0.3626	0.5892	1.1999	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2224	0.3757	0.6302	1.3231	0

Table A.36
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 5$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 11$	0.2444	0.4076	0.6316	1.3292	0
$5 \cdot 7$	0.2269	0.3856	0.5973	1.3452	0
$5 \cdot 11$	0.2374	0.4098	0.6072	1.4808	0
$7 \cdot 11$	0.2388	0.3919	0.5925	1.2243	0
$3 \cdot 5 \cdot 7$	0.2255	0.3821	0.6245	1.3341	0
$3 \cdot 5 \cdot 11$	0.2319	0.3930	0.6247	1.3161	0
$3 \cdot 7 \cdot 11$	0.2316	0.3769	0.6030	1.2222	1
$5 \cdot 7 \cdot 11$	0.2265	0.3595	0.6038	1.4640	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2244	0.3659	0.6143	1.2476	1

Table A.37
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 7$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$5 \cdot 7$	0.2352	0.3985	0.5989	1.2269	0
$5 \cdot 11$	0.2476	0.4362	0.5985	1.2896	0
$7 \cdot 11$	0.2500	0.4318	0.6100	1.2941	0
$3 \cdot 5 \cdot 7$	0.2361	0.3953	0.6418	1.3236	0
$3 \cdot 5 \cdot 11$	0.2386	0.4023	0.6238	1.2812	0
$3 \cdot 7 \cdot 11$	0.2384	0.3874	0.6164	1.2385	0
$5 \cdot 7 \cdot 11$	0.2384	0.4057	0.6065	1.2826	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2351	0.3921	0.6367	1.2372	0

Table A.38
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$5 \cdot 11$	0.2321	0.3959	0.5891	1.2966	0
$7 \cdot 11$	0.2370	0.4073	0.5917	1.2489	0
$3 \cdot 5 \cdot 7$	0.2246	0.3856	0.6281	1.3534	0
$3 \cdot 5 \cdot 11$	0.2269	0.3949	0.6122	1.2929	0
$3 \cdot 7 \cdot 11$	0.2311	0.3962	0.6036	1.2525	0
$5 \cdot 7 \cdot 11$	0.2243	0.3483	0.5920	1.2051	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2222	0.3798	0.6172	1.3426	0

Table A.39
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 5 \cdot 7$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$7 \cdot 11$	0.2492	0.4289	0.5889	1.2201	0
$3 \cdot 5 \cdot 7$	0.2291	0.3876	0.6146	1.2864	0
$3 \cdot 5 \cdot 11$	0.2299	0.3787	0.5900	1.1940	0
$3 \cdot 7 \cdot 11$	0.2364	0.3924	0.5945	1.2073	0
$5 \cdot 7 \cdot 11$	0.2323	0.3922	0.5824	1.2107	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2268	0.3711	0.5983	1.2405	0

Table A.40
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 5 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 5 \cdot 7$	0.2336	0.3917	0.6186	1.2809	0
$3 \cdot 5 \cdot 11$	0.2378	0.4068	0.6072	1.2495	0
$3 \cdot 7 \cdot 11$	0.2388	0.4000	0.5940	1.2137	0
$5 \cdot 7 \cdot 11$	0.2400	0.4042	0.6004	1.2272	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2311	0.3854	0.6165	1.3009	0

Table A.41
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 7 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 5 \cdot 11$	0.2218	0.3692	0.6292	1.2641	0
$3 \cdot 7 \cdot 11$	0.2287	0.3870	0.6388	1.3220	0
$5 \cdot 7 \cdot 11$	0.2243	0.3684	0.6251	1.2701	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2192	0.3591	0.6487	1.3105	0

Table A.42
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 5 \cdot 7$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 7 \cdot 11$	0.2269	0.3681	0.6183	1.2112	0
$5 \cdot 7 \cdot 11$	0.2276	0.3777	0.6213	1.2869	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2218	0.3599	0.6304	1.2532	0

Table A.43
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 5 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$5 \cdot 7 \cdot 11$	0.2270	0.3665	0.6003	1.1796	0
$3 \cdot 5 \cdot 7 \cdot 11$	0.2281	0.3770	0.6348	1.2778	0

Table A.44
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 3 \cdot 7 \cdot 11$.

m_2	$\overline{\text{FWRD}}$	σ (FWRD)	$\overline{\text{QUEUE}}$	σ (QUEUE)	failures
$3 \cdot 5 \cdot 7 \cdot 11$	0.2238	0.3685	0.6247	1.3068	0

Table A.45
Four-prime racing statistics for FWRD and QUEUE, $m_1 = 5 \cdot 7 \cdot 11$.

VITA

Jason Gower was born on November 4th, 1973 in Tulsa, Oklahoma. He earned a B.S. in physics and a B.A. in mathematics from Truman State University in May 1997, and a M.S. from Purdue University in May 2003. He began his studies at Purdue University in August 1997.