UNIVERSITY OF CALGARY

Improved Exponentiation in the Ideal Class Group of Imaginary Quadratic Number Fields

With an Application to Integer Factoring

by

Maxwell Sayles

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE

DEGREE OF NAME OF DEGREE IN FULL

DEPARTMENT OF NAME OF DEPARTMENT

CALGARY, ALBERTA

June, 2013

Abstract

Paragraph 1

Paragraph 2

Paragragh 3

Acknowledgements

Paragraph 1

Paragraph 2

Paragraph 3

Table of Contents

List of Tables

List of Figures and Illustrations

List of Algorithms

Chapter 1

Motivation

1.1 Faster ideal exponentiation on imaginary quadratic fields

1.2 Exponentiation with fixed exponents

1.3 Faster class group computations

1.4 Applications in cryptography

1.5 Examples of fast ideal exponentiation in SuperSPAR

1.6 Contributions

1. A really fast implementation of the Extended Euclidean Algorithm for integers bound by 32, 64, and 128 bits.

2. Optimized implementations of ideal class arithmetic for discriminants bound by 64 and 128 bits.

3. An improvement in the wall clock running time to exponentiate in the ideal class group when the exponent is known in advance.

4. The fastest implementation that we tested for integer factoring in the range of 54bit integers to 62bit integers.

5. A library for optimized 32-bit, 64-bit, and 128-bit arithmetic is available at `https://www.github.com/maxwellsayles/liboptarith`

6. A library for arithmetic in the class group of imaginary quadratic number fields, specialized for 64-bit, 128-bit, and unbound discriminants is available at `https://www.github.com/maxwellsayles/libqform`

7. An integer factoring library (SuperSPAR) suitable for non-cryptographic sizes is available at `https://www.github.com/maxwellsayles/libsspar` (COMING SOON)

The software was developed using the GNU C compiler version 4.7.2 on Ubuntu 12.10. The hardware platform was a personal notebook with a 2.7GHz Intel Core i7-2620M CPU and 8Gb of memory. The CPU has four cores, only one of which was used during timing experiments.

1.7 Overview of Thesis

Chapter 2

Ideal Arithmetic

A focus of this thesis is arithmetic and exponentiation in the ideal class group of imaginary quadratic number fields. We begin with the relevant theory of quadratic number fields, then discuss quadratic orders and ideals of quadratic orders. Finally, we discuss arithmetic in the ideal class group. The theory presented here is available in detail in reference texts on algebraic number theory such as [14], [25], or [28].

2.1 Quadratic Numbers

A *quadratic number* is a root α of a quadratic polynomial $f(x) = ax^2 + bx + c$ with integer coefficients. The roots of $f(x)$ are given by the quadratic formula

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} .$$

The *discriminant* of $f(x)$ is $\Delta = b^2 - 4ac$, and a quadratic number field $\mathbb{K}$ can be constructed as an extension field of the rational numbers $\mathbb{Q}$ as

$$\mathbb{K} = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta}) = \{u + v\sqrt{\Delta} : u, v \in \mathbb{Q}\}.$$

We call Δ the *radicand* of $\mathbb{K}$. Notice that $\Delta \equiv 0, 1 \pmod 4$ and that if Δ is a perfect square, then $\mathbb{K} = \mathbb{Q}$. We are interested in the case that Δ is not a perfect square. Also, if $\Delta = f^2\Delta_0$ where Δ_0 is square free, then $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{\Delta_0})$. As such, Δ_0 or any square multiple of it can be used as the radicand of $\mathbb{K}$. When Δ is positive, $\mathbb{K}$ is a subset of the real numbers, $\mathbb{R}$, and is a *real* quadratic number field. When Δ is negative, $\mathbb{K}$ is a subset of the complex numbers, $\mathbb{C}$, and is an *imaginary* quadratic number field. This thesis only considers the imaginary case.

2.2 Quadratic Integers

A polynomial with a leading coefficient of 1 is a *monic* polynomial, and the root α of a monic polynomial $f(x)$ with integer coefficients is an *algebraic integer*. The rational numbers are degree 1 algebraic numbers since they are roots of degree 1 polynomials $bx - a$, and the roots of monic degree 1 polynomials with integer coefficients are the integers, $\mathbb{Z}$, sometimes called the *rational integers*. When $f(x)$ is a monic quadratic polynomial with integer coefficients, the root α is a *quadratic integer*.

Theorem 2.2.1. [31, Theorem 4.10] A quadratic integer α is an algebraic integer of $\mathbb{Q}(\sqrt{\Delta_0})$ where α can be written as $\alpha = x + y\omega_0$ for $x, y \in \mathbb{Z}$ where

$$\omega_0 = \begin{cases} \sqrt{\Delta_0} & \text{when } \Delta_0 \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{\Delta_0}}{2} & \text{when } \Delta_0 \equiv 1 \pmod 4. \end{cases}$$

2.3 Maximal Order of Algebraic Integers

The *maximal order* of a field $\mathbb{K}$ is the set of all algebraic integers contained within $\mathbb{K}$ and is characterized using a $\mathbb{Z}$-module.

Definition 2.3.1. Let $X = \{\xi_1, \xi_2, \xi_3, ..., \xi_n\}$ be a subset of a number field $\mathbb{K}$. In this case, a $\mathbb{Z}$-*module*, $\mathcal{M}$, is an additive Abelian group such that

$$\begin{aligned} \mathcal{M} &= [\xi_1, \xi_2, ..., \xi_n] \\ &= \xi_1\mathbb{Z} + \xi_2\mathbb{Z} + \cdots + \xi_n\mathbb{Z} \\ &= \left\{ \sum_i^n x_i\xi_i : x_i \in \mathbb{Z}, \xi_i \in X \right\}. \end{aligned}$$

Definition 2.3.2. A *quadratic order* $\mathcal{O}$ of $\mathbb{Q}(\sqrt{\Delta})$ is a sub-ring of the quadratic integers of $\mathbb{Q}(\sqrt{\Delta})$ containing 1. Following Jacobson and Williams [31, p.81], we write $\mathcal{O}$ as

$$\left[1, \frac{\Delta + \sqrt{\Delta}}{2}\right] = [1, f\omega_0].$$

The maximal order $\mathcal{O}_\Delta = [1, \omega_0]$ of $\mathbb{Q}(\sqrt{\Delta})$ is the ring of all quadratic integers in $\mathbb{Q}(\sqrt{\Delta})$, and is maximal since any order $\mathcal{O} = [1, f\omega_0]$ is a sub-ring of $\mathcal{O}_\Delta$.

2.4 Ideals of $\mathcal{O}_\Delta$

Definition 2.4.1. An *ideal* $\mathfrak{a}$ is an additive subgroup of an order $\mathcal{O}$ with the property that for any $a \in \mathfrak{a}$ and $\xi \in \mathcal{O}$, it holds that ξa and $a\xi$ are both elements of the ideal $\mathfrak{a}$.

When $\mathcal{O}_\Delta$ is a quadratic order, for $\alpha, \beta \in \mathcal{O}_\Delta$, the set $\mathfrak{a} = \{x\alpha + y\beta : x, y \in \mathcal{O}_\Delta\}$ is an ideal in the order $\mathcal{O}_\Delta$ and is denoted (α, β) [39, p.16]. Every ideal of a quadratic order $\mathcal{O}_\Delta$ can be represented by at most two generators [14, p.125–126, § 10], while some can be represented by a single generator. An ideal represented by a single generator is a *principal* ideal and is denoted $(\alpha) = \{x\alpha : x \in \mathcal{O}_\Delta\}$ [31, p.87].

For two ideals, $\mathfrak{a} = (\alpha_1, \beta_1)$ and $\mathfrak{b} = (\alpha_2, \beta_2)$ in $\mathcal{O}_\Delta$, their product is

$$\mathfrak{a}\mathfrak{b} = (\alpha_1\alpha_2, \alpha_1\beta_2, \beta_1\alpha_2, \beta_1\beta_2) = (\alpha_3, \beta_3) \tag{2.1}$$

for some $\alpha_3, \beta_3 \in \mathcal{O}_\Delta$ and is also an ideal in $\mathcal{O}_\Delta$. The principal ideal $(1) = \mathcal{O}_\Delta$ is the *identity* ideal since $\mathfrak{a} = \mathfrak{a}\mathcal{O}_\Delta = \mathcal{O}_\Delta\mathfrak{a}$. If there exists an ideal $\mathfrak{c}$ such that $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$, then $\mathfrak{a}$ *divides* $\mathfrak{b}$ and we write $\mathfrak{a} \mid \mathfrak{b}$. If the ideal $\mathfrak{a}$ divides the identity ideal $\mathcal{O}_\Delta$, then $\mathfrak{a}$ has an *inverse*, which is denoted $\mathfrak{a}^{-1}$. Finally, an ideal $\mathfrak{p} \neq (1)$ is *prime* when $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$ implies that either $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$. As such, a prime ideal is divisible only by the identity ideal and itself.

Theorem 2.4.2. [29, p.13] When $\mathcal{O}_\Delta = [1, f\omega_0]$ is an order of a quadratic field, a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ can be uniquely written as a two dimensional $\mathbb{Z}$-module

$$\mathfrak{a} = s\left[a, \frac{b + \sqrt{\Delta}}{2}\right]$$

for $a, b \in \mathbb{Z}, s > 0, a > 0$, $\gcd(a, b, (b^2 - \Delta)/4a) = 1$, $b^2 \equiv \Delta \pmod{4a}$, and b is unique mod $2a$.

Definition 2.4.3. For an ideal $\mathfrak{a} = s[a, (b+\sqrt{\Delta})/2]$, when $s \in \mathbb{Z}$, $\mathfrak{a}$ is an *integral* ideal, and when $s \in \mathbb{Q}$, $\mathfrak{a}$ is a *fractional* ideal. Finally, when $s = 1$, $\mathfrak{a}$ is a *primitive* ideal.

For a prime ideal $\mathfrak{p} \in \mathcal{O}_\Delta$ it can be shown [29, p.19] that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime integer $p \in \mathbb{Z}$. Let

$$\mathfrak{p} = s\left[a, \frac{b+\sqrt{\Delta}}{2}\right]$$

and it follows that either $s = p$ and $a = 1$, or $s = 1$ and $a = p$. In the first case $\mathfrak{p} = p\mathcal{O}_\Delta$, while in the second case, if there exists $b = \sqrt{\Delta} \pmod{4p}$, then $\mathfrak{p} = [p, (b+\sqrt{\Delta})/2]$. This follows since $\Delta = b^2 - 4ac$, $a = p$, and $b, c \in \mathbb{Z}$. As such $c = (b^2 - \Delta)/4p$ and $b^2 \equiv \Delta \pmod{4p}$.

The inverse of an ideal $\mathfrak{a} = s[a, (b+\sqrt{\Delta})/2]$ with $\gcd(a, b, (b^2-\Delta)/4a) = 1$ is given by [29, pp.14–15]

$$\mathfrak{a}^{-1} = \frac{s}{\mathcal{N}(\mathfrak{a})}\left[a, \frac{-b+\sqrt{\Delta}}{2}\right] \tag{2.2}$$

where $\mathcal{N}(\mathfrak{a}) = s^2 a$ is the norm of $\mathfrak{a}$ and is multiplicative. Notice that the resulting ideal $\mathfrak{a}^{-1}$ may be a fractional ideal. When $\mathcal{O}_\Delta$ is maximal, all ideals of $\mathcal{O}_\Delta$ have inverses, and the set of invertible ideals forms a group under ideal multiplication.

2.5 Ideal Class Group

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are *equivalent* if there exists $\alpha, \beta \in \mathcal{O}_\Delta$ such that $\alpha\beta \neq 0$ and $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$ [31, p.88]. We use $[\mathfrak{a}]$ to denote the *ideal class* of all ideals equivalent to the *representative* ideal $\mathfrak{a}$. The *ideal class group*, Cl_Δ, is the set of all equivalence classes of invertible ideals, with the group operation defined as the product of class representatives. By [14, p.136], the ideal class group is a finite Abelian group.

Our implementation uses the primitive ideal $\mathfrak{a} = [a, (b+\sqrt{\Delta})/2]$ as a representative for the ideal class $[\mathfrak{a}]$. Additionally, we maintain the value $c = (b^2 - \Delta)/4a$. The class group is represented by the discriminant Δ. Since an ideal class contains an infinitude of ideals, we work with reduced representatives. This also makes arithmetic faster, since the size of generators are typically smaller.

Subsection 2.5.1 defines the reduced form of a representative and gives an algorithm for finding the reduced form. For two reduced class representatives, Subsection 2.5.4 shows how to compute their product. Subsection 2.5.5 discusses how to perform multiplication such that the result is a reduced or almost reduced representative. This is then extended to the case of computing the square (Subsection 2.5.6) and cube (Subsection 2.5.7) of an ideal class.

2.5.1 Reduced Representatives

Definition 2.5.1. A primitive ideal $\mathfrak{a} = [a, (b + \sqrt{\Delta})/2]$ with $\Delta < 0$ is a *reduced* representative of the ideal class $[\mathfrak{a}]$ when $-a < b \leq a < c$ or when $0 \leq b \leq a = c$ for $c = (b^2 - \Delta)/4a$ [16, p.241]. Often, we refer to the ideal $\mathfrak{a}$ simply as being *reduced*.

Algorithm 2.1 Ideal Reduction

Input: An ideal class representative $\mathfrak{a}_1 = [a_1, (b_1 + \sqrt{\Delta})/2]$ and $c_1 = ({b_1}^2 - \Delta)/4a_1$.
Output: A reduced representative $\mathfrak{a} = [a, (b + \sqrt{\Delta})/2]$.

```
1: $(a, b, c) \leftarrow (a_1, b_1, c_1)$
2: while $a > c$ or $b > a$ or $b \leq -a$ do
3:     if $a > c$ then
4:         swap $a$ with $c$ and let $b \leftarrow -b$
5:     end if
6:     if $b > a$ or $b \leq -a$ then
7:         $b \leftarrow b'$ such that $-a < b' \leq a$ and $b' \equiv b \pmod{2a}$
8:         $c \leftarrow (b^2 - \Delta)/4a$
9:     end if
10: end while
11: if $a = c$ and $b < 0$ then
12:     $b \leftarrow -b$
13: end if
14: return $[a, (b + \sqrt{\Delta})/2]$
```

In an imaginary quadratic field, every ideal class contains exactly one reduced ideal [39, p.20]. There are several algorithms to compute a reduced ideal, many of which are listed in [30]. Here we present the algorithm we use. We adapt the work presented in [30, p.90] and [31, p.99]. If $\mathfrak{a} = [a, (b + \sqrt{\Delta})/2]$ is a representative of the class $[\mathfrak{a}]$ then

$$\mathfrak{b} = \left[-\mathcal{N}((b + \sqrt{\Delta})/2)/a, -(b - \sqrt{\Delta})/2\right] \tag{2.3}$$

is a representative of an equivalent class and can be verified by

$$\left(-(b-\sqrt{\Delta})/2\right)\mathfrak{a} = (a)\mathfrak{b}.$$

Simplifying Equation 2.3 gives

$$\mathfrak{b} = \left[\frac{b^2-\Delta}{4a}, \frac{-b+\sqrt{\Delta}}{2}\right].$$

Since $c = (b^2-\Delta)/4a$ we have

$$\mathfrak{b} = \left[c, \frac{-b+\sqrt{\Delta}}{2}\right]. \tag{2.4}$$

As such, the first step is to reduce a by setting $\mathfrak{a} = [c, (-b+\sqrt{\Delta})/2]$, if $a > c$. Then b is reduced since b is unique modulo $2a$. These steps are repeated while $\mathfrak{a}$ is not reduced. In the case that $a = c$, we use the absolute value of b, since by Equation 2.4 the ideals $[a, (b+\sqrt{\Delta})/2]$ and $[c, (-b+\sqrt{\Delta})/2]$ are equivalent. Algorithm 2.1 gives Pseudo-code.

2.5.2 Class Number

Using $|b| \le a$ from the definition of a reduced representative 2.5.1, $-\Delta = 4ac - b^2 \ge 4ac - a^2$, and using $a \le c$, it follows that $|b| \le a \le \sqrt{|\Delta|/3}$. Since a and b are bound and c is determined by a, b, and Δ, it follows that the number of ideal classes in the class group Cl_Δ is finite [31, p.153].

Definition 2.5.2. The number of ideal classes in the class group Cl_Δ is the *class number* and is denoted h_Δ [31, p.153].

Cohen [16, p.247] states a bound on the number of elements in the class group Cl_Δ as

$$h_\Delta < \frac{1}{\pi}\sqrt{|\Delta|}\log|\Delta| \text{ when } \Delta < -4, \tag{2.5}$$

and C. Siegel shows that $h_\Delta = |\Delta|^{1/2+o(1)}$ as $\Delta \to -\infty$ [16, p.247].

2.5.3 Inverse of Ideal Class

Recall from Equation 2.2 that the inverse of an ideal $\mathfrak{a} = [a, (b + \sqrt{\Delta})/2]$ is the (possibly fractional) ideal

$$\mathfrak{a}^{-1} = \frac{s}{\mathcal{N}(\mathfrak{a})}\left[a, \frac{-b+\sqrt{\Delta}}{2}\right].$$

As such, the ideals $\mathfrak{a}^{-1}$ and $[a, (-b + \sqrt{\Delta})/2]$ are equivalent since

$$(\mathcal{N}(\mathfrak{a}))\, \mathfrak{a}^{-1} = (s)\left[a, \frac{-b+\sqrt{\Delta}}{2}\right]$$

and both $s, \mathcal{N}(\mathfrak{a}) \in \mathcal{O}_\Delta$. The inverse of an ideal class $[\mathfrak{a}]$ for the representative $\mathfrak{a} = [a, (b + \sqrt{\Delta})/2]$ is then given by the representative $[a, (-b + \sqrt{\Delta})/2]$ and by Definition 2.5.1 is reduced. As such, computing the inverse of an ideal class is virtually free.

2.5.4 Ideal Class Multiplication

The ideal class group operation is multiplication of ideal class representatives. Given two representative ideals $\mathfrak{a} = [a_1, (b_1 + \sqrt{\Delta})/2]$ and $\mathfrak{b} = [a_2, (b_2 + \sqrt{\Delta})/2]$ in reduced form, the (non-reduced) product $\mathfrak{ab}$ is computed using

$$c_2 = ({b_2}^2 - \Delta)/4a_2,$$

$$s = \gcd(a_1, a_2, (b_1 + b_2)/2) = Ya_1 + Va_2 + W(b_1 + b_2)/2, \tag{2.6}$$

$$U = (V(b_1 - b_2)/2 - Wc_2) \bmod (a_1/s), \tag{2.7}$$

$$a = (a_1a_2)/s^2, \tag{2.8}$$

$$b = (b_2 + 2Ua_2/s) \bmod 2a, \tag{2.9}$$

$$\mathfrak{ab} = s\left[a, \frac{b+\sqrt{\Delta}}{2}\right].$$

The remainder of this subsection is used to derive the above equations. We adapt much of the presentation given in [31, pp.117,118]. Equation 2.1 for the product of two ideals, $\mathfrak{a}$ and $\mathfrak{b}$, using module notation is

$$\mathfrak{ab} = \left[a_1a_2, \frac{a_1b_2 + a_1\sqrt{\Delta}}{2}, \frac{a_2b_1 + a_2\sqrt{\Delta}}{2}, \frac{b_1b_2 + (b_1+b_2)\sqrt{\Delta} + \Delta}{4}\right]. \tag{2.10}$$

By the multiplicative property of the norm we have

$$\begin{aligned} N(\mathfrak{ab}) = s^2 a = N(\mathfrak{a})N(\mathfrak{b}) = a_1 a_2 \\ \Rightarrow \quad a = \frac{a_1 a_2}{s^2}, \end{aligned}$$

which gives Equation 2.8. Now, by the second term of equation (2.10) we know that $(a_1 b_2 + a_1\sqrt{\Delta})/2 \in \mathfrak{ab}$. It follows that there is some $x, y \in \mathbb{Z}$ such that

$$\frac{a_1 b_2 + a_1\sqrt{\Delta}}{2} = xsa + ys\left(\frac{b+\sqrt{\Delta}}{2}\right).$$

Equating irrational parts gives

$$\frac{a_1\sqrt{\Delta}}{2} = \frac{ys\sqrt{\Delta}}{2}.$$

Hence, $s \mid a_1$. Similarly, by the third and fourth terms of equation (2.10) we have $(a_2 b_1 + a_2\sqrt{\Delta})/2 \in \mathfrak{ab}$, which implies that $s \mid a_2$, and $(b_1 b_2 + (b_1+b_2)\sqrt{\Delta} + \Delta)/4 \in \mathfrak{ab}$, which implies that $s \mid (b_1+b_2)/2$.

By the second generator, $s(b+\sqrt{\Delta})/2$, of $\mathfrak{ab}$ and the entire right hand side of equation (2.10) there exists $X, Y, V, W \in \mathbb{Z}$ such that

$$\frac{sb + s\sqrt{\Delta}}{2} = Xa_1a_2 + Y\frac{a_1b_2 + a_1\sqrt{\Delta}}{2} + V\frac{a_2b_1 + a_2\sqrt{\Delta}}{2} + W\frac{b_1b_2 + (b_1+b_2)\sqrt{\Delta} + \Delta}{4}.$$

Grouping rational and irrational parts gives

$$\frac{sb + s\sqrt{\Delta}}{2} = \left(Xa_1a_2 + Y\frac{a_1b_2}{2} + V\frac{a_2b_1}{2} + W\frac{b_1b_2+\Delta}{4}\right) + \left(Y\frac{a_1}{2} + V\frac{a_2}{2} + W\frac{b_1+b_2}{4}\right)\sqrt{\Delta}. \tag{2.11}$$

Again, by equating irrational parts we have

$$\begin{aligned} \frac{s\sqrt{\Delta}}{2} &= \left(Y\frac{a_1}{2} + V\frac{a_2}{2} + W\frac{b_1+b_2}{4}\right)\sqrt{\Delta} \\ s &= Ya_1 + Va_2 + W\frac{b_1+b_2}{2}, \end{aligned} \tag{2.12}$$

which is the same as Equation 2.6. Since s divides each of a_1, a_2, and $(b_1+b_2)/2$, take $s = \gcd(a_1, a_2, (b_1+b_2)/2)$ to be the largest such common divisor.

It remains to compute $b \pmod{2a}$. Recall that $a = a_1a_2/s^2$. This time, by equating the rational parts of (2.11) we have

$$\begin{aligned}
\frac{sb}{2} &= Xa_1a_2 + Y\frac{a_1b_2}{2} + V\frac{a_2b_1}{2} + W\frac{b_1b_2+\Delta}{4} \\
b &= 2X\frac{a_1a_2}{s} + Y\frac{a_1b_2}{s} + V\frac{a_2b_1}{s} + W\frac{b_1b_2+\Delta}{2s} \\
b &\equiv Y\frac{a_1b_2}{s} + V\frac{a_2b_1}{s} + W\frac{b_1b_2+\Delta}{2s} \pmod{2a}.
\end{aligned} \tag{2.13}$$

This gives b. However, Equation (2.13) can be rewritten with fewer multiplies and divides. Equation (2.12) gives

$$\begin{aligned}
s &= Ya_1 + Va_2 + W\frac{b_1+b_2}{2} \\
1 &= Y\frac{a_1}{s} + V\frac{a_2}{s} + W\frac{b_1+b_2}{2s} \\
Y\frac{a_1}{s} &= 1 - V\frac{a_2}{s} - W\frac{b_1+b_2}{2s}.
\end{aligned}$$

Then substituting into Equation (2.13) gives

$$\begin{aligned}
b &\equiv b_2(1 - V\frac{a_2}{s} - W\frac{b_1+b_2}{2s}) + V\frac{a_2b_1}{s} + W\frac{b_1b_2+\Delta}{2s} && \pmod{2a} \\
&\equiv b_2 - V\frac{a_2b_2}{s} - W\frac{b_1b_2+{b_2}^2}{2s} + V\frac{a_2b_1}{s} + W\frac{b_1b_2+\Delta}{2s} && \pmod{2a} \\
&\equiv b_2 + V\frac{a_2(b_1-b_2)}{s} + W\frac{\Delta-{b_2}^2}{2s} && \pmod{2a} \\
&\equiv b_2 + V\frac{2a_2(b_1-b_2)}{2s} + W\frac{2a_2(\Delta-{b_2}^2)}{2a_2\cdot 2s} && \pmod{2a} \\
&\equiv b_2 + \frac{2a_2}{s}\left(V\frac{b_1-b_2}{2} + W\frac{\Delta-{b_2}^2}{4a_2}\right) && \pmod{2a}.
\end{aligned}$$

Let $c_2 = ({b_2}^2 - \Delta)/4a_2$ and $U = (V(b_1-b_2)/2 - Wc_2) \bmod (a_1/s)$ and we have

$$b \equiv b_2 + \frac{2a_2}{s}U \pmod{2a},$$

which completes the derivation of Equation 2.9. Note that the product ideal $\mathfrak{ab}$ is not a reduced representative and that the size of its coefficients can be as much as twice that of the ideal factors $\mathfrak{a}$ and $\mathfrak{b}$.

2.5.5 Fast Ideal Multiplication (NUCOMP)

Shanks [44] gives an algorithm for multiplying two ideal class representatives such that their product is reduced or almost reduced. The algorithm is known as NUCOMP and stands for "New COMPosition". This algorithm is often faster in practice as the intermediate numbers are smaller and the final product requires at most two[1] applications of the reduction operation to be converted to reduced form [31, pp.439–441]. The description of NUCOMP provided here is a high level description of the algorithm based on [31, pp.119-123].

Equations 2.6, 2.8, and 2.9 from the previous Subsection give a solution to the ideal product $\mathfrak{ab} = s[a, (b+\sqrt{\Delta})/2]$. We begin with the observation ([31, p.119]) that $(b/2)/a$ is roughly equal to the sU/a_1 where U is given by Equation 2.7. To see this, recall from Subsection 2.5.2 that a_1 is approximately $\sqrt{|\Delta|}$ in size, so $s^2/2a_1 \approx 1/\sqrt{|\Delta|}$ and

$$\frac{b}{2a} = \frac{b_2 + 2Ua_2/s}{2a_1a_2/s^2} = \frac{s^2b_2 + s2Ua_2}{2a_1a_2} = \frac{s^2b_2}{2a_1a_2} + \frac{sU}{a_1} \approx \frac{sU}{a_1}.$$

Following Jacobson and Williams [31, pp.120-121], we develop the simple continued fraction expansion of $sU/a_1 = \langle q_0, q_1, \ldots, q_i, \phi_{i+1}\rangle$ using the recurrences

$$q_i = \lfloor R_{i-2} \ / \ R_{i-1} \rfloor \tag{2.14}$$

$$R_i = R_{i-2} - q_iR_{i-1} \tag{2.15}$$

$$C_i = C_{i-2} - q_iC_{i-1} \tag{2.16}$$

until we have R_i and R_{i-1} such that

$$R_i < \sqrt{a_1/a_2}\ |\Delta/4|^{1/4} < R_{i-1}. \tag{2.17}$$

Initial values for the recurrence are given by

$$\begin{bmatrix} R_{-2} & R_{-1} \\ C_{-2} & C_{-1} \end{bmatrix} = \begin{bmatrix} sU & a_1 \\ -1 & 0 \end{bmatrix}.$$

[1]According to [31, p.441], experiments show that 88% of the time the resulting product requires no applications of the reduction operation, 12% of the time only one application is required, and very infrequently are two applications necessary.

Algorithm 2.2 NUCOMP – Fast Ideal Multiplication ([31, pp.441-443]).

```
Input: Reduced representatives $\mathfrak{a} = [a_1, (b_1 + \sqrt{\Delta})/2]$, $\mathfrak{b} = [a_2, (b_2 + \sqrt{\Delta})/2]$
    with $c_1 = ({b_1}^2 - \Delta)/4a_1$, $c_2 = ({b_2}^2 - \Delta)/4a_2$, and discriminant $\Delta$.
Output: A reduced or almost reduced representative $\mathfrak{ab}$.
 1: ensure $\mathcal{N}(\mathfrak{a}) < \mathcal{N}(\mathfrak{b})$ by swapping $\mathfrak{a}$ with $\mathfrak{b}$ if $a_1 < a_2$
 2: compute $s'$ and $V'$ such that $s' = \gcd(a_1, a_2) = Y'a_1 + V'a_2$ for $s', Y', V' \in \mathbb{Z}$
 3: $s \leftarrow 1$
 4: $U \leftarrow V'(b_1 - b_2)/2 \bmod a_1$
 5: if $s' \neq 1$ then
 6:     compute $s, V$, and $W$
        such that $s = \gcd(s', (b_1 + b_2)/2) = Vs' + W(b_1 + b_2)/2$ for $V, W \in \mathbb{Z}$
 7:     $(a_1, a_2) \leftarrow (a_1/s, a_2/s)$
 8:     $U \leftarrow (VU - Wc_2) \bmod a_1$
 9: end if
10: if $a_1 < \sqrt{a_1/a_2}\ |\Delta/4|^{1/4}$ then
11:     $a \leftarrow a_1 a_2$
12:     $b \leftarrow (2a_2U + b_2) \bmod 2a$
13:     return $[a, (b + \sqrt{\Delta})/2]$
14: end if
15: $\begin{bmatrix} R_{-2} & R_{-1} \\ C_{-2} & C_{-1} \end{bmatrix} \leftarrow \begin{bmatrix} U & a_1 \\ -1 & 0 \end{bmatrix}$
16: find $i$ such that $R_i < \sqrt{a_1/a_2}\ |\Delta/4|^{1/4} < R_{i-1}$ using the recurrences:
    $q_i = \lfloor R_{i-2} \ / \ R_{i-1} \rfloor$
    $R_i = R_{i-2} - q_i R_{i-1}$
    $C_i = C_{i-2} - q_i C_{i-1}$
17: $M_1 \leftarrow (R_i a_2 + C_i(b_1 - b_2)/2)/a_1$
18: $M_2 \leftarrow (R_i(b_1 + b_2)/2 - sC_i c_2)/a_1$
19: $a \leftarrow (-1)^{i+1}(R_i M_1 - C_i M_2)$
20: $b \leftarrow ((2(R_i a_2 - C_{i-1} a)/C_i) - b_2) \bmod 2a$
21: return $[a, (b + \sqrt{\Delta})/2]$
```

We then compute

$$
\begin{aligned}
M_1 &= \frac{R_i a_2 + sC_i(b_1 - b_2)/2}{a_1}, \\
M_2 &= \frac{R_i(b_1 + b_2)/2 - sC_i c_2}{a_1}, \\
a &= (-1)^{i+1}(R_i M_1 - C_i M_2), \\
b &= \left(\frac{2(R_i a_2/s - C_{i-1} a)}{C_i} - b_2 \right) \bmod 2a
\end{aligned}
\tag{2.18}
$$

for the reduced or almost reduced product $\mathfrak{ab} = [a, (b + \sqrt{\Delta})/2]$. Note that this procedure assumes that $\mathcal{N}(\mathfrak{a}) \geq \mathcal{N}(\mathfrak{b})$ and that if $a_1 < \sqrt{a_1/a_2}\ |\Delta/4|^{1/4}$ then R_{-1} and R_{-2} satisfy Equation 2.17 and we compute the product $\mathfrak{ab}$ as in the previous subsection without expanding the simple continued fraction sU/a_1. When $a_1 \geq \sqrt{a_1/a_2}\ |\Delta/4|^{1/4}$, at least one iteration of the recurrence 2.16 is performed and so $C_i \neq 0$ and there will not be a divide by zero in Equation 2.18.

Our implementation of fast ideal multiplication includes practical optimizations on the above technique. For example, by Equation 2.6, $s \mid a_1$ and $s \mid a_2$, so a_1 and a_2 are reduced modulo s throughout the computation. Also, Equation 2.6 computes $\gcd(a_1, a_2, (b_1 + b_2)/2)$. Following [26, Algorithm 6], this is separated into two parts: let $s = \gcd(a_1, a_2)$ and compute $\gcd(s, (b_1+b_2)/2)$ only when $s \neq 1$. Chapter 5 discusses practical optimizations for computing the greatest common divisor and the recurrences 2.14, 2.15, and 2.16. Finally, the first coefficient, Y, from Equation 2.6 is never used, and so it is not computed. See Chapter 6 for a more thorough treatment of our implementation of ideal class arithmetic. Pseudo-code is given in Algorithm 2.2.

2.5.6 Fast Ideal Squaring (NUDUPL)

When the two input ideals for multiplication are the same, as is the case when squaring, much of the arithmetic simplifies. For reduced ideals $\mathfrak{a} = [a_1, (b_1 + \sqrt{\Delta})/2]$ and $\mathfrak{b} = [a_2, (b_2 + \sqrt{\Delta})/2]$, we have $a_1 = a_2$ and $b_1 = b_2$. Equations 2.6 and 2.7 simplify to

$$s = \gcd(a_1, b_1) = Xa_1 + Yb_1$$
$$U = -Yc_1 \bmod (a_1/s).$$

One then computes the continued fraction expansion of sU/a_1, but using the bound

$$R_i < |\Delta/4|^{1/4} < R_{i-1}.$$

Computing the ideal class representative simplifies as well – we have

$$\begin{aligned} M_1 &= R_i, \\ M_2 &= \frac{R_i b_1 - sC_i c_1}{a_1}, \\ a &= (-1)^{i+1}({R_i}^2 - C_i M_2), \\ b &= \left(\frac{2(R_i a_1/s - C_{i-1} a)}{C_i} - b_1 \right) \bmod 2a. \end{aligned}$$

Pseudo-code for our implementation is given in Algorithm 2.3.

Algorithm 2.3 NUDUPL – Fast Ideal Squaring.

```
Input: Reduced representative $\mathfrak{a} = [a_1, (b_1 + \sqrt{\Delta})/2]$
    with $c_1 = ({b_1}^2 - \Delta)/4a_1$ and discriminant $\Delta$.
Output: A reduced or almost reduced representative $\mathfrak{a}^2$.
 1: compute $s$ and $Y$ such that $s = \gcd(a_1, b_1) = Xa_1 + Yb_1$ for $s, X, Y \in \mathbb{Z}$
 2: $a_1 \leftarrow a_1/s$
 3: $U \leftarrow -Yc_1 \bmod a_1$
 4: if $a_1 < |\Delta/4|^{1/4}$ then
 5:     $a \leftarrow {a_1}^2$
 6:     $b \leftarrow (2Ua_1 + b_1) \bmod 2a$
 7:     return $[a, (b + \sqrt{\Delta})/2]$
 8: end if
 9: $\begin{bmatrix} R_{-2} & R_{-1} \\ C_{-2} & C_{-1} \end{bmatrix} \leftarrow \begin{bmatrix} U & a_1 \\ -1 & 0 \end{bmatrix}$
10: Find $i$ such that $R_i < |\Delta/4|^{1/4} < R_{i-1}$ using the recurrences:
    $q_i = \lfloor R_{i-2}/R_{i-1} \rfloor$
    $R_i = R_{i-2} - q_i R_{i-1}$
    $C_i = C_{i-2} - q_i C_{i-1}$
11: $M_2 \leftarrow (R_i b_1 - sC_i c_1)/a_1$
12: $a \leftarrow (-1)^{i+1}({R_i}^2 - C_i M_2)$
13: $b \leftarrow (2(R_i a_1 + C_{i-1} a)/C_i) \bmod 2a$
14: return $[a, (b + \sqrt{\Delta})/2]$
```

2.5.7 Fast Ideal Cubing (NUCUBE)

When we consider binary-ternary representations of exponents, cubing is required. In general, if we want to compute $\mathfrak{a}^3$ for an ideal class representative $\mathfrak{a} = [a_1, (b_1 + \sqrt{\Delta})/2]$, we can take advantage of the simplification that happens when expanding the computation of $\mathfrak{a}^2\mathfrak{a}$.

Here we provide a high level description of a technique for cubing based on similar ideas to NUCOMP and NUDUPL, namely that of computing the quotients of a continued fraction expansion. A detailed description and analysis of this technique can be found in [26].

Similar to ideal squaring, compute integers s' and Y' such that

$$s' = \gcd(a_1, b_1) = X'a_1 + Y'b_1.$$

Note that X' is unused. If $s' \neq 1$, compute

$$s = \gcd(s'a_1, {b_1}^2 - a_1c_1) = Xs'a_1 + Y({b_1}^2 - a_1c_1)$$

for $s, X, Y \in \mathbb{Z}$. If $s' = 1$ then let $s = 1$ too. Then compute U using

$$U = \begin{cases} Y'c_1(Y'(b_1 - Y'c_1a_1) - 2) \bmod {a_1}^2 & \text{if } s' = 1 \\ -c_1(XY'a_1 + Yb_1) \bmod {a_1}^2/s & \text{otherwise.} \end{cases}$$

Next, develop the simple continued fraction expansion of $sU/{a_1}^2$ until

$$R_i < \sqrt{a_1}|\Delta/4|^{1/4} < R_{i-1}.$$

Finally, compute the representative $\mathfrak{a}^3 = [a, (b + \sqrt{\Delta})/2]$ using the equations

$$\begin{aligned} M_1 &= \frac{(R_ia_1 + C_iUa_1)}{{a_1}^2}, \\ M_2 &= \frac{R_i(b_1 + Ua_1) - sC_ic_1}{{a_1}^2}, \\ a &= (-1)^{i+1}R_iM_1 - C_iM_2, \\ b &= \left(\frac{2(R_ia_1/s - C_{i-1}a)}{C_i} - b_1\right) \bmod 2a. \end{aligned}$$

By [26, p.15 Theorem 5.1], the ideal $[a, (b+\sqrt{\Delta})/2]$ is at most two reduction steps from being reduced. Pseudo-code for our implementation of fast ideal cubing is given in Algorithm 2.4.

The next Chapter discusses some exponentiation techniques that use the ideal arithmetic presented in this chapter, namely fast multiplication, squaring, and cubing.

Algorithm 2.4 NUCUBE – Fast Ideal Cubing. Adapted from [26, p.26].

```
Input: A reduced representative $\mathfrak{a} = [a_1, (b_1 + \sqrt{\Delta})/2]$.
Output: A reduced or almost reduced representative $\mathfrak{a}^3$.
 1: compute $s'$ and $Y'$ such that $s' = \gcd(a_1, b_1) = X'a_1 + Y'b_1$ for $s', X', Y' \in \mathbb{Z}$
 2: if $s' = 1$ then
 3:     $s \leftarrow 1$
 4:     $U \leftarrow Y'c_1(Y'(b_1 - Y'c_1a_1) - 2) \bmod {a_1}^2$
 5: else
 6:     compute $s, X$, and $Y$ such that $s = \gcd(s'a_1, {b_1}^2 - a_1c_1) = Xs'a_1 + Y({b_1}^2 - a_1c_1)$ for
        $s, X, Y \in \mathbb{Z}$
 7:     $U \leftarrow -c_1(XY'a_1 + Yb_1) \bmod {a_1}^2/s$
 8: end if
 9: if ${a_1}^2/s < \sqrt{a_1}\ |\Delta/4|^{1/4}$ then
10:     $a \leftarrow {a_1}^3/s^2$
11:     $b \leftarrow (b_1 + 2Ua_1/s) \bmod 2a$
12:     return $[a, (b + \sqrt{\Delta})/2]$
13: end if
14: $\begin{bmatrix} R_{-2} & R_{-1} \\ C_{-2} & C_{-1} \end{bmatrix} \leftarrow \begin{bmatrix} U & ({a_1}^2/s) \\ -1 & 0 \end{bmatrix}$
15: Find $i$ such that $R_i < \sqrt{a_1}|\Delta/4|^{1/4} < R_{i-1}$ using the recurrences:
    $q_i = \lfloor R_{i-2}/R_{i-1} \rfloor$
    $R_i = R_{i-2} - q_iR_{i-1}$
    $C_i = C_{i-2} - q_iC_{i-1}$
16: $M_1 \leftarrow (R_ia_1 + C_iUa_1)/{a_1}^2$
17: $M_2 \leftarrow (R_i(b_1 + Ua_1) - sC_ic_1)/{a_1}^2$
18: $a \leftarrow (-1)^{i+1}R_iM_1 - C_iM_2$
19: $b \leftarrow (2(R_ia_1/s - C_{i-1}a)/C_i - b_1) \bmod 2a$
20: return $[a, (b + \sqrt{\Delta})/2]$
```

Chapter 3

Exponentiation

Exponentiation has many applications. Diffie-Hellman key exchange uses exponentiation so that two parties may jointly establish a shared secret key over an insecure channel. An application discussed in detail in this thesis is that of computing the order of a group element (see Sections 4.1 and 4.3). Our approach is to exponentiate a group element to the product, P, of several small primes. The result is an element whose order is likely to not be divisible by any of these primes. We then compute the order using a variant of Shanks' baby-step giant-step algorithm where only powers relatively prime to P are computed. Determining the order of an element is useful in computing the structure of a group, and in factoring an integer associated with a group. Faster exponentiation means the entire computation is faster.

In Sections 3.1 and 3.2 we discuss standard exponentiation techniques that rely on a base 2 representation of the exponent. In Section 3.3 we describe double-base number systems, which, as the name implies, are number systems that make use of two bases in the representation of a number. We are particularly interested in representations that use bases 2 and 3, since our implementation of ideal class group arithmetic provides multiplication, squaring, and cubing. In Section 3.4 we discuss some methods to compute double-base representations found in the literature. Throughout this chapter, the running time and space complexities are given in terms of the number of group operations and elements required. They do not take into consideration the binary costs associated with each.

3.1 Binary Exponentiation

The simplest method of exponentiation is binary exponentiation. Let g be an element in the group G and n a positive integer. To compute g^n, we first represent n in binary as

$$n = \sum_{i=0}^{\lfloor \log_2 n \rfloor} b_i 2^i$$

where $b_i \in \{0, 1\}$ such that b_i represents the i^{th} bit of n. We then represent g^n as

$$g^n = \prod_{i=0}^{\lfloor \log_2 n \rfloor} g^{b_i 2^i}.$$

and compute g^{2^i} by repeated squaring of g. The result, g^n, is the product of each g^{2^i} where $b_i = 1$. This description is known as right-to-left binary exponentiation because the result is computed by generating the terms of the product from right to left in the written binary representation of n. The left-to-right variant evaluates the bits of the exponent n from high order to lower order by repeatedly squaring an accumulator and multiplying this with the base element g when $b_i = 1$. The left-to-right variant has the advantage that one of the values in each multiplication, namely g, remains fixed throughout the evaluation. There also exist windowed variants where g^w is precomputed for each w in some window $0 \leq w < 2^k$ for some k (typically chosen to be cache efficient). The exponent n is then expressed in base 2^k. For further discussion of windowed techniques, see [13].

Binary exponentiation algorithms require $\lfloor \log_2 n \rfloor$ squarings and $(\lfloor \log_2 \ n \rfloor + 1)/2$ multiplications on average, since a multiplication is only necessary when $b_i = 1$ and the probability of $b_i = 1$ is $1/2$.

3.2 Non-Adjacent Form Exponentiation

The Non-Adjacent Form (NAF) of an integer is a *signed* base two representation such that no two non-zero terms in the representation are adjacent. Each integer, n, has a unique representation in non-adjacent form. Formally, an integer n is represented by

$$n = \sum_{i=0}^{\lfloor \log_2 n \rfloor + 1} s_i 2^i$$

where $s_i \in \{0, 1, -1\}$ and $s_i \cdot s_{i+1} = 0$. For example, suppose $n = 23814216$. In binary we have

$$23814216 = 2^3 + 2^6 + 2^{13} + 2^{14} + 2^{16} + 2^{17} + 2^{19} + 2^{21} + 2^{22} + 2^{24} \tag{3.1}$$

and in non-adjacent form we have

$$23814216 = 2^3 + 2^6 - 2^{13} - 2^{15} - 2^{18} - 2^{20} - 2^{23} + 2^{25}. \tag{3.2}$$

Similar to the binary case, we compute

$$g^n = \prod_{i=0}^{\lfloor \log_2 n \rfloor + 1} g^{s_i 2^i}.$$

When computing in the ideal class group, the cost of inversion is negligible, but when inversion is expensive, we can instead compute

$$g^n = \left(\prod_{i:s_i=1} g^{2^i} \right) \cdot \left(\prod_{i:s_i=-1} g^{2^i} \right)^{-1}$$

which requires at most one inversion (but this is not necessary for our purposes).

To compute the non-adjacent form of an integer n, inspect n two bits at a time from least significant to most significant. Let $n = \sum b_i 2^i$ be the binary representation of n and let $j = 0$. If the bit pattern $\langle b_{j+1}, b_j \rangle = \texttt{01}_2$ then let $s_j = 1$ and subtract 2^j from n. If $\langle b_{j+1}, b_j \rangle = \texttt{11}_2$ then let $s_j = -1$ and add 2^j to n. When the bit pattern $\langle b_{j+1}, b_j \rangle$ is $\texttt{00}_2$ or $\texttt{10}_2$, let $s_j = 0$. Next, increment j and repeat while $n \neq 0$.

In our experiments, we use a variation of the above, originally due to Reitwiesner [40], that maintains a carry flag c (see Algorithm 3.1). Instead of adding 2^i to n, set $c = 1$, and instead of subtracting 2^i from n, set $c = 0$. When inspecting n two bits at a time, we consider the bit pattern $(m + c) \bmod 4$ where $m = 2b_{i+1} + b_i$. This technique is faster since addition and subtraction is performed with constant sized integers.

Algorithm 3.1 Computes g^n using right-to-left non-adjacent form (Reitwiesner [40]).

```
Input: $g \in G, n \in \mathbb{Z}_{\geq 0}$
 1: $c \leftarrow 0$                                          {carry flag}
 2: $T \leftarrow g$                                          {invariant: $T = g^{2^i}$}
 3: $R \leftarrow 1_G$
 4: $i \leftarrow 0$
 5: while $n \geq 2^i$ do
 6:    if $\lfloor n/2^i \rfloor + c \equiv 1 \pmod 4$ then
 7:       $R \leftarrow R \cdot T$
 8:       $c \leftarrow 0$
 9:    else if $\lfloor n/2^i \rfloor + c \equiv 3 \pmod 4$ then
10:       $R \leftarrow R \cdot T^{-1}$
11:       $c \leftarrow 1$
12:    end if
13:    $T \leftarrow T^2$
14:    $i \leftarrow i + 1$
15: end while
16: if $c = 1$ then
17:    $R \leftarrow R \cdot T$
18: end if
19: return $R$
```

An advantage of non-adjacent form is that it requires at most $\lfloor \log_2 n \rfloor + 1$ squares and on average $(\lfloor \log_2 n \rfloor + 2)/3$ multiplications, as opposed to $(\lfloor \log_2 n \rfloor + 1)/2$ for binary exponentiation. To see this, recall that non-adjacent form requires that no two non-zero terms be adjacent. Consider any two adjacent terms. The possible outcomes are $(0, 0)$, $(s, 0)$, or $(0, s)$ where $s \in \{-1, 1\}$. This means that $2/3$ of the time, $1/2$ of the terms will be non-zero, and so the probability of any given term being non-zero is $1/3$.

3.3 Double-Base Number Systems

Binary representation and non-adjacent form use only a single base, namely base 2. Double-base number systems (DBNS), which were first introduced by Dimitrov and Cooklev [17, 18], use two bases. Given two coprime integers p and q and an integer n, we represent n as the sum and difference of the product of powers of p and q,

$$n = \sum_{i=1}^{k} s_i p^{a_i} q^{b_i} \tag{3.3}$$

where $s_i \in \{-1, 1\}$ and $a_i, b_i, k \in \mathbb{Z}_{\geq 0}$. This thesis pays particular attention to representations using bases $p = 2$ and $q = 3$ such that $n = \sum s_i 2^{a_i} 3^{b_i}$. Such representations are referred to as *2,3 representations.*

As an example of a 2,3 representation, consider the number $n = 23814216$ again. Given the bases $p = 2$ and $q = 3$, *one* possible representation of n is

$$23814216 = 2^3 3^3 - 2^4 3^5 + 2^5 3^6 + 2^7 3^7 + 2^9 3^8 + 2^{10} 3^9. \tag{3.4}$$

Another possible representation is

$$23814216 = 2^3 3^2 - 2^{13} 3^2 + 2^{15} 3^6. \tag{3.5}$$

There may be many possible 2,3 representations for a given number, and different representations will trade off between cubings, squarings, and the number of terms. Exponentiation using Equation 3.4 requires 10 squarings, 9 cubings, 1 inverse, and 5 multiplications, while Equation 3.5 requires 15 squarings, 6 cubings, 1 inverse, and 3 multiplications. Contrast this with the binary representation (3.1), which requires 24 squarings, 0 inverses, and 9 multiplications, and the non-adjacent form (3.2), which requires 25 squarings, 5 inverses, and 7 multiplications. The best representation will depend on the needs of the application and the cost of each operation. Later, we shall see some algorithms that take this into account (see Chapter 7), but many are designed to either find representations quickly, of a special form, or with few terms.

3.3.1 Chained 2,3 Representations

One way to classify algorithms that compute 2,3 representations is by the constraints placed on the partition of an integer n.

Definition 3.3.1. A *partition* of n is written $n = x_1 \pm x_2 \pm \cdots \pm x_k$ where the terms x_i are monotonically increasing by absolute value.

One such constraint is on the divisibility of subsequent terms.

Definition 3.3.2. A partition of an integer $n = x_1 \pm x_2 \pm \cdots \pm x_k$ is *chained* if every term x_i divides every term x_j for $i < j$ and $x_i \leq x_j$. A partition is said to be *strictly chained* if it is chained and x_i is *strictly* less than x_j for each $i < j$.

Binary and non-adjacent form are special types of strictly chained partitions, since for any two non-zero terms where $i < j$, we have $x_i = 2^i$, $x_j = 2^j$, $x_i \mid x_j$, and $x_i < x_j$. The 2,3 representation of $23814216 = 2^3 3^2 - 2^{13} 3^2 + 2^{15} 3^6$ is another example of a strictly chained partition, since $2^3 3^2 \mid 2^{13} 3^2 \mid 2^{15} 3^6$.

The benefit of restricting 2,3 representations to chained representations is the ease with which one can compute g^n when n is given as a chain. For example $g^{23814216} = g^{2^3 3^2 - 2^{13} 3^2 + 2^{15} 3^6}$ can be computed by first computing $x_0 = g$, $x_1 = g^{2^3 3^2}$, $x_2 = {x_1}^{2^{10}}$, $x_3 = {x_2}^{2^2 3^4}$, each term being computed by repeated squaring and cubing from the previous term. Finally $g^{23814216} = x_1 \cdot {x_2}^{-1} \cdot x_3$. When n is given as a chained 2,3 representation, Algorithm 3.2 will compute g^n using exactly a_k squares, b_k cubes, $k-1$ multiplications, and at most k inverses[1]. Since $x_i \mid x_{i+1}$, an implementation need only retain x_i in order to compute x_{i+1}, and so only requires storage of a constant number of group elements.

3.3.2 Unchained 2,3 Representations

There is evidence [26] that the shortest possible chained representations require a linear number of terms in relation to the size of the input. This is in contrast to unchained representations for which there are algorithms where the number of terms in the representation is

[1]Recall that when inversion is expensive, the product of terms with negative exponents can be computed separately from terms with positive exponents – the inverse is then computed only once for this product. Since computing inverses is negligible in the ideal class group, we instead compute the product of all terms directly.

Algorithm 3.2 Computes g^n given n as a chained 2,3 partition. Adapted from [20].

```
Input: $g \in G$, $n = \sum_{i=1}^{k} s_i 2^{a_i} 3^{b_i}$,
    $s_1, ..., s_k \in \{-1, 1\}$, $0 \leq a_1 \leq ... \leq a_k \in \mathbb{Z}$, $0 \leq b_1 \leq ... \leq b_k \in \mathbb{Z}$.
 1: $i \leftarrow 1$
 2: $a \leftarrow 0$                                  {current power of 2}
 3: $b \leftarrow 0$                                  {current power of 3}
 4: $T \leftarrow g$                                  {loop invariant: $T = g^{2^a 3^b}$}
 5: $R \leftarrow 1_G$
 6: while $i \leq k$ do
 7:   while $a < a_i$ do
 8:     $T \leftarrow T^2, a \leftarrow a + 1$
 9:   end while
10:   while $b < b_i$ do
11:     $T \leftarrow T^3, b \leftarrow b + 1$
12:   end while
13:   $R \leftarrow R \cdot T^{s_i}$                  {multiply with $T$ or $T^{-1}$}
14:   $i \leftarrow i + 1$
15: end while
16: return $R$
```

provably sublinear in the length of the input [19, 12], however, these algorithm still require $O(\log n)$ operations overall.

Given an unchained 2,3 representation for an integer $n = \sum s_i 2^{a_i} 3^{b_i}$, Méloni and Hasan [36, Section 3.2] give an algorithm that achieves the same bound on the number of operations as in algorithm 3.2, but with a bound of $O(\min\{\max a_i, \max b_i\})$ on the memory used. Suppose $\max b_i < \max a_i$ and that the terms are labelled and sorted such that $a_1 \geq ... \geq a_k$. The algorithm works by precomputing a table of $T_b = g^{3^b}$ for $0 \leq b \leq \max b_i$. Let $i = 1$ and begin with the first term $s_i 2^{a_i} 3^{b_i}$. Look up $T_{b_i} = g^{3^{b_i}}$ and, after applying the sign s_i, multiply ${T_{b_i}}^{s_i}$ with the running result. Let $a_\Delta = a_i - a_{i+1}$ when $i < k$ and $a_\Delta = a_k$ when $i = k$. Then square the running result a_Δ times. The algorithm then removes the term $s_i 2^{a_i} 3^{b_i}$ from the list of terms, and continues in this way with the next largest a_i. The algorithm terminates when there are no more terms in the list. Algorithm 3.3 gives pseudo-code for this approach and requires the storage of $O(\max b_i)$ group elements. When $\max a_i < \max b_i$, we use a related algorithm that requires the terms to be sorted such that $b_1 \geq ... \geq b_k$;

it precomputes $T_a = g^{2^a}$ for $0 \leq a \leq \max a_i$ and works similar to Algorithm 3.3 but with cubing and squaring appropriately swapped.

Algorithm 3.3 Computes g^n given n in 2,3 representation. Méloni [36, Section 3.2].

```
Input: $g \in G$, $n = \sum_{i=1}^{k} s_i 2^{a_i} 3^{b_i}$,
    $s_1, ..., s_k \in \{-1, 1\}$, $a_1 \geq ... \geq a_k \in \mathbb{Z}_{\geq 0}$, $b_1, ..., b_k \in \mathbb{Z}_{\geq 0}$.
1: $T_b \leftarrow g^{3^b}$ for $0 \leq b \leq \max\{b_1, ..., b_k\}$          {by repeated cubing}
2: $R \leftarrow 1_G$
3: $i \leftarrow 1$
4: while $i < k$ do
5:     $R \leftarrow R \cdot {T_{b_i}}^{s_i}$          {multiply with $T_{b_i}$ or ${T_{b_i}}^{-1}$}
6:     $a_\Delta \leftarrow a_i - a_{i+1}$
7:     $R \leftarrow R^{2^{a_\Delta}}$          {by squaring $a_\Delta$ number of times}
8:     $i \leftarrow i + 1$
9: end while
10: $R \leftarrow R \cdot {T_{b_k}}^{s_k}$
11: $R \leftarrow R^{2^{a_k}}$          {by squaring $a_k$ number of times}
12: return $R$
```

For example, the 2,3 representation $23814216 = 2^{15}3^6 - 2^8 3^5 - 2^4 3^6 + 2^3 3^3$ is sorted by decreasing a_i. The algorithm first computes $T_b = g^{3^b}$ for $0 \leq b \leq 6$. Note that it is sufficient to store only the values of $g^{3^{b_i}}$ that actually occur in terms (in this case T_3, T_5, and T_6). Let R_j represent the partial exponentiation of the first j terms with the largest a_i such that $g^{2^{a_{j+1}}}$ is factored out. Let $R_0 = 1_G$ and then compute

$$\begin{aligned}
R_1 &= (T_6)^{2^7} && \Rightarrow g^{2^7 3^6}, \\
R_2 &= \left(R_1 {T_5}^{-1}\right)^{2^4} && \Rightarrow g^{-2^4 3^5 + 2^{11} 3^6}, \\
R_3 &= \left(R_2 {T_6}^{-1}\right)^{2^1} && \Rightarrow g^{-2^1 3^6 - 2^5 3^5 + 2^{12} 3^6}, \\
R_4 &= (R_3 T_3)^{2^3} && \Rightarrow g^{2^3 3^3 - 2^4 3^6 - 2^8 3^5 + 2^{15} 3^6},
\end{aligned}$$

using 15 squares, 6 cubes, 2 inverses, and 3 multiplications. The result of the computation is $R_4 = g^{23814216}$ and the steps (executed from left-to-right, top-to-bottom) are depicted by figure 3.1.

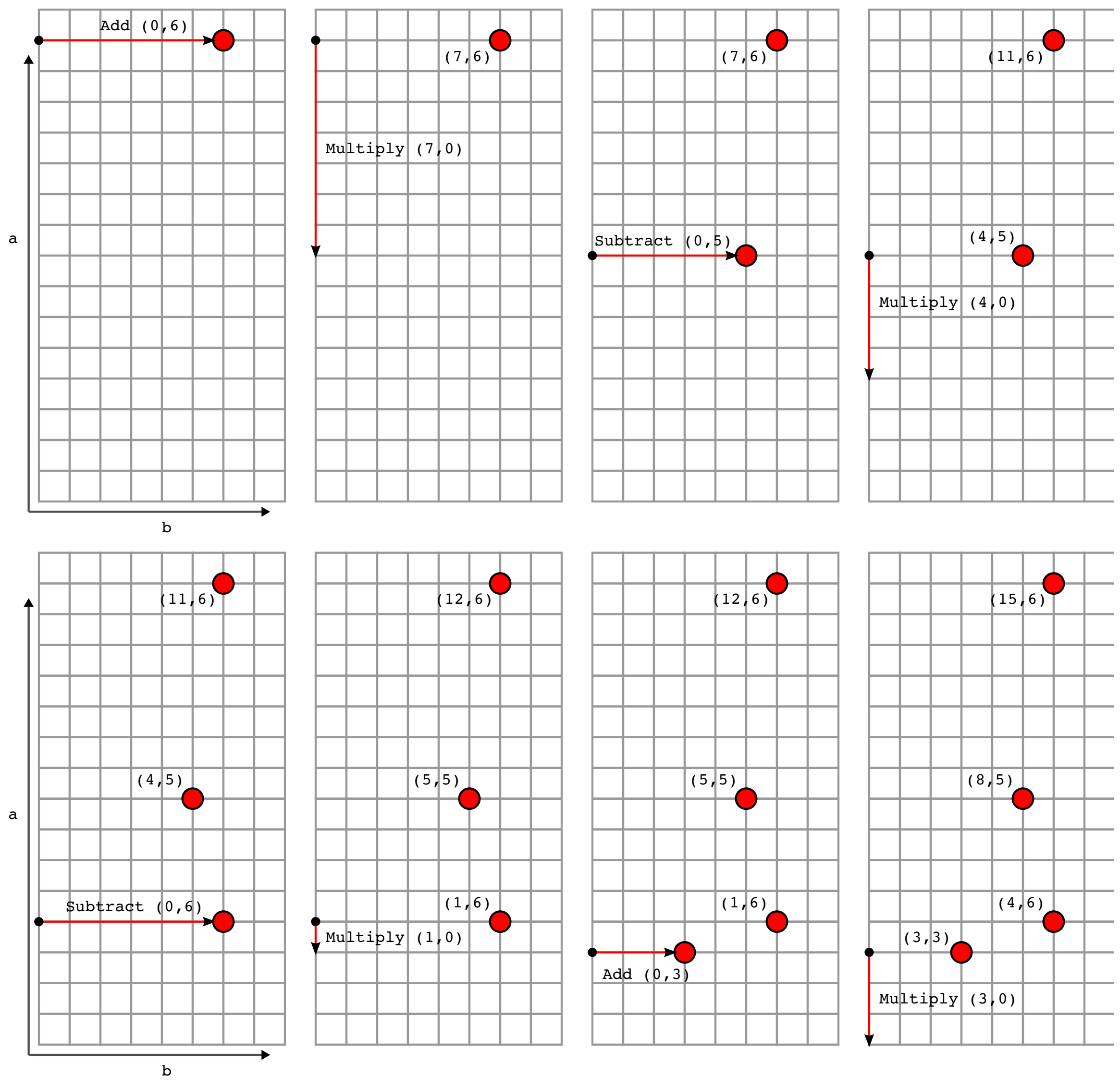


Figure 3.1: The construction of $2^{15}3^{6} - 2^{8}3^{5} - 2^{4}3^{6} + 2^{3}3^{3}$ using algorithm 3.3. Steps are executed from left-to-right, top-to-bottom.

3.4 Methods for Computing 2,3 Chains/Representations

The section discusses some of the methods from the literature for computing 2,3 representations. The first method generates strict chains from low order to high order (right-to-left), while the second method generates representations (both chained and unchained) from high order to low order (left-to-right). The third technique generates strict chains using a tree-based approach, while the final method computes additive only strict chains of shortest length in a manner similar to chains generated from low order to high order.

These methods trade off the time to compute a representation against the time to exponentiate using that representation. When the exponent is known in advance, one can precompute the chain or representation best suited to the application. Chapter 4 discusses two factoring algorithms that use precomputed representations of exponents to speed their computations. While none of the methods presented in this Chapter take into account the relative cost of multiplying, squaring, or cubing ideals, Chapter 7 looks at some variations that attempt to minimize the cost of exponentiation given the average costs of group operations.

3.4.1 Right-to-Left Chains (from low-order to high-order)

The first method we present computes a strictly chained 2,3 partition that is generated from low order to high order and is from Ciet et al [11]. We begin by recalling the technique for binary exponentiation that computes from low order to high order. Given an element $g \in G$ and an integer n, the function

$$\operatorname{bin}(g,n) = \begin{cases} 1 & \text{if } n = 0 \\ \operatorname{bin}(g, n/2)^2 & \text{if } n \equiv 0 \pmod 2 \\ \operatorname{bin}(g, n-1) \cdot g & \text{if } n \equiv 1 \pmod 2 \end{cases}$$

will compute the binary exponentiation of g^n from low order to high order. This algorithm repeatedly removes factors of 2 from n. When n is not divisible by 2, it subtracts 1 such that the input to the recursive call will be divisible by 2. The recursion terminates with the base case of $n = 0$.

This concept is extended to a 2,3 number system by repeatedly removing factors of 2 from n, and then factors of 3 from n. At this point, either $n \equiv 1 \pmod 6$ or $n \equiv 5 \pmod 6$. When $n \equiv 1 \pmod 6$, we recurse on $n - 1$ and the input will be divisible by both 2 and 3.

When $n \equiv 5 \pmod 6$, we recurse on $n+1$. Again, the input to the recursive call will be divisible by both 2 and by 3. Using this idea, we perform a 2,3 exponentiation recursively as

$$\text{rtl}(g,n) = \begin{cases} 1 & \text{if } n = 0 \\ \text{rtl}(g, n/2)^2 & \text{if } n \equiv 0 \pmod 2 \\ \text{rtl}(g, n/3)^3 & \text{if } n \equiv 0 \pmod 3 \\ \text{rtl}(g, n-1) \cdot g & \text{if } n \equiv 1 \pmod 3 \\ \text{rtl}(g, n+1) \cdot g^{-1} & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

Algorithm 3.4 implements a non-recursive function with group operations that correspond to those generated by the function rtl. The idea is as follows: let $a = 0$, $b = 0$, and $i = 1$. While $n > 0$, repeatedly remove factors of 2 from n and increment a for each factor of 2 removed. Then repeatedly remove factors of 3 from n and increment b for each factor of 3 removed. At this point, either $n \equiv 1 \pmod 6$ or $n \equiv 5 \pmod 6$ and so continue on $n-1$ or $n+1$ respectively. When we continue on $n-1$, this corresponds to adding the current term, so we set $s_i = 1$, and when we continue on $n+1$, this corresponds to subtracting the current term, so we set $s_i = -1$. Let $a_i = a$ and $b_i = b$ and then increment i and then repeat this process while $n > 0$. We then use Algorithm 3.2 to compute the exponentiation given the strictly chained 2,3 partition. When we are not able to precompute the chain, it is relatively straightforward to interleave the computation of the partition with the computation of the exponentiation, since the terms $s_i 2^{a_i} 3^{b_i}$ are computed in increasing order for $i = 1..k$.

To see the correctness of the above procedure, consider a modification to the recursive function rtl such that it returns a partition of the input n as a list of terms $s_i 2^{a_i} 3^{b_i}$. When the result of the recursive call is squared, this corresponds to incrementing a_i in each term of the list. Similarly, when the result is cubed, this corresponds to incrementing b_i in each term of the list. When the result is multiplied with g, we prepend a term of $+1$ to the partition, and when the result is multiplied with g^{-1}, we prepend a term of -1 to the partition. On

Algorithm 3.4 2,3 strict chains from low order to high order (Ciet et al [11]).

```
Input: $n \in \mathbb{Z}_{\geq 0}$
1: $(a, b) \leftarrow (0, 0)$
2: $i \leftarrow 1$
3: while $n > 0$ do
4:     while $n \equiv 0 \pmod 2$ do
5:         $n \leftarrow n/2, a \leftarrow a + 1$
6:     end while
7:     while $n \equiv 0 \pmod 3$ do
8:         $n \leftarrow n/3, b \leftarrow b + 1$
9:     end while
10:    if $n \equiv 1 \pmod 3$ then
11:        $n \leftarrow n - 1, s \leftarrow 1$
12:    else if $n \equiv 2 \pmod 3$ then
13:        $n \leftarrow n + 1, s \leftarrow -1$
14:    end if
15:    $(s_i, a_i, b_i) \leftarrow (s, a, b)$
16:    $i \leftarrow i + 1$
17: end while
18: $k \leftarrow i$
19: return $(a_1, b_1, s_1), ..., (a_k, b_k, s_k)$
```

each iteration of the loop, either $n \equiv 0 \pmod 2$ or $n \equiv 0 \pmod 3$, so either a increases or b increases. Since every term $|s_i 2^{a_i} 3^{b_i}|$ is strictly less than $|s_j 2^{a_j} 3^{b_j}|$ when $i < j$, the partition is strictly chained.

3.4.2 Left-to-Right Chains (from high-order to low-order)

The previous section gives a procedure for generating a strictly chained 2,3 partition for an integer n such that the terms are ordered from smallest absolute value to largest. Here we present a greedy approach, suggested by Berthé and Imbert [9], which generates the terms in order of the largest absolute value to the smallest. The idea is to find a term, $s2^a3^b$, that is closest to the remaining target integer n and then repeat on $n - s2^a3^b$. Let

$$\text{closest}(n) = s2^a3^b$$

such that $a, b \in \mathbb{Z}_{\geq 0}$ minimize $\big||n| - 2^a 3^b\big|$ and $s = -1$ when $n < 0$ and $s = 1$ otherwise. A recursive function to compute a 2,3 representation greedily is

$$\text{greedy}(n) = \begin{cases} 0 & \text{if } n = 0 \\ \text{closest}(n) + \text{greedy}(n - \text{closest}(n)) & \text{otherwise.} \end{cases}$$

Note that the representation generated may not be a chained partition. To generate a chained partition we restrict the maximum powers of 2 and 3 generated by the function closest. We bound the function closest, such that it returns the triple

$$\text{closest}'(n, A, B) = (s2^a 3^b, a, b)$$

where $0 \leq a \leq A$, $0 \leq b \leq B$, a and b minimize $\big||n| - 2^a 3^b\big|$, and $s = -1$ when $n < 0$ and $s = 1$ when $n > 0$. Our recursive function is then

$$\text{greedy}'(n, A, B) = \begin{cases} 0 & \text{if } n = 0 \\ v + \text{greedy}'(n - v, a, b) & \text{where } (v, a, b) = \text{closest}'(n, A, B). \end{cases}$$

We present pseudocode in Algorithm 3.5. Note that on successive invocations of greedy$'$, the absolute value of $v = |s2^a 3^b|$ returned by closest$'$ is monotonically decreasing. Reversing the terms of the partition gives a chained 2,3 partition of n that we can use to perform exponentiation using Algorithm 3.2.

Algorithm 3.5 Greedy left to right representations. Berthé and Imbert [9].

```
Input: $n, A, B \in \{\mathbb{Z}_{\geq 0}, +\infty\}$        {$+\infty$ for unbounded $a$ or $b$}
1: $L \leftarrow$ empty list
2: while $n \neq 0$ do
3:     compute integers $a$ and $b$ that minimize $\big||n| - 2^a 3^b\big|$
       such that $0 \leq a \leq A$ and $0 \leq b \leq B$
4:     $s \leftarrow -1$ when $n < 0$ and 1 otherwise
5:     push $(s, a, b)$ onto the front of $L$
6:     optionally set $(A, B) \leftarrow (a, b)$ when a chain is desired
7:     $n \leftarrow n - s2^a 3^b$
8: end while
9: return $L$
```

To compute the 2,3 term closest to n, a straightforward approach is to compute the set

$$V = \{2^a 3^b, 2^{a+1} 3^b : 0 \leq b \leq B \leq \lceil \log_3 |n| \rceil, a = \lfloor \log_2 |n/(3^b)| \rfloor \text{ when } a \leq A\}.$$

Then take the element $v \in V$ that is closest to $|n|$, and take $s \in \{-1, 1\}$ based on the sign of n. Since the set V contains $O(\log |n|)$ elements, computing the term closest to n by this method takes $\Omega(\log |n|)$ steps. When a and b are not constrained (i.e. $A \geq \lceil \log_2 |n| \rceil$ and $B \geq \lceil \log_3 |n| \rceil$), and we simply want to compute the 2,3 term closest to n, Berthé and Imbert [9] present a method that requires at most $O(\log \log |n|)$ steps.

They also found that applying a global bound A^* and B^* such that $0 \leq a \leq A^*$ and $0 \leq b \leq B^*$ often lead to representations with a lower density. In the unchained case, recursive calls to greedy$'$ use the global values of A^* and B^* rather than the values a and b generated by closest$'$. Finding the best greedy representation is then a matter of iterating over the global bounds A^* and B^* to compute 2,3 representations constrained appropriately. We discuss some of the results of this in Chapter 7.

3.4.3 Pruned Tree of ±1 Nodes

The next technique for finding strictly chained 2,3 partitions was suggested by Doche and Habsieger [21]. The idea is similar to the method for generating chains from right to left as described in Subsection 3.4.1 above, but this technique differs by generating multiple values that may be further reduced by powers of 2 and 3. The procedure is given in Algorithm 3.6. The idea is to maintain a tree, T, with at most L leaf nodes. At each iteration, each leaf node $v \in T$ generates two new leaves, $v - 1$ and $v + 1$, which are then reduced as much as possible by removing factors of 2 and 3. We then discard any duplicate nodes and all but the smallest L elements generated. The path from the root to the first leaf with a value of 1 represents a chained 2,3 partition of the number n.

Larger values of L sometimes produce chains with fewer terms, but take longer to compute. When the the input integer n is known in advance, this might not be a problem,

Algorithm 3.6 Chain from ± 1 Pruned Tree (Doche and Habsieger [21]).

```
Input: $n \in \mathbb{Z}_{>0}$ and a bound $L \in \mathbb{Z}_{>0}$.
 1: $T \leftarrow$ a binary tree on the node $n$
 2: while no leaf is 1 do
 3:    for all leaf nodes $v \in T$ do
 4:       insert as a left child $(v - 1)$ with all factors of 2 and 3 removed
 5:       insert as a right child $(v + 1)$ with all factors of 2 and 3 removed
 6:    end for
 7:    discard any duplicate leaves
 8:    discard all but the smallest $L$ leaves
 9: end while
10: return the chained 2,3 partition generated by the path from the root to the first leaf
    node containing 1
```

however, large values of L can still be prohibitively expensive. Empirically, the authors found that $L = 4$ was a good compromise between the length of the chain generated and the time to compute the chain.

3.4.4 Shortest Additive 2, 3 Chains

In the previous Subsection, the search for a 2,3 chain iterates on ± 1 the value of the L smallest candidates. When we further restrict a chain to contain only positive terms, the number of possible 2,3 chains is reduced. Imbert and Phillipe [27] consider searching for additive 2,3 strictly chained partitions that contain as few terms as possible. They give the following recursive function to compute the minimum number of terms in such a chain. Let $s(n)$ denote the smallest k such that n can be represented as $n = \sum_{i=1}^{k} 2^{a_i} 3^{b_i}$. We define

$s(n)$ as

$$s(n) = \begin{cases} \min\{s(n/3), s(n/2)\} & \text{when } n \equiv 0 \pmod 6 \\ 1 + s(n-1) & \text{when } n \equiv 1 \pmod 6 \\ s(n/2) & \text{when } n \equiv 2 \pmod 6 \\ \min\{s(n/3), 1 + s((n-1)/2)\} & \text{when } n \equiv 3 \pmod 6 \\ \min\{s(n/2), 1 + s((n-1)/3)\} & \text{when } n \equiv 4 \pmod 6 \\ 1 + s((n-1)/2) & \text{when } n \equiv 5 \pmod 6 \end{cases}$$

where the base cases are handled by $s(n) = 1$ when $n \leq 2$.

The corresponding 2,3 chain is computed by memoizing a shortest chain for each solution to $s(n)$ encountered. When a recursive call uses $n/2$, the chain for n is the chain for $n/2$ with each term multiplied by 2. Similarly, if the recursion uses $n/3$, each term is multiplied by 3. When the recursion uses $n - 1$, we simply add the term 1 to the chain representing $n - 1$.

3.5 Summary

This chapter outlined some exponentiation techniques from the literature. We started with binary exponentiation based on a binary representation of the exponent. Next we described non-adjacent form using a signed base 2 encoding of the exponent. Since cubing is often faster than combined multiplication with squaring, we discussed 2,3 number systems where an integer can have many representations as the sum of the products of 2 and 3. Exponentiation based on 2,3 representations fall under two classes: chained and unchained. Chained representations can typically be computed while interleaved with the exponentiation operation. They also require storage of only a constant number of group elements in addition to the input arguments. Unchained representations often have fewer terms or operations in their representation. Exponentiation of a group element using an unchained representation of the exponent can be performed using a linear number of group elements in the size of the exponent.

Coming up, Chapter 7 discusses several variations of chained and unchained 2,3 representations, many of which take into account the average time to multiply, square, and cube elements from the ideal class group. The actual performance of these variations guide our implementation of a factoring algorithm called “SuperSPAR”. In the next chapter, we provide the background for SPAR and the SuperSPAR factoring algorithm.

Chapter 4

SuperSPAR

One contribution of this thesis is to improve the speed of arithmetic in the ideal class group of imaginary quadratic number fields with an application to integer factoring. Chapter 2 describes the ideal class group, and Chapter 3 gives methods for exponentiation in generic groups. In this chapter, we make a connection between the two and that of integer factoring. Section 4.1 discusses an algorithm due to Schnorr and Lenstra [41], called SPAR, that uses the ideal class group to factor an integer associated with the discriminant. Section 4.2, discusses the primorial steps algorithm for order finding in generic groups that is asymptotically faster than both Pollard's rho method [38] and Shank's baby-steps giant-steps technique [43]. Finally, Section 4.3 reconsiders the factoring algorithm SPAR in the context of primorial steps for order finding. We call this new algorithm "SuperSPAR".

4.1 SPAR

SPAR is an integer factoring algorithm that works by finding a reduced ambiguous class with a discriminant associated with the integer to be factored. The algorithm was published by Schnorr and Lenstra [41], but was independently discovered by Atkin and Rickert who named it SPAR after Shanks, Pollard, Atkin, and Rickert [29, p.182].

4.1.1 Ambiguous Classes and the Factorization of the Discriminant

The description of SPAR uses binary quadratic forms. A binary quadratic form is a quadratic equation in two variables, x and y, such that

$$f(x,y) = ax^2 + bxy + cy^2$$

where a, b, and c are integer coefficients. For a given form there is a set of integers represented by $f(x,y)$ for integers x and y. Two forms are equivalent if the sets of integers they represent are identical [16, pp.239-240]. In which case, there exists an invertible integral linear change of variables that transforms one form into the other. Necessarily, two equivalent forms have the same discriminant, which is $\Delta = b^2 - 4ac$. The set of all forms equivalent to a given form comprises an equivalence class, and as shown by Gauß, representatives of equivalence classes of forms can be multiplied together to form a group. In the case of a negative discriminant, each form is equivalent to a unique reduced form [16, p.241].

The group of equivalence classes of binary quadratic forms is isomorphic to the ideal class group of imaginary quadratic fields (see Frölich and Taylor [22]). This thesis uses reduced representatives for elements of the ideal class group, and the equivalence class $[\mathfrak{a}]$ for a reduced representative $\mathfrak{a}$ is denoted using the $\mathbb{Z}$-module $\mathfrak{a} = [a, (b + \sqrt{\Delta})/2]$. In our implementation we also maintain a third term $c = (b^2 - \Delta)/4a$. We note that the variables a, b, and c correspond to the representative binary quadratic form $ax^2 + bxy + cy^2$ with discriminant Δ. As such, we adapt our discussion of the SPAR factoring algorithm to the language of ideal classes.

Definition 4.1.1. The *ambiguous classes* are the classes $[\mathfrak{a}]$ such that $[\mathfrak{a}]^2$ is the identity class [41, p.302]. Notice that the identity ideal class $[\mathcal{O}_\Delta] \in Cl_\Delta$ is an ambiguous class.

According to [41, p.303], every reduced representative of an ambiguous class with negative discriminant has either $b = 0$, $a = b$, or $a = c$. Since the discriminant is defined as $\Delta = b^2 - 4ac$, these reduced representatives correspond to a factorization of the discriminant. For a reduced ambiguous ideal class either

$$\begin{aligned}
\Delta &= 4ac && \text{when } b = 0, \\
\Delta &= b(b - 4c) && \text{when } a = b, \text{ or} \\
\Delta &= (b - 2a)(b + 2a) && \text{when } a = c.
\end{aligned}$$

Suppose we wish to find a factor of an odd integer N. Since $\Delta = b^2 - 4ac$ we must have $\Delta \equiv 0, 1 \pmod 4$. Therefore, for some square free integer k, let $\Delta = -kN$ when $-kN \equiv 1 \pmod 4$ and $\Delta = -4kN$ otherwise. Now to find a factor of N, we find a reduced ambiguous class representative with discriminant Δ. For a reduced ambiguous class representative, compute $d = \gcd(a, N)$ if $b = 0$ or $a = b$, and $d = \gcd(b - 2a, N)$ otherwise. If we are lucky, d is a proper factor of N. See Chapter 5 for a discussion on how to compute $\gcd(N, m)$.

4.1.2 SPAR Algorithm

Subsection 2.5.2 states that for a negative discriminant Δ, the ideal class group Cl_Δ has a finite number of elements. This means that for a random ideal class $[\mathfrak{a}]$, there exists an integer m such that $[\mathfrak{a}]^m = [\mathcal{O}_\Delta]$. We say that m is the *order* of the element $[\mathfrak{a}]$ and denote this by $m = \mathrm{ord}([\mathfrak{a}])$. When the order is even, then $[\mathfrak{b}] = [\mathfrak{a}]^{m/2}$ is an ambiguous ideal class. This follows from the fact that $[\mathfrak{b}]^2 = [\mathcal{O}_\Delta]$. Therefore, factoring an integer N reduces to the problem of determining the order of a random ideal class $[\mathfrak{a}] \in Cl_\Delta$ for Δ a square free multiple of $-N$ or $-4N$.

Definition 4.1.2. An integer, x, is *smooth* with respect to y if all of the prime factors dividing x are no larger than y.

The SPAR algorithm works in two stages. The first stage is the exponentiation stage, where a random ideal class $[\mathfrak{a}] \in Cl_\Delta$ is exponentiated to the product of many small odd prime powers E, such that $[\mathfrak{b}] = [\mathfrak{a}]^E$. Assuming the order of $[\mathfrak{b}]$ is even and smooth with respect to the exponent E, the algorithm then attempts to find an ambiguous ideal by repeated squaring of $[\mathfrak{b}]$. If this fails, the second stage is to perform a random walk on the group generated by the ideal class computed in the first stage. This is the search stage. We limit the number of group operations performed by each stage, and if both stages fail to find a factorization of N, we try again with a different square free multiple $\Delta = -kN$ or $\Delta = -4kN$. The use of a multiplier k changes the group structure and order of elements, and the hope is to find a group with smooth order.

Following Schnorr and Lenstra [41], we take the first t primes $p_1 = 2, p_2 = 3, ..., p_t \leq N^{1/2r}$ for $r = \sqrt{\ln N / \ln \ln N}$. Let $e_i = \max\{v : {p_i}^v \leq {p_t}^2\}$ and compute

$$[\mathfrak{b}] = [\mathfrak{a}]^{\prod_{i=2}^{t} {p_i}^{e_i}}.$$

Notice that we exponentiate $[\mathfrak{a}]$ to the product of only *odd* prime powers. The reason for this is that if $\mathrm{ord}([\mathfrak{a}])$ is smooth with respect to p_t, then we can compute $[\mathfrak{b}]^{\left(2^k\right)}$ for the smallest k such that $[\mathfrak{b}]^{\left(2^k\right)} = [\mathcal{O}_\Delta]$. It follows that $[\mathfrak{b}]^{\left(2^{k-1}\right)}$ is an ambiguous ideal class and we attempt to factor N.

Since we do not know if $\mathrm{ord}([\mathfrak{a}])$ is smooth, we instead bound k such that 2^k is no larger than the number of elements in the class group. Schnorr and Lenstra [41, p.291] use $k = \left\lfloor \log_2 \sqrt{N} \right\rfloor$. As such, we only need to compute $[\mathfrak{b}]^{\left(2^k\right)}$ for the smallest $k \leq \left\lfloor \log_2 \sqrt{N} \right\rfloor$ such that $[\mathfrak{b}]^{\left(2^k\right)} = [\mathcal{O}_\Delta]$ if such a k exists. If such a k does not exist, then the algorithm continues with the second stage.

In the first stage, we compute $[\mathfrak{b}] = [\mathfrak{a}]^{\prod_{i=2}^{t} {p_i}^{e_i}}$ and $[\mathfrak{c}] = [\mathfrak{b}]^{\left(2^k\right)}$. The second stage is a random walk through the cyclic group generated by the ideal class $[\mathfrak{c}]$ in an attempt to find the order $h = \mathrm{ord}([\mathfrak{c}])$. Let $\langle [\mathfrak{c}] \rangle$ denote the cyclic group generated by $[\mathfrak{c}]$ and let $f : \langle [\mathfrak{c}] \rangle \to \langle [\mathfrak{c}] \rangle$ be a function from one element in the cyclic group to another. The function f should have the property that if x is known for some $[\mathfrak{c}]^x$, then y can be determined for $[\mathfrak{c}]^y = f([\mathfrak{c}]^x)$. Let $[\mathfrak{c}_1] = [\mathfrak{c}]$ and repeatedly compute

$$[\mathfrak{c}_{i+1}] = f([\mathfrak{c}_i])$$

until there is some $j < k$ such that $[\mathfrak{c}_j] = [\mathfrak{c}_k]$. By the function f, we compute u and v such that $[\mathfrak{c}_j] = [\mathfrak{c}]^u$ and $[\mathfrak{c}_k] = [\mathfrak{c}]^v$. The order of $[\mathfrak{c}]$ is then a multiple of $h = v - u$. We compute an ambiguous class representative by computing $[\mathfrak{d}] = [\mathfrak{b}]^h$ and then compute $[\mathfrak{d}]^{\left(2^k\right)}$ for the smallest $k \leq \left\lfloor \log_2 \sqrt{N} \right\rfloor$ as before. Assuming that such a k exists, then $[\mathfrak{d}]^{\left(2^{k-1}\right)}$ is an ambiguous class representative and we attempt to factor N.

4.1.3 SPAR Complexity

The original publication of SPAR by Schnorr and Lenstra [41] claimed that every composite integer N could be factored in $o\left(\exp\sqrt{\ln N \ln\ln N}\right)$ bit operations. This was the first factoring algorithm for which this runtime had been conjectured, and it was also the first for which this conjecture had to be withdrawn [35].

The first stage of the algorithm exponentiates a random ideal class $[\mathfrak{a}] \in Cl_\Delta$ to the product $\prod_{i=2}^{t} {p_i}^{e_i}$ of the first t primes where $e_i = \max\{v : {p_i}^v \leq {p_t}^2\}$. Using binary exponentiation, this takes $O(p_t)$ group operations since there are about $p_t/\log p_t$ prime powers in the product, each of which is at most $\lceil 2\log_2 p_t \rceil$ in size. According to [41, p.290], for a random composite integer $m \in [0, N]$, this stage will factor m with probability $\geq r^{-r}$. Stage 2 performs a random walk of at most $O(p_t)$ group operations and with probability $\geq (r-2)^{-(r-2)}$ will factor m [41, p.290]. Their claim is that if Stage 1 is run on each integer kN for $k \leq r^r$, then every composite integer N will be factored within $o\left(\exp\sqrt{\ln N \ln\ln N}\right)$ bit operations.

This claim was based on a false assumption – for a complete discussion, see Lenstra and Pomerance [35, §11]. In short, the original assumption was that for fixed N and variable k, that the class number (h_Δ for $\Delta = -kN$) was as likely to be smooth with respect to some largest prime p_t as the class number associated with a random discriminant of approximately the same size. This assumption meant that one could take both k and p_t to be no larger than $N^{1/2r} = \exp\left(\frac{1}{2}\sqrt{\ln N \ln\ln N}\right)$, leading to an upper bound of $\exp\left(\sqrt{\ln N \ln\ln N}\right)$ for the expected running time. However, as Lenstra and Pomerance show [35, §11], this assumption is incorrect for a sufficiently dense sequence of integers.

4.2 Bounded Primorial Steps

The Bounded Primorial Steps algorithm [46] is an order finding algorithm for generic groups with asymptotic complexity $o(\sqrt{M})$ where M is a bound on the order of the group element.

This is asymptotically better than previously known order finding algorithms for generic groups, such as the Pollard-Brent method [10] and Shanks' baby-step giant-step method [43], both of which have complexity $O(\sqrt{M})$.

4.2.1 Shank's Baby-Step Giant-Step Method

The idea is similar to Shanks' baby-step giant-step method, which is as follows. For some element α in a group G and some bound M on the order of the element α, let $s = \left\lceil \sqrt{M} \right\rceil$ and compute $\alpha^1, \alpha^2, ..., \alpha^s$ storing each $\alpha^i \mapsto i$ in a table[1] – these are the baby steps. If any $\alpha^i = 1_G$, then $\text{ord}(\alpha) = i$ and we are finished. Otherwise compute $\alpha^{2s}, \alpha^{3s}, ...$ and for each α^{js}, if α^{js} is in the table then $\alpha^{js} = \alpha^i$ for some i and $js - i$ is a multiple of the order of α. These are the giant steps. Notice that s is chosen such that after an equal number of baby steps and giant steps, the last giant step has an exponent $s^2 \geq M$.

To see that this works, consider the order of the element α. Let $h = \text{ord}(\alpha)$. If $h \leq s$ then the algorithm finds some $\alpha^i = 1_G$ with $i \leq s$ during the baby steps. Otherwise, $h = js + i$ for some integer j and $i < s$, in which case the algorithm finds $\alpha^{js} = \alpha^i$ for some j, which implies $\alpha^{js-i} = 1_G$.

Following Sutherland [46, p.50], we point out that if computing the inverse of an element is cheaper than multiplying two elements, the number of multiplications is reduced by letting $s = \left\lceil \sqrt{M/2} \right\rceil$ and computing the giant steps $\alpha^{2s}, \alpha^{-2s}, \alpha^{4s}, \alpha^{-4s}, ...$ instead. Again, if the order $h \leq s$, we find some $\alpha^i = 1_G$ during the baby steps. Otherwise, either $h = 2js - i$ or $h = 2js + i$ for $i \leq s$. In the first case, there is some $\alpha^{2js} = \alpha^i$, which implies $\alpha^{2js-i} = 1_G$, and in the second case, there is some $\alpha^{-2js} = \alpha^i$, which implies $\alpha^{2js+i} = 1_G$.

4.2.2 Bounded Primorial Steps Algorithm

Sutherland observed [46, p.56] that if $h = \text{ord}(\alpha)$ is odd, then computing only odd powers $\alpha^1, \alpha^3, ..., \alpha^{s-1}$ for the baby steps is sufficient. We still need to compute giant steps $\alpha^{2s}, \alpha^{3s}, ...,$

[1]The table maps group elements α^i to exponents i.

for some s that is even since we want to find some $\alpha^{js} = \alpha^i$ where $js - i$ is odd. In this case, $s = \left\lceil \sqrt{2M} \right\rceil$ so that after roughly $\sqrt{M/2}$ baby steps and $\sqrt{M/2}$ giant steps, the last giant step has exponent $\geq M$.

The problem is that $\operatorname{ord}(\alpha)$ may not be odd. However, by repeated squaring of α it is easy to find an element whose order is guaranteed to be even [46, p.56]. Given a bound M on the group order, compute $\beta = \alpha^{2^\ell}$ where $\ell = \lfloor \log_2 M \rfloor$ and now run the modified algorithm on β to find $h' = \operatorname{ord}(\beta)$. The order of α can be found by computing $\zeta = \alpha^{h'}$ and then repeatedly squaring ζ until $\zeta^{2^k} = 1_G$ for some k. The order of α is then $2^k h'$.

Algorithm 4.1 Primorial Steps (Sutherland [46, p.57]).

```
Input: $\alpha \in G$, a bound $M \geq \operatorname{ord}(\alpha)$, and a fast order algorithm $\mathcal{A}(\alpha, E)$.
 1: maximize $w$ such that $P_w \leq \sqrt{M}$
 2: maximize $m$ such that $m^2 P_w \phi(P_w) \leq M$
 3: $s = mP_w$
 4: $E = \prod_{i=1}^{n} p_i^{\lfloor \log_{p_i} M \rfloor}$
 5: $\beta \leftarrow \alpha^E$
 6: for $i$ from 1 to $s$ where $i$ is coprime to $P_w$ do
 7:    compute $\beta^i$ and store $\beta^i \mapsto i$ in the table          {baby steps}
 8:    if $\beta^i = 1_G$ then
 9:       return $i \cdot \mathcal{A}(\alpha^i, E)$
10:    end if
11: end for
12: for $j = 2s, 3s, ...$ do
13:    if $\beta^j$ is in the table then
14:       lookup $\beta^j \mapsto i$ from the table                      {giant steps}
15:       $h' = j - i$
16:       return $h' \cdot \mathcal{A}(\alpha^{h'}, E)$
17:    end if
18: end for
```

This approach is extended to computing $\beta = \alpha^E$ where $E = 2^{\lfloor \log_2 M \rfloor} 3^{\lfloor \log_3 M \rfloor}$ and the order of β is coprime to both 2 and 3. In this case, compute baby steps with exponents coprime to 6 and giant steps that are a multiple of 6. More generally, this works for any primorial P_w such that

$$P_w = 2 \times 3 \times \cdots \times p_w = \prod_{i=1}^{w} p_i$$

where p_i is the i^{th} prime. Following Sutherland [46, p.57], select the largest $P_w \leq \sqrt{M}$ and then maximize m such that $m^2 P_w \phi(P_w) \leq M$, where $\phi(P_w)$ is the number of integers coprime to P_w given as

$$\phi(P_w) = (2-1) \times (3-1) \times \cdots \times (p_w - 1) = \prod_{i=1}^{w} (p_i - 1). \tag{4.1}$$

Let $e_i = \lfloor \log_{p_i} M \rfloor$ for $1 \leq i \leq w$ and $E = 2^{e_2} \times 3^{e_3} \times \cdots \times {p_w}^{e_w}$. Then compute $\beta = \alpha^E$. The bound on the largest baby step is $s = mP_w$, and we compute $h' = \text{ord}(\beta)$ by taking at most $m\phi(P_w)$ baby steps coprime to P_w and at most $m\phi(P_w)$ giant steps of size mP_w. Pseudo-code for the bounded Primorial Steps technique is given in Algorithm 4.1. By [46, p.59 Proposition 4.2], the number of group operations in the worst case is bound by $O(\sqrt{M/\log\log M})$.

To compute $h = \text{ord}(\alpha)$ given $h' = \text{ord}(\beta)$, one uses a fast order finding algorithm. One fast order finding algorithm, $\mathcal{A}(\alpha^{h'}, E)$, uses the factorization of $E = \prod {p_i}^{e_i}$. Notice that $\alpha^{Eh'} = \beta^{h'} = 1_G$. The idea is to iterate on the factors of E, removing each factor p before computing $\zeta = \alpha^{E'h'}$ for the product $E' = E/p$. If $\zeta \neq 1_G$, then $\text{ord}(\alpha)$ does not divide $E'h'$ and p must be a factor of the order of α. The algorithm then continues with the next prime factor of E'. Additional fast order finding algorithms are given in [46, Chapter 7].

4.2.3 Primorial Steps for a Set

Suppose the success of a computation is not limited to computing the order of a single element, but that the order of any element from a set of groups will work. Let $\{\alpha_i \in G_i\}$ be a set of elements from different groups such that the order of α_i is distributed uniformly at random on the interval $[1, M]$ where M is a bound on the largest order of the elements α_i. When the order of any element α_i from the set will suffice, Sutherland [46, §5.4] gives an algorithm with subexponential complexity.

Recall that an integer x is y-smooth if none of its prime factors are larger than y. By [46, p.81], the probability that a random integer x is $x^{1/u}$ smooth is $u^{-u+o(1)}$. Assuming that there is some α_i such that $\mathrm{ord}(\alpha_i)$ is $M^{1/u}$ smooth, we let $M' = M^{2/u}$ and attempt to compute $\mathrm{ord}(\alpha_i)$ using M' as a bound for the bounded primorial steps algorithm. This will use $o(M^{1/u})$ group operations[2]. If the algorithm fails to find the order of α_i, we try again for the next α_{i+1} in the set. Using this approach, according to [46, pp.81–82] the expected running time to find the order of some α_i is approximately

$$u^{u+o(1)}M^{1/u} = \exp\left(\frac{1}{u}\log M + u\log u + o(1)\right).$$

The cost is minimized for $u \approx \sqrt{2\log M/\log\log M}$, which gives an expected running time of

$$\exp\left(\left(\sqrt{2} + o(1)\right)\sqrt{\log M \log\log M}\right).$$

Notice that the idea behind the SPAR factoring algorithm is to find an ambiguous ideal for one of the class groups with valid discriminant $\Delta = -kN$ for $1 \le k \le r^r$ where $r = \sqrt{\ln N/\ln\ln N}$. In this case, the success of splitting a composite integer N is not limited to finding an ambiguous ideal within a single group, but instead to finding an ambiguous ideal from any of several groups. As such, we directly apply the above approach to that of the SPAR factoring algorithm.

4.3 SuperSPAR

Here we introduce SuperSPAR – an integer factoring algorithm and our motivation for improving the performance of exponentiation in the ideal class group. Let N be the odd integer we wish to factor. For some square free integer k, choose a discriminant $\Delta = -kN$ or $\Delta = -4kN$ such that $\Delta \equiv 0, 1 \pmod 4$. Similar to SPAR, SuperSPAR attempts to find an ambiguous class in Cl_Δ that splits N. SuperSPAR uses two stages, the first of which is the same as SPAR.

[2]This is $o(M^{1/u})$ operations since the bounded primorial steps algorithm uses $o(\sqrt{M'})$ operations for a bound M' on the order of an element.

Stage 1 takes the first t primes $p_1 = 2, p_2 = 3, ..., p_t \leq N^{1/2r}$ for $r = \sqrt{\ln N / \ln \ln N}$, sets $e_i = \max\{v : {p_i}^v \leq {p_t}^2\}$, lets $E = \prod_{i=2}^{t} {p_i}^{e_i}$ be the product of the odd prime powers, and then computes $[\mathfrak{b}] = [\mathfrak{a}]^E$ for a random ideal class $[\mathfrak{a}]$. Finally, it computes $[\mathfrak{c}] = [\mathfrak{b}]^{\left(2^k\right)}$ for $k = \left\lfloor \log_2 \sqrt{|\Delta|} \right\rfloor$. If $[\mathfrak{b}] = [\mathcal{O}_\Delta]$, then $\operatorname{ord}([\mathfrak{a}])$ divides E and is odd, and the algorithm tries again with a different random ideal class $[\mathfrak{a}]$. If the odd part of $\operatorname{ord}([\mathfrak{a}])$ divides E and the order of $[\mathfrak{a}]$ is even, then there is some $[\mathfrak{b}]^{\left(2^j\right)}$ for $0 \leq j < k$ that is an ambiguous ideal and we attempt to factor the discriminant Δ. Failing this, SuperSPAR continues with Stage 2.

Stage 2 of SuperSPAR differs from that of SPAR. SPAR attempts to find the order of $[\mathfrak{c}]$ by performing a random walk and using $O(p_t)$ group operations. Schnorr and Lenstra [41, p.294] suggest a Pollard-Brent Recursion [10] based on Pollard's rho method [38], but also remark [41, p.298] that Shanks' baby-step giant-step method [43] could be used to deterministically find $\operatorname{ord}([\mathfrak{c}])$. They point out that this approach could be made faster by exploiting the fact that $\operatorname{ord}([\mathfrak{c}])$ is likely to have no prime divisors $p_1, ..., p_t$, and this is precisely what SuperSPAR does.

Stage 2 of SuperSPAR attempts to find the order of $[\mathfrak{c}]$ by taking baby steps coprime to some primorial, and then giant steps that are a multiple of that primorial. First maximize w such that $\phi(P_w) \leq p_t$, then let $m = \lfloor p_t / \phi(P_w) \rfloor$ and $s = mP_w$. Notice that s is a multiple of the primorial P_w and that the number of baby steps is $d = m\phi(P_w) \leq p_t$. Then take baby steps $[\mathfrak{c}]^i$ for $1 \leq i \leq s$ with i coprime to P_w, followed by giant steps $[\mathfrak{c}]^j$ for $j = 2s, -2s, 4s, -4s, ..., 2sd, -2sd$[3]. Taking an equal number of giant steps as baby steps means that this stage of SuperSPAR uses $O(p_t)$ group operations (not counting inversions).

If Stage 2 successfully computes $h' = \operatorname{ord}([\mathfrak{c}])$ and assuming that $\operatorname{ord}([\mathfrak{b}])$ is even, we compute an ambiguous ideal by repeated squaring of $[\mathfrak{b}]^{h'}$ and then attempt to factor the integer associated with the discriminant. If the order is odd, however, then the algorithm runs Stage 1 again with a different random ideal class $[\mathfrak{a}]$. If Stage 2 fails to compute the

[3]We use this sequence of giant steps since computing the inverse in the ideal class group is essentially free.

order of $[\mathfrak{c}]$, the algorithm tries again with a different square free multiplier k.

4.3.1 SuperSPAR in Practice

In both SPAR and SuperSPAR, each stage uses $O(p_t)$ group operations where $p_t \approx N^{1/2r}$ and $r = \sqrt{\ln N / \ln \ln N}$. The value for r is chosen to theoretically minimize the expected running time of the algorithm. However, the value for r relates to the likelihood that the algorithm will find an ambiguous ideal class for a given discriminant[4]. Since r is chosen to minimize the expected running time in theory, in practice other values may be more efficient, effectively trading off the number of group operations used for each class group against the number of class groups tried.

Furthermore, balancing both stages of SuperSPAR to use $O(N^{1/2r})$ group operations is not ideal. This is partly because the actual cost of multiplication, squaring, and cubing differ, but also because the success of each stage depends on different properties of the class number. The exponentiation stage is successful when the order of a random ideal class is smooth with respect to some primorial E, while the search stage is successful when the non-smooth part of the order is sufficiently small. In this sense, the efficiency of the factoring algorithm depends both on the smoothness of the order of a random ideal class $[\mathfrak{a}]$ with respect to the primorial E, but also on the size of its non-smooth part with respect to the largest exponent reached by the search stage. Selecting bounds for each stage independently of r varies the time spent during each stage inversely to the probability of its success.

Experimentally we found that the prime factorization of the order of ideal classes consists of prime powers with exponents that are typically 1 for all but the smallest primes (see Subsection 8.2.1). Schnorr and Lenstra [41, p.293] also advise the use of smaller exponents in practice. Additionally, we found that the order of an ideal class $[\mathfrak{a}_1]$ was, with high probability (about 96.9% in our experiments), either the same as or a multiple of the order of some other ideal class $[\mathfrak{a}_2]$ in the same class group (see Subsection 8.2.2). For this reason,

[4]The assumption is that the order of a random ideal class is $N^{1/2r}$ smooth with probability r^{-r}.

if the algorithm finds some h' such that $[\mathfrak{a}_1]^{h'\left(2^j\right)}$ is an ambiguous class for some j, but is unsuccessful at factoring N, the algorithm simply attempts to find an ambiguous class by repeated squaring of $[\mathfrak{a}_i]^{h'}$ for several $[\mathfrak{a}_i]$. If this fails for several ideal classes, the algorithm then starts over with a different multiplier k for the discriminant. Let c be the maximum number of ideal classes tried.

Assuming good parameters are known, the SuperSPAR factoring algorithm used in practice is given in listing 4.2. Chapter 8 discusses the experiments and results that lead to parameters for this algorithm that perform well in practice. Notice, that parameters for Algorithm 4.2 can be selected based on the theoretical analysis of SuperSPAR from the previous section.

4.4 Summary

This chapter introduced SuperSPAR, a factoring algorithm based on the ideal class group and our motivation for practical improvements to the performance of arithmetic in the class group. The next two chapters discuss several techniques used to improve performance, as well as our experiments and results. Following that, Chapter 8 discusses techniques, experiments, and results used to improve the performance of SuperSPAR in practice.

Algorithm 4.2 SuperSPAR Integer Factoring Algorithm.

```
Input: $N \in \mathbb{Z}_{\geq 0}$ odd and composite,
    $E = \prod_{i=2}^{t} {p_i}^{e_i}$ for the exponentiation phase,
    $m$ a multiplier of the primorial $P_w$ for the search phase,
    $c \in \mathbb{Z}_{>0}$ the number of ideal classes to try before switching multipliers.
 1: $s = mP_w$
 2: $k \leftarrow 0$                    {the next line sets $k$ to 1 on the first run}
 3: $k \leftarrow$ smallest square free integer $> k$
 4: $\Delta \leftarrow -kN$
 5: $\Delta \leftarrow 4\Delta$ if $\Delta \not\equiv 0, 1 \pmod 4$
 6: $[\mathfrak{a}_1], [\mathfrak{a}_2], ..., [\mathfrak{a}_t]$ are the first $t$ prime ideal classes in $Cl_\Delta$
 7: {– exponentiation stage –}
 8: $[\mathfrak{b}] \leftarrow [\mathfrak{a}_1]^E$    {compute $[\mathfrak{b}]^{\left(2^{\lfloor \log_2 h_\Delta \rfloor}\right)}$ and test for an ambiguous ideal class}
 9: for $1 \leq k \leq \lfloor \log_2 h_\Delta \rfloor$ do
10:   if $[\mathfrak{b}]$ is an ambiguous ideal class then
11:     $h \leftarrow E$, then go to line 30
12:   end if
13:   $[\mathfrak{b}] \leftarrow [\mathfrak{b}]^2$
14: end for
15: {– search stage –}
16: clear the lookup table
17: for $1 \leq i \leq s$ where $\gcd(i, P_w) = 1$ do
18:   compute $[\mathfrak{b}]^i$ and store $[\mathfrak{b}]^i \mapsto i$ in the lookup table    {coprime baby-steps}
19:   if $[\mathfrak{b}]^i = [\mathcal{O}_\Delta]$ then
20:     $h \leftarrow iE$, then go to line 30
21:   end if
22: end for
23: for $1 \leq j \leq m\phi(P_w)$ do
24:   if $[\mathfrak{b}]^{2js}$ is in the table, first lookup $i$ then
25:     $h \leftarrow$ odd part of $(2js - i)E$, then go to line 30    {positive giant-step}
26:   else if $[\mathfrak{b}]^{-2js}$ is in the table, first lookup $i$ then
27:     $h \leftarrow$ odd part of $(2js + i)E$, then go to line 30    {inverted giant-step}
28:   end if
29: end for
30: {– attempt to factor $N$ by finding an ambiguous form –}
31: for $1 \leq i \leq c$ do
32:   $[\mathfrak{b}] \leftarrow [\mathfrak{a}_i]^h$
33:   for $1 \leq k \leq \lfloor \log_2 h_\Delta \rfloor$ and $[\mathfrak{b}] \neq [\mathcal{O}_\Delta]$ do
34:     if $[\mathfrak{b}]$ is an ambiguous ideal and $[\mathfrak{b}]$ leads to a factor of $N$ then
35:       return a factor of $N$
36:     end if
37:     $[\mathfrak{b}] \leftarrow [\mathfrak{b}]^2$
38:   end for
39: end for
40: start over at line 3
```

Chapter 5

Extended Greatest Common Divisor Experiments

One contribution of this thesis is an efficient implementation of arithmetic in the ideal class group of imaginary quadratic number fields. Arithmetic in the ideal class group uses solutions to equations of the form $s = Ua + Vb$ where s is the largest integer dividing both a and b. Much of the computational effort of the algorithm for fast ideal multiplication (Algorithm 2.2) is in computing integral solutions to equations of the form

$$s = Ua + Vb$$

where a and b are fixed integers given as input, and s is the greatest common divisor (GCD) of both a and b. Solutions to this equation are referred to as the *extended greatest common divisor* (or extended GCD for short). A first step to improving the performance of arithmetic in the ideal class group, is to improve performance of GCD computations. This Chapter discusses several algorithms for computing such solutions and studies their performance in practice.

This Chapter and Chapter 6 focus on the techniques and experimental data that lead us to our implementation of arithmetic in the ideal class group. We specialized much of our implementation for the x64 architecture. Many of our routines benefit when the input is bound by a single machine word, i.e. 64-bits, but we were also able to take advantage of integers that fit within two machine words by implementing a custom library for 128-bit arithmetic. When integers are larger than 128-bits, we use the GNU Multiple Precision (GMP) arithmetic library [3]. All the software in this Chapter was developed using the GNU C compiler version 4.7.2 on Ubuntu 12.10. Assembly language was used for the inner loops of the routines presented here, as well as for processing features not available in the C programming language (such as 128-bit arithmetic). The hardware platform was a personal notebook with a 2.7GHz Intel Core i7-2620M CPU and 8Gb of memory. The CPU has four cores, only one of which was used during timing experiments.

5.1 The Euclidean Algorithm

The Euclidean Algorithm is an algorithm for computing the greatest common divisor of two integers. We start with two positive integers a and b. At each iteration of the algorithm, we subtract the smaller of the two numbers from the larger, until one of them is 0. At this point, the non-zero number is the largest divisor of a and b. Since the smaller number may still be smaller after a single iteration, we use fewer steps by subtracting an integer multiple of the smaller number from the larger one.

The Euclidean Algorithm is extended by using a system of equations of the form

$$s = Ua + Vb \tag{5.1}$$

$$t = Xa + Yb. \tag{5.2}$$

Initially, let

$$\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

and Equations 5.1 and 5.2 hold. We maintain the invariant that $s \geq t$. When $s < t$, simply swap the rows in the matrix representation above. At each iteration, subtract $q = \lfloor s/t \rfloor$ times the second row from the first, and then swap rows to maintain the invariant. When $t = 0$, the first row of the matrix is a solution such that s is the largest positive divisor of a and b. The algorithm is given in Algorithm 5.1. Negative inputs a and b are handled by using $a' = |a|$ and $b' = |b|$ as inputs instead and modifying the output such that $U' = U \cdot \text{sign}(a)$

and $V' = V \cdot \mathrm{sign}(b)$ where

$$\mathrm{sign}(x) = \begin{cases} -1 & \text{when } x < 0 \\ 0 & \text{when } x = 0 \\ 1 & \text{when } x > 0. \end{cases}$$

Algorithm 5.1 Extended Euclidean Algorithm.

```
Input: $a, b \in \mathbb{Z}_{\geq 0}$
1: $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$
2: if $t > s$ then
3:     $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$        {Swap rows. Maintain $s \geq t$.}
4: end if
5: while $t \neq 0$ do
6:     $q \leftarrow \lfloor s/t \rfloor$
7:     $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$        {Subtract $q$ times $2^{\text{nd}}$ row and swap.}
8: end while
9: return $(s, U, V)$        {Such that $s = Ua + Vb$.}
```

In practice, these operations are performed by manipulating each variable directly, rather than by using matrix arithmetic. Furthermore, we typically implement division with remainder, which solves $s = qt + r$ for $q, r \in \mathbb{Z}$ and $|r| < |t|$. Notice that $r = s - qt$ is the target value of t for each iteration of the Euclidean Algorithm.

5.2 Lehmer's GCD

In the previous section, each iteration subtracts a multiple, $q = \lfloor s/t \rfloor$, of the smaller number from the larger number. Derrick Henry Lehmer noticed that most of the quotients, q, were small and that those small quotients could be computed from the leading digits (or machine word) of the numerator and denominator [34].

The idea is similar to the Extended Euclidean Algorithm, only that there is an inner loop that performs an Extended GCD computation using values that fit within a single machine word. As before, start by letting

$$\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

for positive integers a and b. Assume that $s \geq t$ (if this is not the case, then swap the rows of the matrix). Compute $s' = \lfloor s/2^k \rfloor$ for some k such that s' fits within a single machine word and is as large as possible (if s already fits within a single machine word, then let $k = 0$), and compute $t' = \lfloor t/2^k \rfloor$ for the same value k. Then perform an Extended GCD computation on the values s' and t' but only for as long as the quotients $q' = \lfloor s'/t' \rfloor$, generated by each step of the single precision GCD computation, are equal to the quotients $q = \lfloor s/t \rfloor$, generated by a full precision GCD computation. To determine when the quotients q' differ from the quotients q, compute $q_1 = \lfloor (s' + A)/(t' + C) \rfloor$ and $q_2 = \lfloor (s' + B)/(t' + D) \rfloor$. Let $q' = q_1$ and when $q_1 = q_2$ it follows that $q' = q$ [34, p.229, Theorem A].

Let

$$\begin{bmatrix} s' & A & B \\ t' & C & D \end{bmatrix} \leftarrow \begin{bmatrix} s' & 1 & 0 \\ t' & 0 & 1 \end{bmatrix}$$

be the initial matrix consisting of single precision integers. Then perform the extended Euclidean Algorithm until $q_1 \neq q_2$ and the resulting matrix

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

represents the concatenation of the operations performed during the single precision GCD. If $B \neq 0$, these operations are combined with the outer loop of the larger GCD by computing

$$\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} A & B \\ C & D \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}.$$

Then continue with the outer loop of the computation until $t = 0$. In the event that $B = 0$, then s and t differ in length by more than a machine word, and we use a step of the full precision GCD computation to adjust their lengths. The complete algorithm is given in Algorithm 5.2.

Algorithm 5.2 Lehmer's GCD ([34]).

```
Input: $a, b, \in \mathbb{Z}$ and $a \geq b > 0$.
    Let $m$ be the number of bits in a machine word.
 1: $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$
 2: while $t \neq 0$ do
 3:     $k \leftarrow \lfloor \log_2 s \rfloor + 1 - m$
 4:     $s' \leftarrow \lfloor s/2^k \rfloor$                {Shift right for most significant word.}
 5:     $t' \leftarrow \lfloor t/2^k \rfloor$
 6:     $\begin{bmatrix} A & B \\ C & D \end{bmatrix} \leftarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
 7:     while $t' \neq 0$ and $\lfloor (s'+A)/(t'+C) \rfloor = \lfloor (s'+B)/(t'+D) \rfloor$ do
 8:         $q' \leftarrow \lfloor (s'+A)/(t'+C) \rfloor$                {Single precision step.}
 9:         $\begin{bmatrix} s' & A & B \\ t' & C & D \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ 1 & -q' \end{bmatrix} \cdot \begin{bmatrix} s' & A & B \\ t' & C & D \end{bmatrix}$
10:     end while
11:     if $B = 0$ then
12:         $q \leftarrow \lfloor s/t \rfloor$                {Full precision step.}
13:         $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$
14:     else
15:         $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} A & B \\ C & D \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$                {Combine step.}
16:     end if
17: end while
```

5.3 Right-to-Left Binary GCD

The previous extended GCD algorithms use divide with remainder, which is often expensive. Binary GCD algorithms emphasize bit shifting over multiplication and division. Such algorithms may perform better than other GCD algorithms in practice (see Section 5.8 for results). Here we describe a binary GCD algorithm that works from the least significant bit to the most significant bit. We refer to this as right-to-left since this is the direction in which we process the written binary representation. The concept was originally published by Stein [45].

To compute the greatest common divisor of two positive numbers, repeatedly apply the following identities,

$$\gcd(a,b) = \begin{cases} 2 \cdot \gcd(a/2, b/2) & \text{when both } a \text{ and } b \text{ are even} \\ \gcd(a/2, b) & \text{when only } a \text{ is even} \\ \gcd(a, b/2) & \text{when only } b \text{ is even} \\ \gcd((a-b)/2, b) & \text{when } a \geq b \text{ and both are odd} \\ \gcd((b-a)/2, a) & \text{when } a < b \text{ and both are odd.} \end{cases}$$

In the case that only a is even, we divide a by 2 since 2 is not a common divisor of both. The same is true when only b is even. When both a and b are odd, their difference is even and so is further reduced by 2. Notice that each relation reduces at least one of the arguments and so the recursion terminates with either $\gcd(a, 0) = a$ or $\gcd(0, b) = b$.

When both a and b are even, $\gcd(a, b) = 2 \cdot \gcd(a/2, b/2)$. So the first step of our binary GCD algorithm is to remove all common powers of two from a and b. Let r be the number of times 2 is removed from both. Now either a or b or both are odd. If a is not odd, then swap a and b so that a is guaranteed to be odd. We will compute the GCD of the reduced a and b. As such, the final solution to the original input is $s2^r = Ua2^r + Vb2^r$.

As before, begin with the matrix representation

$$\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}.$$

An invariant of the algorithm is that s is odd at the beginning of each iteration. Since a was chosen to be odd, s is initially odd. First remove any powers of 2 from t. While t is even, we would like to apply the operation

$$(t, X, Y) \leftarrow \left(\frac{t}{2}, \frac{X}{2}, \frac{Y}{2}\right)$$

but this may result in rational values for X and Y if either are odd. We first point out that

$$\begin{aligned} t &= Xa + Yb \\ &= Xa + Yb + (ab - ab) \\ &= (X + b)a + (Y - a)b. \end{aligned}$$

As such, we can simultaneously add b to X and subtract a from Y when it suits us.

Theorem 5.3.1. When t is even, either both X and Y are even, or Y is odd and both $X + b$ and $Y - a$ are even.

Proof. Assume t is even and that Y is odd. We have

$$\begin{aligned} & t \equiv Xa + Yb && \pmod 2 \\ \Rightarrow \quad & 0 \equiv X + b && \pmod 2 \quad \{\text{Since } t \text{ is even and } Y \text{ and } a \text{ are odd.}\} \\ \Rightarrow \quad & 0 \equiv X + b \equiv Y - a && \pmod 2 \quad \{\text{Since } Y - a \text{ is even.}\}. \end{aligned}$$

Now assume t is even and that X is odd. We have

$$\begin{aligned} & t \equiv Xa + Yb && \pmod 2 \\ \Rightarrow \quad & 0 \equiv 1 + Yb && \pmod 2 \quad \{\text{Since } t \text{ is even and } X \text{ and } a \text{ are odd.}\} \\ \Rightarrow \quad & 1 \equiv Yb && \pmod 2 \quad \{\text{Both } Y \text{ and } b \text{ are odd.}\} \\ \Rightarrow \quad & 0 \equiv X + b \equiv Y - a && \pmod 2. \end{aligned}$$

Therefore, if t is even, either both X and Y are even, or Y is odd and both $X + b$ and $Y - a$ are even. □

By Theorem 5.3.1, we have a way to reduce t by 2 and maintain integer coefficients. While t is even,

$$(t, X, Y) \leftarrow \begin{cases} \left(\frac{t}{2}, \frac{X}{2}, \frac{Y}{2}\right) & \text{if } Y \text{ is even} \\ (t, X, Y) \leftarrow \left(\frac{t}{2}, \frac{X+b}{2}, \frac{Y-a}{2}\right) & \text{otherwise.} \end{cases}$$

At this point, both s and t are odd. If $s \geq t$ then let

$$\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$$

otherwise let

$$\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}.$$

This ensures that s is odd, t is even, and that both s and t are positive. Repeat the steps of reducing t by powers of 2 and then subtracting one row from the other until $t = 0$. The complete algorithm is given in Algorithm 5.3. Note that in practice, integer division by 2 is performed using a bit shift right.

Algorithm 5.3 Right-to-left Binary GCD (Based on [45]).

```
Input: $a, b, \in \mathbb{Z}_{>0}$.
 1: let $r$ be the largest integer such that $2^r$ divides both $a$ and $b$
 2: $a \leftarrow a/2^r, b \leftarrow b/2^r$
 3: swap $a$ and $b$ if $a$ is not odd
 4: $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$
 5: while $t \neq 0$ do
 6:    while $t$ is even do
 7:       if $Y$ is odd then
 8:          $(X, Y) \leftarrow (X + b, Y - a)$
 9:       end if
10:       $(t, X, Y) \leftarrow \left(\frac{t}{2}, \frac{X}{2}, \frac{Y}{2}\right)$
11:    end while
12:    if $s \geq t$ then
13:       $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$
14:    else
15:       $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$
16:    end if
17: end while
18: return $(s2^r, U, V)$ if $a$ and $b$ were not swapped and $(s2^r, V, U)$ otherwise
```

5.4 Windowed Right-to-Left Binary GCD

Windowing is a common technique used to extend the base of an algorithm. We saw this earlier in our discussion of binary exponentiation in Section 3.1. The idea there was to precompute g^w for each w in some window $0 \leq w < 2^k$ for some k and then to iterate over the exponent k bits at a time. We can apply this technique to the right-to-left extended binary GCD.

The algorithm in the previous subsection repeatedly reduces either the equation $t = Xa + Yb$ or the equation $t = (X + b)a + (Y - a)b$ by 2. When Y is odd, we simultaneously add b to X and subtract a from Y in order to make both X and Y even. Suppose that t was a multiple of 4. We could simultaneously add b to X and subtract a from Y repeatedly until both X and Y were divisible by 4. Choose m such that $ma \equiv Y \pmod 4$, and then $t = (X + mb)a + (Y - ma)b$ is evenly divisible by 4 when t is divisible by 4.

This is easily extended for any 2^k where k is a positive integer. The algorithm first computes $x_j = mb$ and $y_j = ma$ for $0 \leq m < 2^k$ where $j = ma \bmod 2^k$. While t is divisible by 2^h for some $h \leq k$, we look up x_j and y_j for $j = Y \bmod 2^h$ and compute $(X + x_j)/2^h$ and $(Y - y_j)/2^h$. The complete Algorithm is given in listing 5.4.

5.5 Left-to-Right Binary GCD

Just as exponentiation can be performed from high-order to low-order, so too can an extended binary GCD computation. This is termed a left-to-right binary GCD, since it works from the left most bit to the right most bit of the written binary representation of the inputs.

Recall that at each iteration of the extended Euclidean Algorithm, we subtract $q = \lfloor s/t \rfloor$ times the equation $t = Xa + Yb$ from the equation $s = Ua + Vb$ and then swap (s, U, V) with (t, X, Y). Computing $q = \lfloor s/t \rfloor$ uses integer division, and then subtracting q times one equation from the other uses multiplication. Since it is not necessary to subtract exactly q times the equation, the idea is instead to use a value $q' = 2^k$ such that q' is *close* in some

Algorithm 5.4 Windowed Right-to-left Binary GCD.

```
Input: $a, b, \in \mathbb{Z}_{>0}$ and let $k \in \mathbb{Z}_{>0}$ be the window size in bits.
 1: let $r$ be the largest integer such that $2^r$ divides both $a$ and $b$
 2: $a \leftarrow a/2^r, b \leftarrow b/2^r$
 3: swap $a$ and $b$ if $a$ is not odd
 4: for $m$ from $2^k - 1$ downto 0 do
 5:     $j \leftarrow ma \bmod 2^k$
 6:     $x_j \leftarrow mb$
 7:     $y_j \leftarrow ma$
 8: end for
 9: $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$
10: while $t \neq 0$ do
11:     while $t$ is even do
12:         let $h$ be the largest integer such that $h \leq k$ and $2^h$ divides $t$
13:         $j \leftarrow Y \bmod 2^h$
14:         $(t, X, Y) \leftarrow \left(\frac{t}{2^k}, \frac{X+x_j}{2^h}, \frac{Y+y_j}{2^h}\right)$        {Reduce by $2^h$}
15:     end while
16:     if $s \geq t$ then
17:         $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$
18:     else
19:         $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$
20:     end if
21: end while
22: return $(s2^r, U, V)$ if $a$ and $b$ were not swapped and $(s2^r, V, U)$ otherwise
```

sense to q. Subtracting q' times the second equation from the first can then be done using a binary shift left by k bits.

Shallit and Sorenson [42] propose to select $q' = 2^k$ such that $q't \leq s < 2q't$. If $s - q't < 2q't - s$, compute

$$\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q' \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix},$$

otherwise, compute

$$\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2q' \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}.$$

Notice that after this step s has the previous value of t and that the binary representation of t is one digit shorter than the binary representation of the previous value of s, i.e. the the left most set bit of the previous value of s is now cleared. As with the extended Euclidean Algorithm, maintain the invariant that $s \geq t$; if after the above operation $s < t$, then swap the rows of the matrix to restore the invariant. The complete algorithm is given in Algorithm 5.5.

Algorithm 5.5 Shallit and Sorenson Left-to-Right binary GCD [42].

```
Input: $a, b \in \mathbb{Z}$
1: $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$
2: if $t > s$ then
3:     $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$        {Swap rows. Maintain $s \geq t$.}
4: end if
5: while $t \neq 0$ do
6:     find $q = 2^k$ such that $qt \leq s < 2qt$
7:     if $s - qt < 2qt - s$ then
8:         $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$
9:     else
10:        $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2q \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$
11:    end if
12:    if $t > s$ then
13:        $\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$        {Swap rows. Maintain $s \geq t$.}
14:    end if
15: end while
16: return $(s, U, V)$
```

In practice, to find $q = 2^k$ we compute the number of bits in both s and t and then use the difference as a candidate for k. Let $k' = (\lfloor \log_2 s \rfloor + 1) - (\lfloor \log_2 t \rfloor + 1) = \lfloor \log_2 s \rfloor - \lfloor \log_2 t \rfloor$ be our candidate. If $t2^{k'} \leq s$ then $k = k'$, otherwise $k = k' - 1$. Notice that either $k = k'$ in which case $t2^k = t2^{k'}$, or $k = k' - 1$ and then $t2^{k+1} = t2^{k'}$. Either way $t2^{k'}$ can be reused for one half of the comparison of $s - qt < 2qt - s$. Also, if $k' = 0$ then $t \leq s$ (by our invariant) and so there is no possibility of using $t2^{-1}$, since we will use $t2^{k'}$ and $t2^{k'+1}$ in the comparison.

This approach requires us to first compare $t2^{k'}$ to s and then compare one of $t2^{k'-1}$ or $t2^{k'+1}$ to s in order to find which is closer. Because of this, we also experimented with a simplified version of the algorithm. We only compute $k = \lfloor \log_2 s \rfloor - \lfloor \log_2 t \rfloor$. Let $q = 2^k$ and compute

$$\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}.$$

If $qt > s$ then the resulting value for $s - qt$ is negative, and so we negate the first row of the product matrix to ensure that the new value for s is positive. The result is fewer comparisons for the inner loop of the GCD overall.

5.6 Partial Extended GCD

Subsections 2.5.5, 2.5.6, and 2.5.7 give algorithms to compute the partially reduced coefficients of ideal representatives for multiplication, squaring, and cubing respectively. In each case, a continued fraction expansion is computed using the recurrences

$$q_i = \lfloor R_{i-2} \ / \ R_{i-1} \rfloor$$
$$R_i = R_{i-2} - q_i R_{i-1}$$
$$C_i = C_{i-2} - q_i C_{i-1}.$$

These recurrences perform the same operation as a single step in the Extended Euclidean Algorithm of Section 5.1, but the initial and stopping conditions are different. As such, this is referred to as the *Partial Extended Euclidean Algorithm.* The algorithm is listed in Algorithm 5.6.

All the operations performed on the matrix

$$\begin{bmatrix} R_0 & C_0 \\ R_1 & C_1 \end{bmatrix}$$

during the Partial Extended Euclidean Algorithm can be represented by an invertible 2×2 matrix with determinant ± 1 (known as a *unimodular* matrix). This is necessarily the

Algorithm 5.6 Partial Extended Euclidean Algorithm.

```
Input: $a, b, \in \mathbb{Z}$ and a termination bound $B \in \mathbb{Z}$.
1: $\begin{bmatrix} R_0 & C_0 \\ R_1 & C_1 \end{bmatrix} = \begin{bmatrix} a & 0 \\ b & -1 \end{bmatrix}$
2: if $R_1 > R_0$ then
3:     $\begin{bmatrix} R_0 & C_0 \\ R_1 & C_1 \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} R_0 & C_0 \\ R_1 & C_1 \end{bmatrix}$        {Swap rows. Maintain $s \geq t$.}
4: end if
5: while $R_1 > B$ do
6:     $q \leftarrow \lfloor R_0/R_1 \rfloor$
7:     $\begin{bmatrix} R_0 & C_0 \\ R_1 & C_1 \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \cdot \begin{bmatrix} R_0 & C_0 \\ R_1 & C_1 \end{bmatrix}$        {Subtract $q$ times 2nd row and swap.}
8: end while
9: return $(R_0, R_1, C_0, C_1)$
```

case since each operation relates one representative of an ideal equivalence class to another representative[1]. This is critical since only extended GCD computations that are restricted to operations representable using invertible 2×2 matrices can be used for the partial extended GCD.

Of the extended GCD algorithms in this section, only the right-to-left binary GCD of Section 5.3 cannot be adapted to the partial extended GCD. The reason is due to the step where t is reduced by 2. The Algorithm uses the computation

$$(t, X, Y) \leftarrow \begin{cases} \left(\frac{t}{2}, \frac{X}{2}, \frac{Y}{2}\right) & \text{if } Y \text{ is even} \\ (t, X, Y) \leftarrow \left(\frac{t}{2}, \frac{X+b}{2}, \frac{Y-a}{2}\right) & \text{otherwise.} \end{cases}$$

The step $(t, X, Y) \leftarrow (t/2, (X+b)/2, (Y-a)/2)$ cannot be expressed as a unimodular matrix.

The other extended GCD algorithms of this section can be adapted to the partial extended GCD by letting

$$\begin{bmatrix} R_0 & C_0 \\ R_1 & C_1 \end{bmatrix} = \begin{bmatrix} s & U \\ t & X \end{bmatrix}$$

and dropping the terms V and Y from the computation.

[1]Recall our discussion of binary quadratic forms (see subsection 4.1.1). Two forms are related if there exists an invertible linear transformation of variables.

5.7 Specialized Implementations of the Extended GCD

To further improve performance, we specialized implementations of each of the GCD algorithms discussed in this section for the x64 architecture. All algorithms are implemented for the GNU C compiler[2] and often benefit from hand optimized x64 assembler. Assembly language is used in line and is conditionally compiled based on the target platform[3]. For each of the GCD algorithms presented here, we implemented 32-bit and 64-bit versions, and when arithmetic overflows do not require us to use GMP, we also implemented 128-bit versions. For appropriately sized inputs, we use these specialized implementations, otherwise we use GMP for the extended GCD computation.

Many of the techniques used here are described in the book "Hacker's Delight" [48]. We use $\texttt{and}_2$ to denote bitwise 'and', $\texttt{or}_2$ for bitwise 'or', '$\oplus$' for bitwise 'exclusive or', and '$\neg$' for bitwise negation. Computing $x2^k$ corresponds to shifting x left by k bits, while computing the integer $\lfloor x/2^k \rfloor$ corresponds to shifting x right by k bits. To compute $x \bmod 2^k$ use $x \ \texttt{and}_2 \ (2^k - 1)$.

Assuming a two's complement representation of machine words, the most significant bit of a machine word x is set if $x < 0$ and clear otherwise. Let m denote the number of bits in a machine word; then the result of an arithmetic shift right on x by $m - 1$ bits is either a word with m set bits when $x < 0$ or a word with m clear bits otherwise. Let $\texttt{sign\_mask}(x)$ denote this operation. Notice that a word with m set bits, corresponds to the integer -1 under a signed two's complement representation.

Using these operations, the absolute value of a signed machine word x can be computed without using any conditional statements. Let $y = \texttt{sign\_mask}(x)$ and the absolute value of x is $(x \oplus y) - y$. To see this, suppose $x \geq 0$. Then y is 0 and so $(x \oplus y) - y = x$. When

[2]The source code was compiled using GCC 4.7.2 with the default dialect, which is the GNU dialect of ISO C90.

[3]For time critical paths and to take advantage of special instructions, x64 assembly language is used when __x86_64 is defined, otherwise 80386 assembly language is used when __i386 is defined, and when neither are defined, C is used.

$x < 0$, y has all of its bits set (and is also -1). Therefore, $(x \oplus y) - y = \neg x + 1 = -x$.

Similarly, a word x can be conditionally negated depending on a bit-mask y. This is useful since the extended GCD algorithms described previously expect their input, a and b, to be positive integers. First compute the absolute value of a and b by computing a signed mask for each and then conditionally negate each. Since the extended GCD algorithm computes a solution to $s = Ua + Vb$, where a and b have been made positive, the solution for the original inputs is to conditionally negate U based on the signed mask of a, and V based on the signed mask of b.

Furthermore, many of the algorithms maintain the invariant that $s > t$ and that both are positive. Suppose the algorithm computes

$$\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$$

when $s \geq t$ and

$$\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ -1 & q \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$$

otherwise. The conditional instruction is removed by first computing $m = \texttt{sign\_mask}(s - t)$ and then

$$\begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix} \leftarrow \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \cdot \begin{bmatrix} s & U & V \\ t & X & Y \end{bmatrix}$$

and conditionally negating the triple (t, X, Y) based on the signed mask m.

To swap two machine words, x_0 and y_0, without using additional words, compute $x_1 = x_0 \oplus y_0$, $y_1 = x_1 \oplus y_0$, and then $x_2 = x_1 \oplus y_1$. Notice that x_2 expands to

$$x_2 = (x_0 \oplus y_0) \oplus ((x_0 \oplus y_0) \oplus y_0)$$

and this reduces to $x_2 = y_0$. Also, y_1 expands to $(x_0 \oplus y_0) \oplus y_0$, which is just x_0. In practice, each assignment to x_i and y_i overwrites the previous x_{i-1} and y_{i-1} and so is performed in place.

Two words, x and y, are conditionally swapped when $x < y$ by using two additional words. Let $d = x - y$. Notice that simply computing $x \leftarrow x - d$ and $y \leftarrow y + d$ swaps x and y. Instead, let $m = \texttt{sign\_mask}(d)$ and then $x \leftarrow x - (d \; \texttt{and}_2 \; m)$ and $y \leftarrow y + (d \; \texttt{and}_2 \; m)$ swaps x and y only when $x < y$. In the left-to-right binary GCD, we conditionally swap the triple (s, U, V) with (t, X, Y) when $s < t$. By fixing $m = \texttt{sign\_mask}(s - t)$, but letting d take on $s - t$, and then $U - X$, and finally $V - Y$, we conditionally swap the triples when $s < t$. The algorithm is given in Algorithm 5.7. On the x64 architecture we optimize the

Algorithm 5.7 Conditionally swap (s, U, V) with (t, X, Y) when $s < t$.

```
1: $d \leftarrow s - t$
2: $m \leftarrow \texttt{sign\_mask}(d)$
3: $d \leftarrow d \; \texttt{and}_2 \; m$
4: $s \leftarrow s - d$
5: $t \leftarrow t + d$
6: $d \leftarrow (U - X) \; \texttt{and}_2 \; m$
7: $U \leftarrow U - d$
8: $X \leftarrow X + d$
9: $d \leftarrow (V - Y) \; \texttt{and}_2 \; m$
10: $V \leftarrow V - d$
11: $Y \leftarrow Y + d$
```

computation of $d \leftarrow s - t$ and $m \leftarrow \texttt{sign\_mask}(d)$ since the operation $s - t$ sets the carry flag when the result is negative. Using a subtract with borrow, we subtract m from itself. This sets m to 0 when the carry is clear, and -1 when the carry is set.

Often our implementation uses the number of bits in a positive integer x. In the algorithm description we use $\lfloor \log_2 x \rfloor + 1$. On the x64 architecture there is an instruction (`bsr`) that returns the index of the most significant set bit. This allows us to quickly compute that value. On a platform that does not have such an instruction, we use a logarithmic search to find the most significant set bit[4]. Let $k = \lfloor m/2 \rfloor$ where m is the number of bits in a machine word and let i be the computed index (initially $i \leftarrow 0$). We first check if $x \geq 2^k$. If it is, then $i \leftarrow i + k$ and x is shifted right by k. We repeat on $k \leftarrow \lfloor k/2 \rfloor$ until $k = 0$. At which point, i is the index of the most significant set bit (see Algorithm 5.8). Notice that we can

[4]There is also a similar algorithm to find the *least* significant set bit of a machine word (`bsl` on x64).

use the signed mask of $2^k - x$ instead of the conditional 'if' statement, and we can unroll the while loop for fixed values of m.

Algorithm 5.8 Return the index of the most significant set bit of x.

```
1: $i \leftarrow 0$
2: $k \leftarrow \lfloor m/2 \rfloor$                {$m$ is the number of bits in a machine word.}
3: while $k \neq 0$ do
4:    if $x \geq 2^k$ then
5:       $x \leftarrow \lfloor x/2^k \rfloor$
6:       $i \leftarrow i + k$
7:    end if
8: end while
9: return $i$
```

Finally, Lehmer's GCD algorithm is especially useful when the arguments to the GCD are several words in size. However, since our implementations are specialized up to 128-bit words, we consider 8-bit words for the inner extended GCD computation. As such, it is possible to precompute the resulting 2×2 matrix for all possible inputs into the single precision extended GCD computation. Since there are two inputs, each 8-bits in size, there are 65536 possible pairs of inputs. The coefficients of the resulting 2×2 matrix can be bound by 8-bits each, and so the table requires 256Kb of memory. This simplifies the GCD computation since the inner loop of Lehmer's GCD becomes a lookup from this table.

5.8 Experimental Results

We specialized the implementation of each of the extended GCD algorithms for 32-bit and 64-bit words. When intermediate terms did not overflow 128-bit words, we also implemented 128-bit versions. For each k from 1 to 127, we generated 1,000,000 pairs of integers of k bits each, and measured the time to compute the extended GCD of each pair using each algorithm and its specialized implementation when available.

First, we present evidence that in each case, the 32-bit implementation is no slower than the 64-bit implementation, and in all but one case, always faster. Figure 5.1 shows that a

32-bit Extended Euclidean Algorithm using division with remainder is faster than a 64-bit one, for the same inputs.

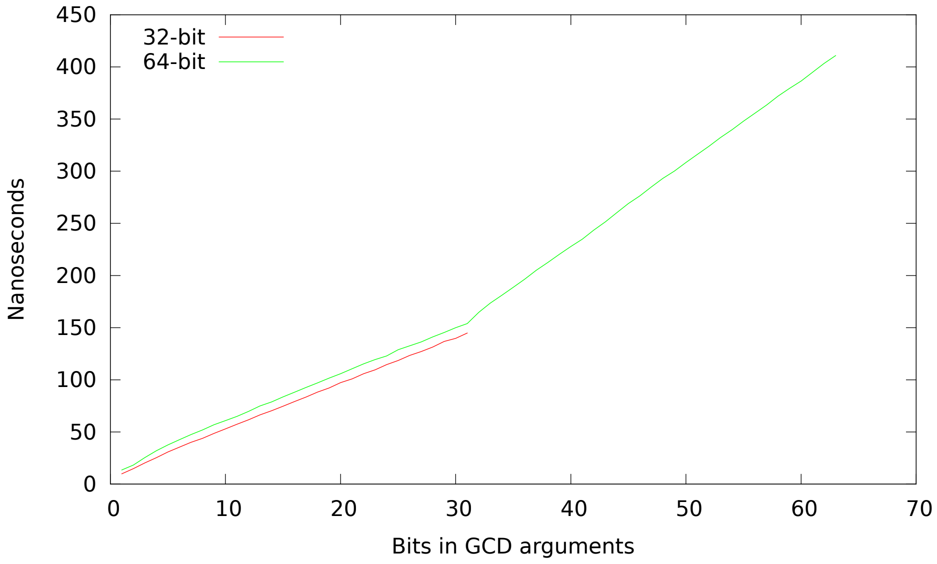


Figure 5.1: Extended Euclidean Algorithm using division with remainder.

For Lehmer's GCD, we precomputed a table of 8-bit inputs for the inner GCD computation – see Figure 5.2. In each case, the 32-bit implementation is faster than the 64-bit implementation.

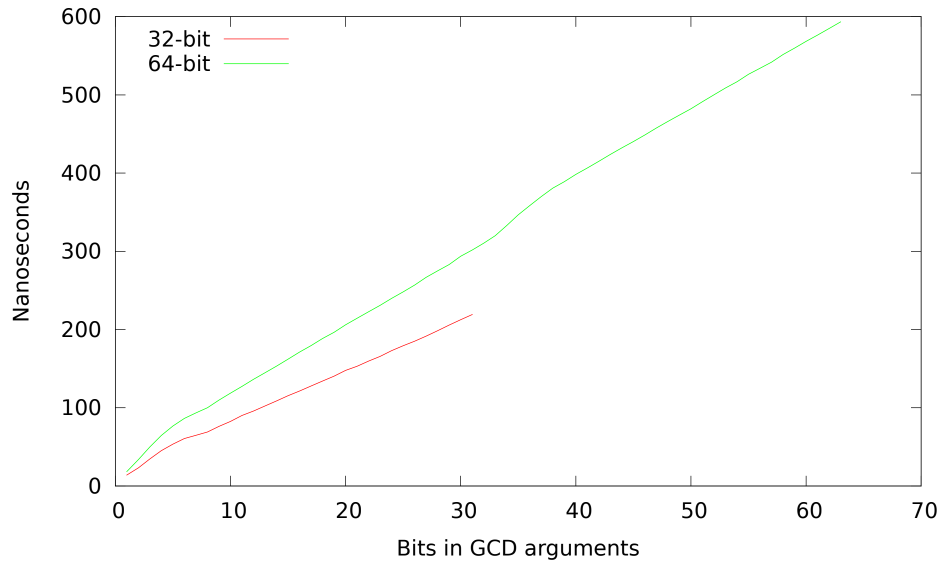


Figure 5.2: Lehmer's GCD with 8-bit precomputed inner GCD.

The graphs in Figures 5.3, 5.4, 5.5, 5.6, and 5.7 show that for all window sizes from 1 to 5 bits, that the 32-bit version of the right-to-left binary GCD is faster than the 64-bit version.

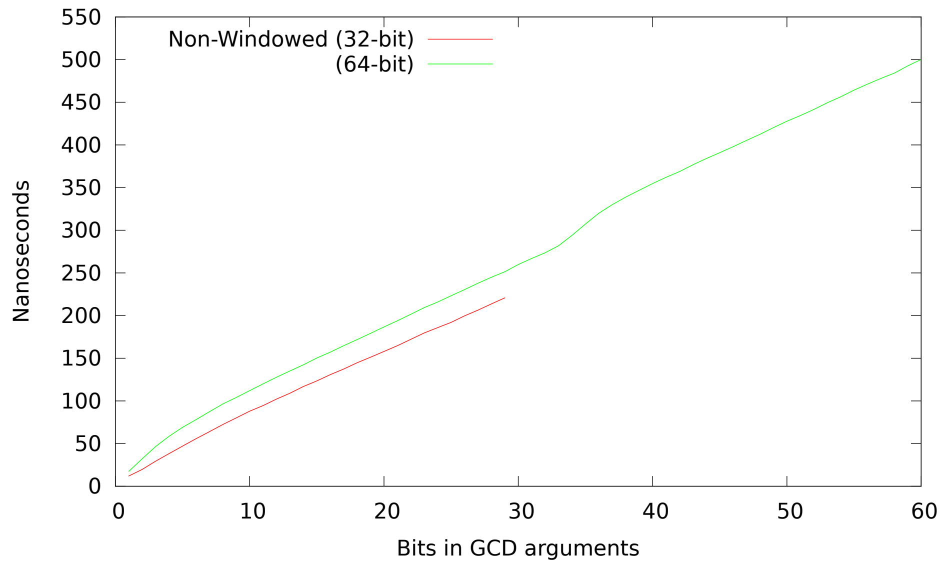


Figure 5.3: Right-to-Left Binary GCD.

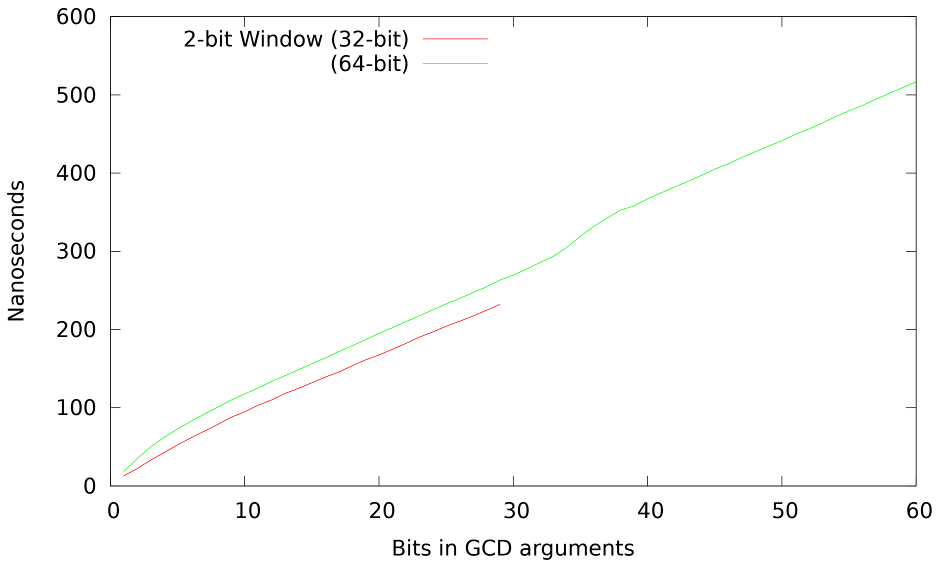


Figure 5.4: 2-bit Windowed Right-to-Left Binary GCD.

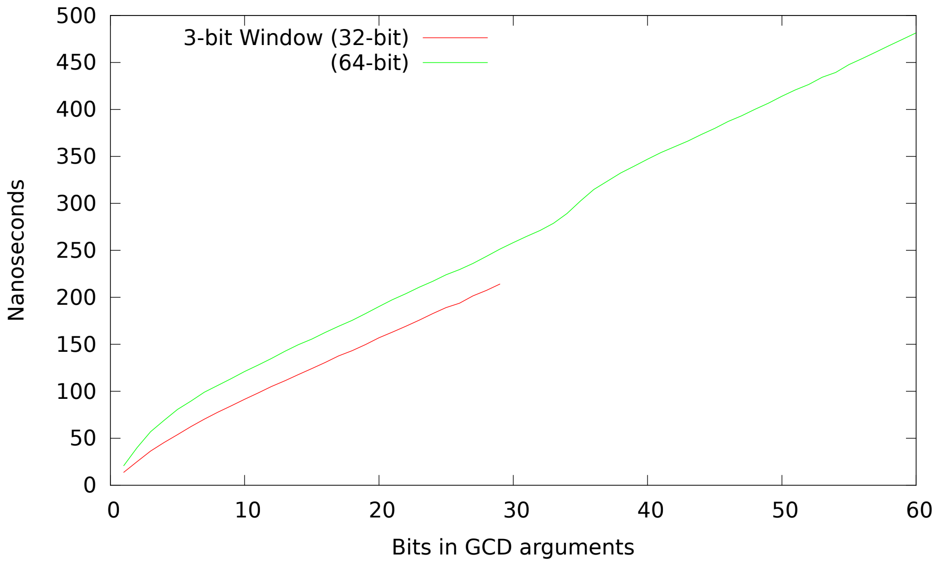


Figure 5.5: 3-bit Windowed Right-to-Left Binary GCD.

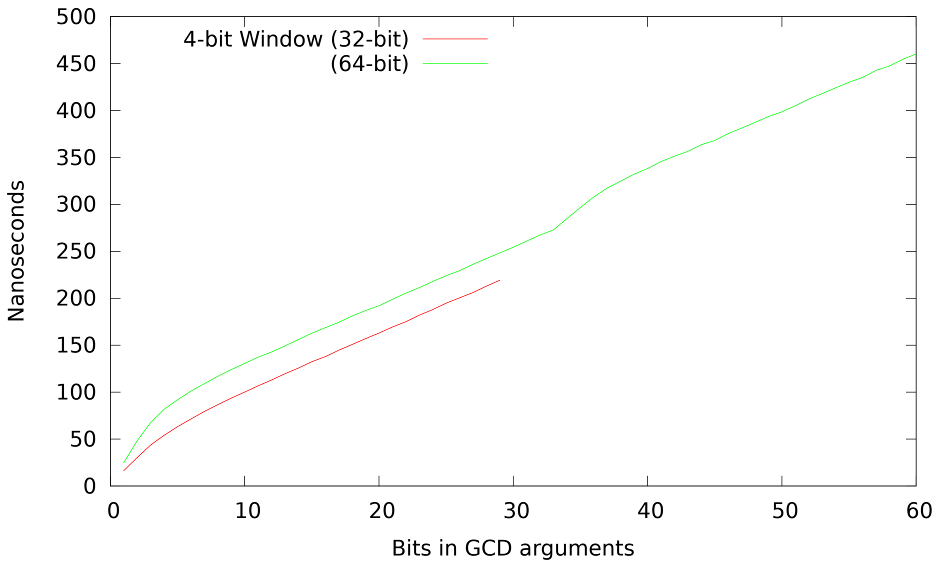


Figure 5.6: 4-bit Windowed Right-to-Left Binary GCD.

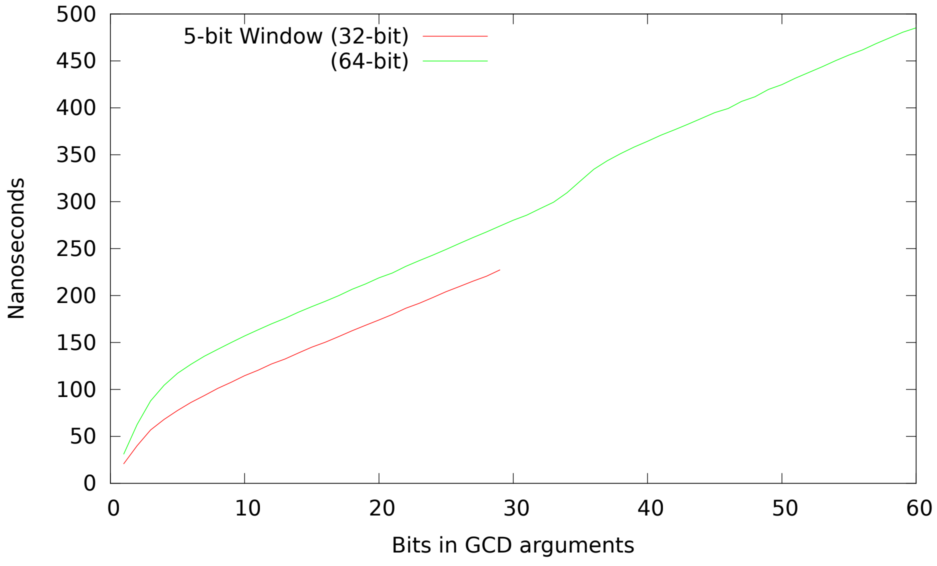


Figure 5.7: 5-bit Windowed Right-to-Left Binary GCD.

The left-to-right variant of the binary GCD proposed by Shallit and Sorenson is shown in figure 5.8. Here the 32-bit implementation is slightly faster than the 64-bit implementation.

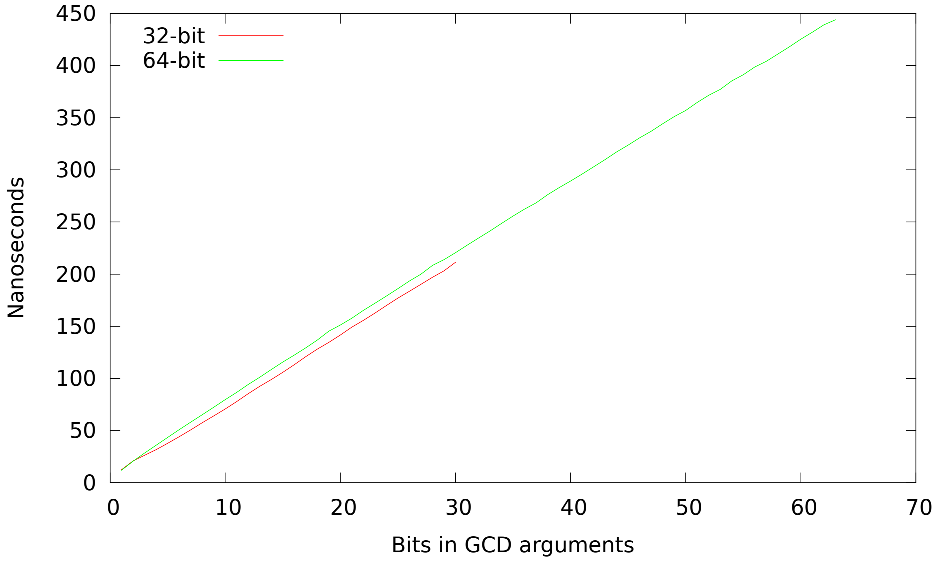


Figure 5.8: Left-to-Right binary GCD of Shallit and Sorenson.

Lastly, our simplified version of the left-to-right binary GCD is shown in figure 5.9. In this case, the benefit, if any, to using a 32-bit implementation over a 64-bit implementation is negligible[5].

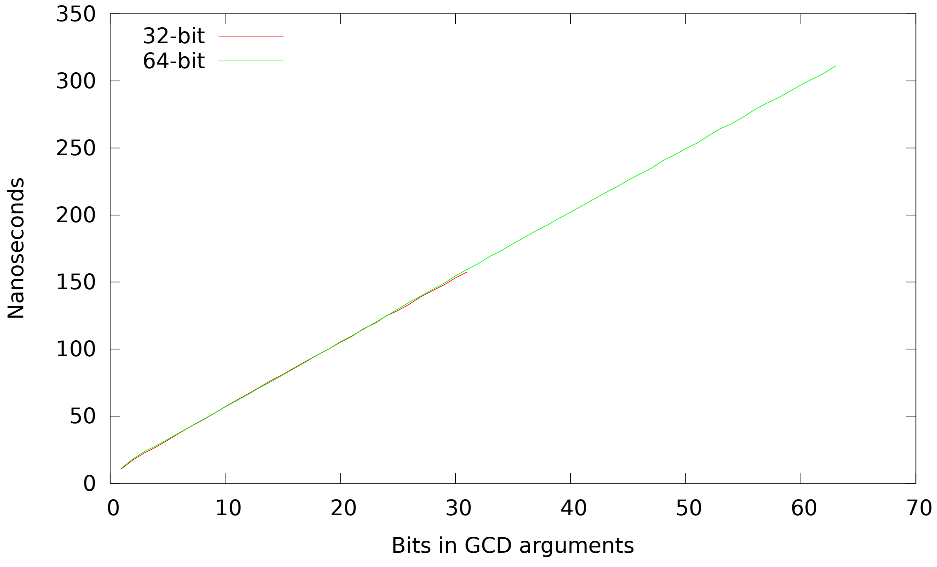


Figure 5.9: Simplified Left-to-Right binary GCD.

[5]Nanosecond differences between the two versions could be attributed to timing inaccuracies.

Note that the 32-bit versions of the right-to-left binary GCD are only accurate up to 29-bits (ignoring sign), while the 64-bit versions are only accurate to 60-bits. All other 32-bit implementations are accurate to 31-bits[6] and all other 64-bit implementations are accurate to 63-bits[7].

Since the 32-bit implementation of each algorithm is at least no slower than the 64-bit implementation, when comparing the different algorithms, we always prefer the 32-bit implementation of each when the algorithm is known to be accurate for the size of the inputs.

Both the Extended Euclidean Algorithm and Lehmer's GCD use division with remainder to compute their result, so we first compare our implementations of both. Figure 5.10 shows that the Extended Euclidean Algorithm is always faster.

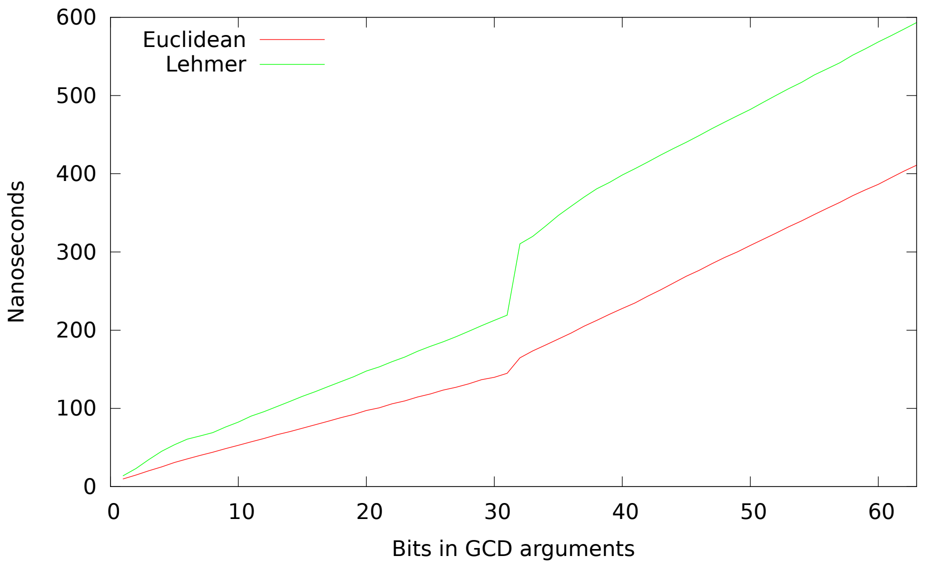


Figure 5.10: Extended Euclidean Algorithm compared to Lehmer's GCD using precomputed 8-bit words.

In Figure 5.11, we compare each of our windowed implementations of the right-to-left binary GCD. Larger windows trade off precomputation against the likelihood that a number will be divisible by some power of two. You can see that the non-windowed version is most

[6]The input is less than or equal to 31-bits, since in a two's complement representation the sign of the input variable takes the most significant bit and accounts for all 32-bits.

[7]Similar to the 32-bit implementation, the most significant bit represents the sign of the integer.

efficient for inputs less than 16-bits in size, at which point the 3-bit windowed version is best until 30 bits. After 30 bits, the 4-bit windowed version out performs other window sizes in the range with which we experimented. In the 64-bit implementation, the slope of the 5-bit windowed version is the lowest and so presumably it would out perform the 4-bit window once inputs were large enough.

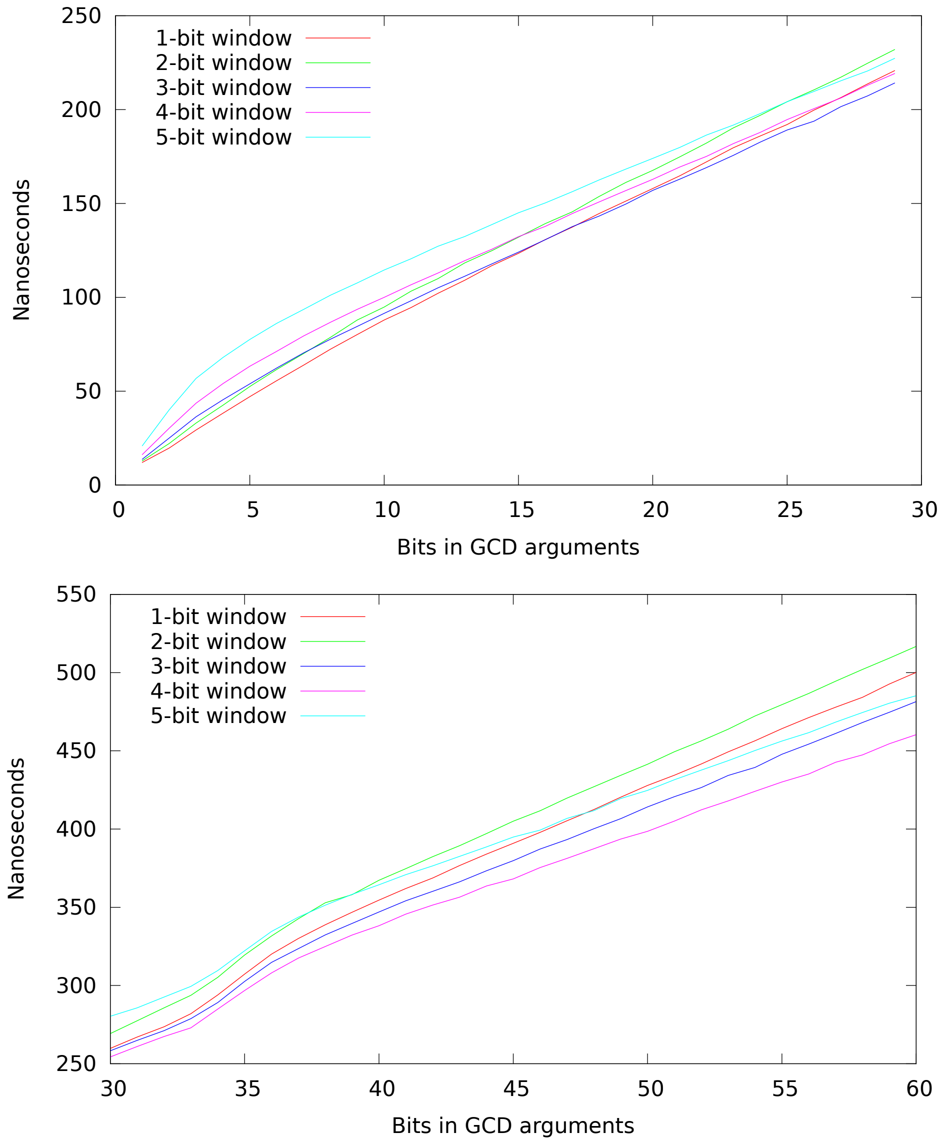


Figure 5.11: Windowed right-to-left binary GCDs.

Figure 5.12 compares the left-to-right binary GCD proposed by Shallit and Sorenson to our own simplified version.

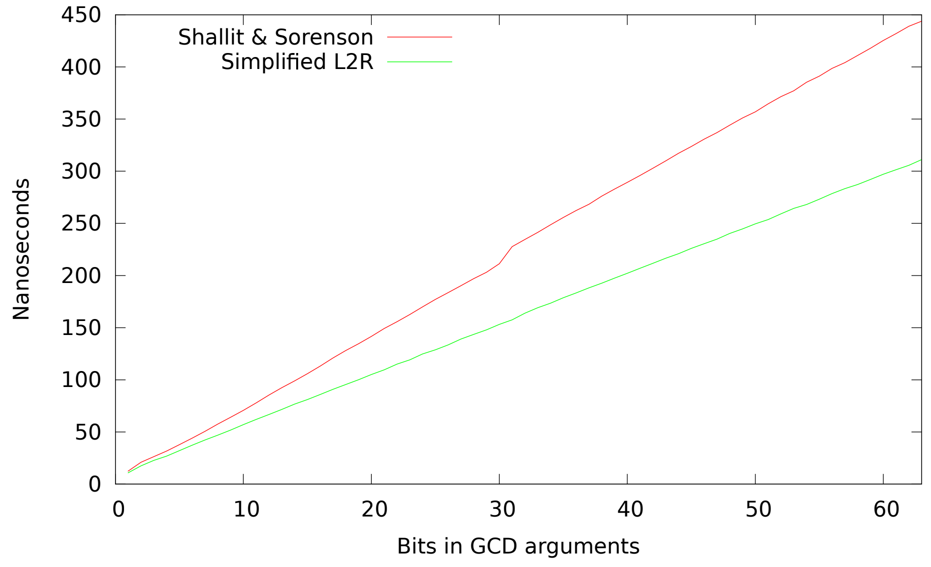
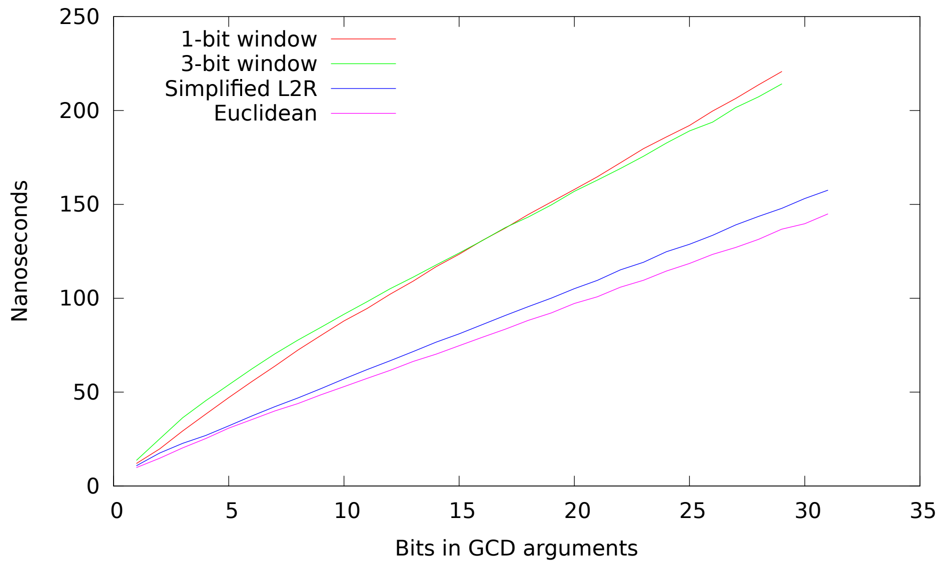


Figure 5.12: Shallit and Sorenson compared to our simplified left-to-right binary GCD.

Our implementation of the Euclidean Algorithm always out performs Lehmer's GCD. For our implementations of the right-to-left binary GCD, among the 32-bit implementations, the non-windowed and the 3-bit windowed versions perform well. For the 64-bit implementation, the 4-bit windowed version out performs the other window sizes. Finally, for the left-to-right variants of the binary GCD, our simplified version always out performs the approach proposed by Shallit and Sorenson. In Figure 5.13, we compare these top performers. For integer inputs less than 32-bits, the standard Euclidean Algorithm performs best, and for inputs between 32-bits and 64-bits, our simplified left-to-right binary GCD is fastest.



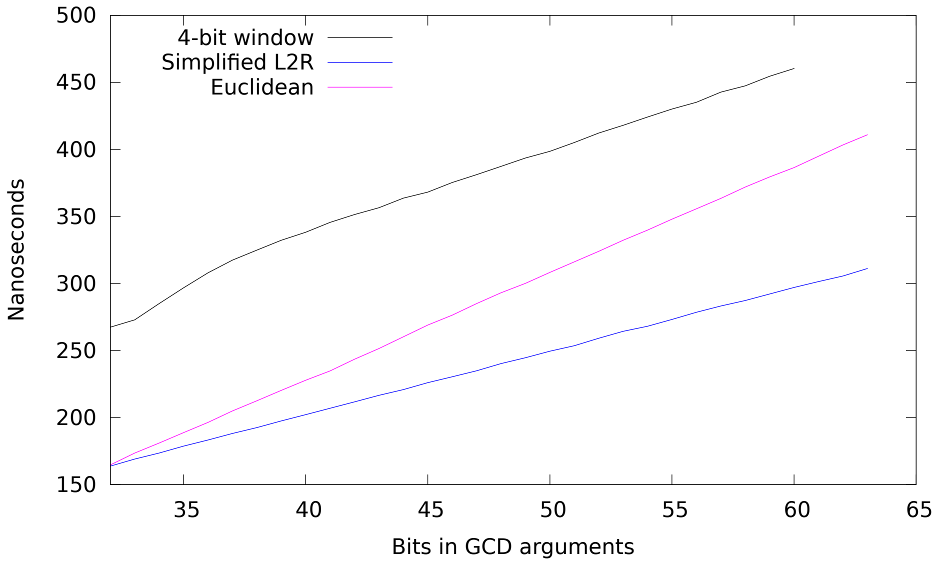


Figure 5.13: Euclidean vs windowed right-to-left binary vs simplified left-to-right binary.

Since the Euclidean Algorithm and our simplified left-to-right binary GCD are our fastest implementations for inputs less than 64-bits, we extended both to work on 128-bit integers. We also compared these with the implementation of the extended GCD algorithm from the GNU Multiple Precision (GMP) library. Figure 5.14 show that our implementations perform faster than the implementation in GMP for inputs smaller than 64-bits.

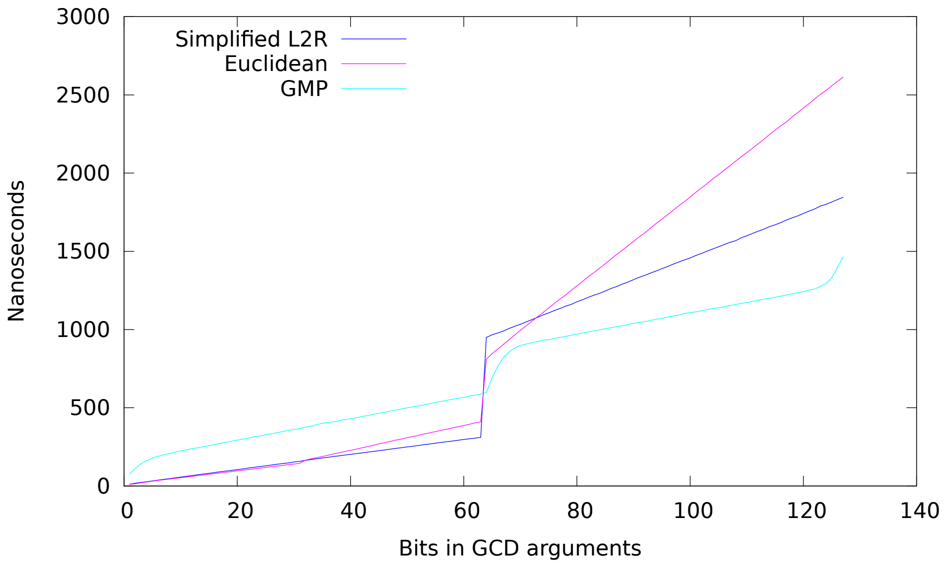


Figure 5.14: The extended Euclidean algorithm vs our simplified left-to-right binary GCD vs the mpz_gcdext function from the GNU Multiple Precision library.

This chapter discussed methods that lead to practical improvements for computing the greatest common divisor of two integers, and this indirectly contributes to the performance of arithmetic in the ideal class group. The Chapter began with several methods for computing solutions to equations of the form $s = Ua + Vb$ where s is the greatest common divisor of both a and b, since arithmetic in the ideal class group is dominated by this operation. We found that when the inputs a and b are bound by 2^{32}, that the standard Extended Euclidean Algorithm performs best. When $2^{32} \le a, b < 2^{64}$, a left-to-right binary GCD computation is fastest. Finally, for $a, b \ge 2^{64}$ we defer to the implementation in the GNU Multiple Precision (GMP) library.

Chapter 6

Ideal Arithmetic Experiments

The previous Chapter demonstrated results that lead to practical improvements in computing the extended GCD – the dominating operation in reduced ideal multiplication. This Chapter discusses our implementations of ideal arithmetic. To improve the performance of ideal arithmetic, specialized implementations using at most a single machine word, i.e. 64-bits, or at most two machine words, i.e. 128-bits were developed. A reference implementation using GMP, that works for unbounded discriminant sizes, was developed for comparison. Our 64-bit implementation of ideal arithmetic is accurate for negative discriminants up to 59-bits in size, while our 128-bit implementation of ideal arithmetic is accurate for discriminants up to 118-bits. The related software developed for this Chapter uses the GNU C compiler version 4.7.2, and assembly language for 128-bit arithmetic. The software was developed on Ubuntu 12.10 using a personal notebook with a 2.7GHz Intel Core i7-2620M CPU and 8Gb of memory. Experiments are restricted to using only a single core of the CPU's four cores.

6.1 Specialized Implementations of Ideal Arithmetic

Throughout this thesis, an ideal class $[\mathfrak{a}]$ is represented using the $\mathbb{Z}$-module for the reduced ideal representative $\mathfrak{a} = [a, (b + \sqrt{\Delta})/2]$. Ideal class multiplication and ideal reduction use the value $c = (b^2 - \Delta)/4a$, which is also useful in determining if an ideal is an ambiguous ideal[1]. For this reason, our implementation represents an ideal class using the triple (a, b, c). We also maintain a representation of the group[2], which includes the discriminant Δ.

In Subsections 2.5.5, 2.5.6, and 2.5.7 we gave algorithms for fast ideal class multiplication,

[1]Recall that an ideal is ambiguous if $b = 0$, $a = b$, or $a = c$.

[2]The group representation also includes all intermediate integers needed for use by the GMP library. The reason for this is that GMP integers are managed on the heap, and preallocating them alongside the representation of the group reduces the overhead of managing them during ideal class group operations.

squaring, and cubing. These compute a termination bound for the partial extended GCD useful for computing partially reduced coefficients of the product ideal class. In all cases, the termination bound contains the coefficient $|\Delta/4|^{1/4}$. Since the coefficients of the partial extended GCD are integers, we instead compute $\left\lceil|\Delta/4|^{1/4}\right\rceil$ as well as $\left\lceil|\Delta/4|^{1/2}\right\rceil$ and store both in our representation of the class group. The reason we store $\left\lceil|\Delta/4|^{1/2}\right\rceil$ is that the termination bound for ideal multiplication is

$$\sqrt{a_1/a_2}|\Delta/4|^{1/4} = \sqrt{(a_1/a_2)|\Delta/4|^{1/2}} \approx \sqrt{(a_1/a_2)\left\lceil|\Delta/4|^{1/2}\right\rceil}.$$

For ideal squaring, the bound is simply $|\Delta/4|^{1/4}$ and for ideal cubing the bound is $\sqrt{a_1}|\Delta/4|^{1/4} \approx \sqrt{a_1\left\lceil|\Delta/4|^{1/2}\right\rceil}$. By approximating the termination bound, we can speed the arithmetic at the expense of additional reduction steps. We note here that we compute the values $\left\lceil|\Delta/4|^{1/2}\right\rceil$ and $\left\lceil|\Delta/4|^{1/4}\right\rceil$ as accurately as possible, since these are only computed once per class group and then stored with the representation of the group.

We further approximate the computation of integer square roots when computing the termination bound for fast multiplication. We note that

$$\begin{aligned} x^{1/2} &= 2^{(\log_2 x)/2} &&\approx 2^{\lfloor\lfloor\log_2 x+1\rfloor/2\rfloor} \\ \Rightarrow\ x/x^{1/2} &= x/2^{(\log_2 x)/2} &&\approx x/2^{\lfloor\lfloor\log_2 x+1\rfloor/2\rfloor}, \end{aligned}$$

where $\lfloor\log_2 x + 1\rfloor$ is the number of bits in the binary representation of x. Using this approximation, we compute the integer square root of x as roughly $\left\lfloor x/2^{\lfloor\lfloor\log_2 x+1\rfloor/2\rfloor}\right\rfloor$. This is simply a bit shift right by half the number of bits in x.

Other practical considerations are to minimize the size of variables and intermediate values, as smaller operands often lead to faster arithmetic. Recall from Subsection 2.5.2 that $|b| \le a \le \sqrt{\Delta/3}$. As such, the variables a and b only require half the memory needed to store Δ.

In our 64-bit implementation, Δ and c take 64-bits of storage, while both a and b require only 32-bits at most. As such, we take advantage of 32-bit operations when possible, such as our 32-bit implementations of the extended GCD algorithm. Similarly in our 128-bit implementation, Δ and c fit within 128-bits of storage, and both a and b fit within one 64-bit machine word. Again, we use 64-bit arithmetic when possible, and even 32-bit when operands are small. However, since intermediates may be larger, we sometimes require the full 64-bits or 128-bits of the implementation. Cubing requires even larger intermediates – our 64-bit implementation requires some 128-bit arithmetic, while our 128-bit implementation uses GMP when necessary.

To keep intermediates small, we compute using residue classes. For example, Equations 2.7 states that we can compute $U \pmod{a_1/s}$ and Equation 2.9 allows us to compute $b \pmod{2a}$. When an intermediate is known to be close to zero, we do not perform a complete division with remainder, but only add or subtract the divisor as appropriate (often using the signed mask discussed in Section 5.7). Furthermore, rather than computing the positive remainder, we typically compute the remainder that is closest to zero. The idea here is to minimize the number of bits required by intermediates in order to avoid overflows as much as possible.

In the specific case of ideal reduction (see Algorithm 2.1), one step is to compute b' such that $-a < b' \leq a$ and $b' \equiv b \pmod{2a}$. To compute $b \bmod 2a$ we effectively compute $b = q2a + r$ for $q, r \in \mathbb{Z}$ where $|r| < 2a$. We note that $q = \lfloor b/(2a) \rfloor = \lfloor (b/a)/2 \rfloor$, and instead compute $b = q'a + r'$ for $q', r' \in \mathbb{Z}$ where $|r'| < a$. Now q' is at least twice q. If q' is even, then $b = q'a + r' = (q'/2)2a + r'$ and we let $b' = r'$. Suppose q' is odd and r' is positive. Then $b = q'a + r' = (q'+1)a + (r' - a) = ((q'+1)/2)2a + (r' - a)$. Since $0 < r' < a$, we have $b' = r' - a$ and $-a < b' \leq a$. The proof is similar when q is odd and r' is negative.

This leads us to the following implementation, which we optimize to be free of conditionals. Using two's complement for fixed sized words, we compute

$$\begin{aligned}
b &= q'a + r' && \{\text{division with remainder}\} \\
q_m &= -(q \mathbin{\texttt{and}_2} 1) && \{q_m \text{ has all bits set when } q \text{ is odd}\} \\
r_m &= \neg\texttt{sign\_mask}(r) && \{r_m \text{ has all bits set when } r \geq 0\} \\
a' &= (a \oplus r_m) - r_m && \{\text{negate } a \text{ when } r_m \text{ is all set}\} \\
r &= r' + (a' \mathbin{\texttt{and}_2} q_m) && \{\text{move } r \text{ towards zero when } q \text{ is odd}\} \\
d &= r_m \mathbin{\texttt{or}_2} 1 && 1 \text{ when } r < 0 \text{ and } -1 \text{ otherwise} \\
q &= (q' - (d \mathbin{\texttt{and}_2} q_m))/2 && \{\text{adjust } q \text{ with respect to } r\}
\end{aligned}$$

and finally $b' = r$.

Since we represent an ideal class using the triple (a, b, c), it is necessary to compute a new value $c' = (b'^2 - \Delta)/4a$ after a reduction step. This can be simplified as

$$\begin{aligned}
c &= (b^2 - \Delta)/4a \\
&= ((2aq + r)^2 - \Delta)/4a \\
&= (4a^2q^2 + 4aqr + r^2 - \Delta)/4a \\
&= (r^2 - \Delta)/4a + aq^2 + qr \\
&= c' + q(aq + r) \\
&= c' + q(2aq + r - aq) \\
&= c' + q(b - aq) \\
&= c' + q(b + r)/2.
\end{aligned}$$

As such, we have

$$c' = c - q(b + r)/2.$$

Note, the last step above is obtained by rewriting $b = 2aq + r$ as

$$\begin{aligned} b - 2aq &= r \\ 2b - 2aq &= b + r \\ b - aq &= (b + r)/2. \end{aligned}$$

Since $b - aq \in \mathbb{Z}$, the divide by 2 can be performed with an arithmetic bit shift right. (TODO: Is this method of computing c' published anywhere?)

We further improve ideal arithmetic by noting that multiplication computes

$$s = \gcd(a_1, a_2, (b_1 + b_2)/2) = Ya_1 + Va_2 + W(b_1 + b_2)/2$$

(this is Equation 2.6 from Subsection 2.5.4). Our implementations of ideal multiplication (Algorithm 2.2) performs this in two parts: the first computes $s' = \gcd(a_1, a_2) = Y'a_1 + V'a_2$ and the second only computes $s = \gcd(s', (b_1 + b_2)/2) = Vs' + W(b_1 + b_2)/2$ when $s' \neq 1$. We do this since checking for $s \neq 1$ is relatively inexpensive when compared to performing an extended GCD computation. In addition, we note that the coefficient Y' is not used in order to derive the product ideal, and so we drop the corresponding term from our GCD computation. Lastly, we use our simplified left-to-right binary GCD to compute partially reduced coefficients of the product ideal when the operands are between 32-bits and 64-bits (since this GCD algorithm is unimodular and performed fastest in this range).

The final performance improvement is for generating prime ideals. For a given prime p, we would like to find an ideal of the form $[p, (b + \sqrt{\Delta})/2]$. We have $b^2 - 4pc = \Delta$, and so we take everything in the residue class modulo p and get $b^2 \equiv \Delta \pmod{p}$ or $b \equiv \pm\sqrt{\Delta} \pmod{p}$. Computing b is a matter of computing a square root modulo a prime, if one exists. There are efficient algorithms for this (see [8]), but since we are interested in finding some prime ideal, rather than a specific prime ideal, we instead precompute all square roots modulo each prime p for sufficiently many small p. For our purposes, all primes $p < 1000$ was enough. Finding $b \equiv \pm\sqrt{\Delta} \pmod{p}$ is now a table lookup. Having found a value for b, we have not necessarily found a prime ideal $[p, (b + \sqrt{\Delta})/2]$. Since $\Delta = b^2 - 4pc$, this implies that $c = (b^2 - \Delta)/4p$ must have an integral solution. Our implementation maintains the value c for an ideal class, so we compute c and if c is an integer, than we have found a prime ideal. Otherwise, we try again for some other prime (usually the smallest prime greater than p).

6.2 Average time for operations

This Subsection demonstrates the performance of our implementations of ideal class arithmetic. Let k be the target number of bits in the discriminant Δ. We iterate k from 16 to 140, and for each k we repeat the following 10,000 times: We compute two prime numbers p and q such that p is $\lfloor k/2 \rfloor$ bits and q is $k - \lfloor k/2 \rfloor$ bits. We use the negative of their product $\Delta = -pq$ as the discriminant for a class group, unless $\Delta \not\equiv 1 \pmod 4$. In which case, we try again with a different p and q. We then pick a prime form, $[\mathfrak{a}]$, randomly from among the primes less than 1000. To time the performance of squaring and cubing, we iterate 1000 times either $[\mathfrak{a}] \leftarrow [\mathfrak{a}^2]$ or $[\mathfrak{a}] \leftarrow [\mathfrak{a}^3]$ respectively. Dividing the total cost by 10,000,000 gives the average time to square or cube an ideal. For multiplication, we initially set $[\mathfrak{b}] \leftarrow [\mathfrak{a}]$. We then iterate 1000 times the sequence of operations $[\mathfrak{c}] \leftarrow [\mathfrak{a}\mathfrak{b}]$, $[\mathfrak{a}] \leftarrow [\mathfrak{b}]$, and $[\mathfrak{b}] \leftarrow [\mathfrak{c}]$. Figures 6.1, 6.2, and 6.3 show the results of these timings. For all discriminant sizes, our 64-bit implementation performs faster than our 128-bit implementation, which performs faster than our GMP implementation.

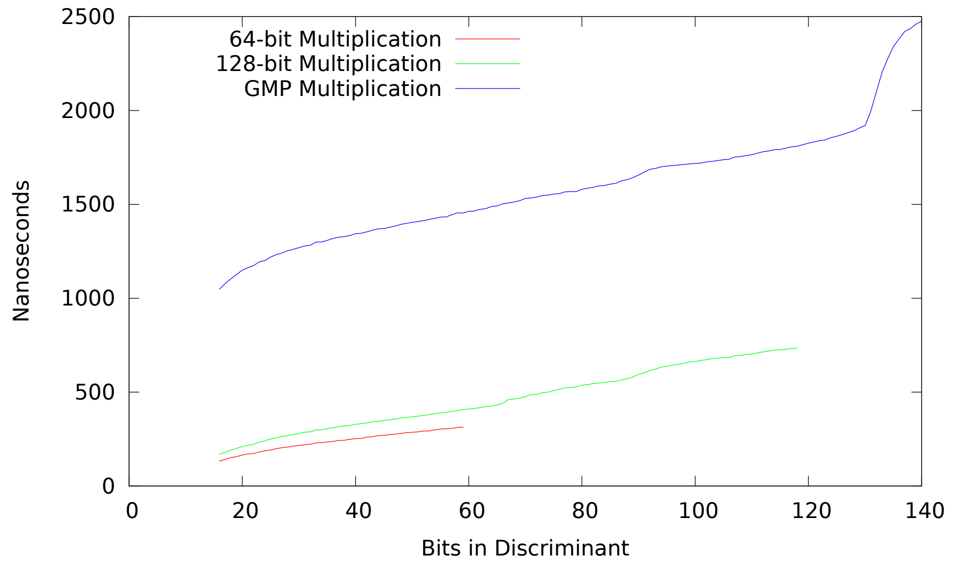


Figure 6.1: Average Time to Multiply Reduced Ideal Class Representatives.

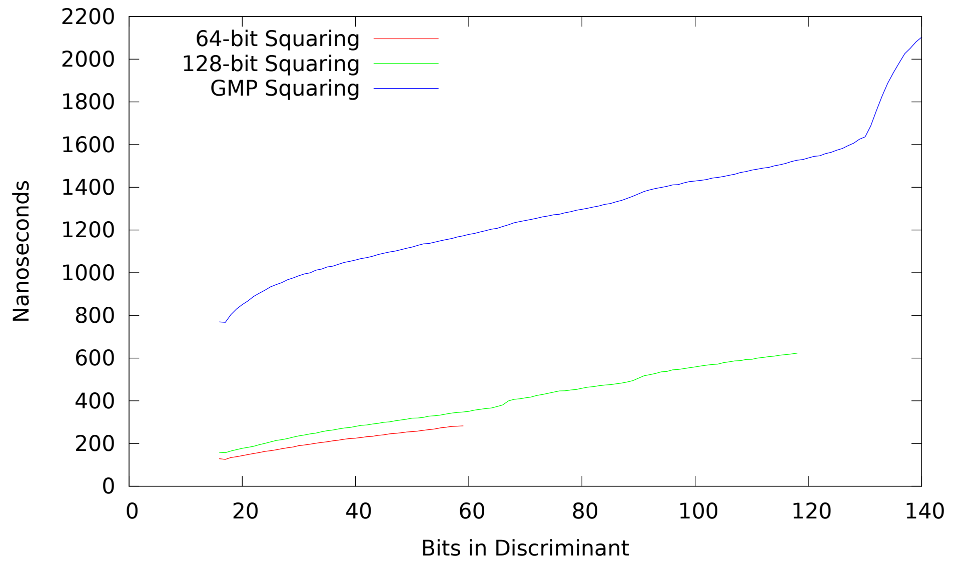


Figure 6.2: Average Time to Square Reduced Ideal Class Representatives.

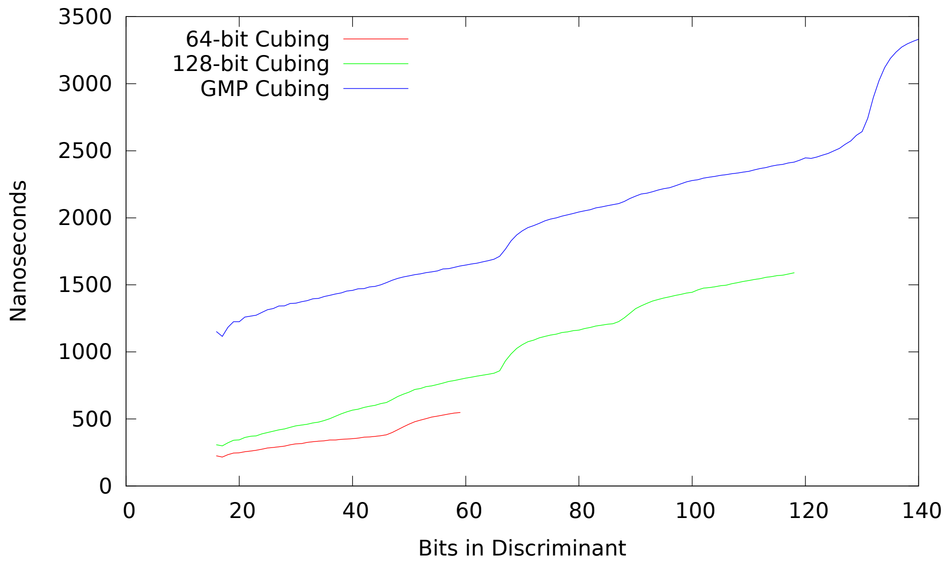


Figure 6.3: Average Time to Cube Reduced Ideal Class Representatives.

In Figures 6.4, 6.5, and 6.6 we compare the average time to cube against the average time to multiply a representative with its square. One thing to notice is that our 128-bit implementation of cubing performs more poorly than that of multiplying an ideal with its square. This is likely because we rely on GMP integers for overflow. Contrast this to our 64-bit implementation that does not use GMP at all, and our GMP implementation that only uses GMP for arithmetic – in both of these implementations, cubing is faster than multiplying an ideal with its square.

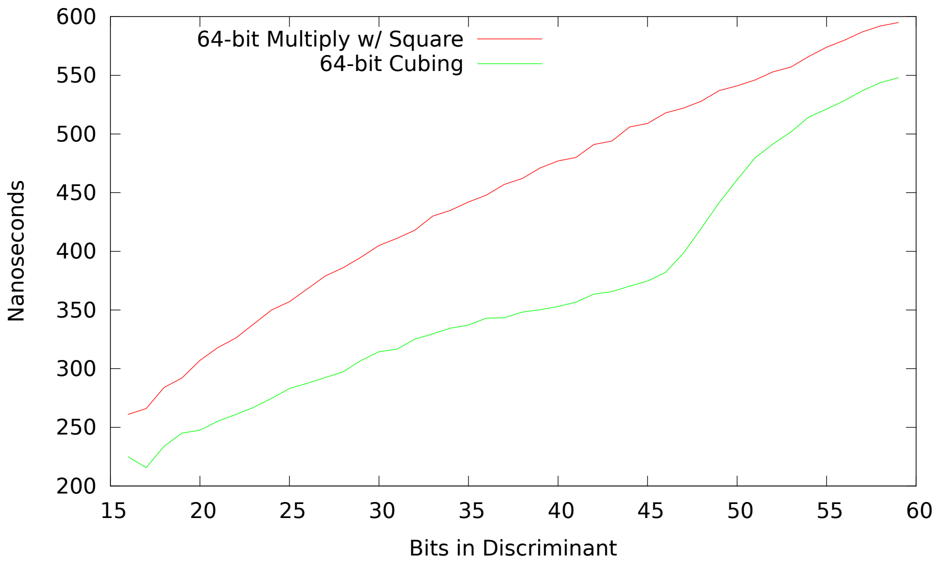


Figure 6.4: Time to compute $[\mathfrak{a}^3]$ in our 64-bit implementation.

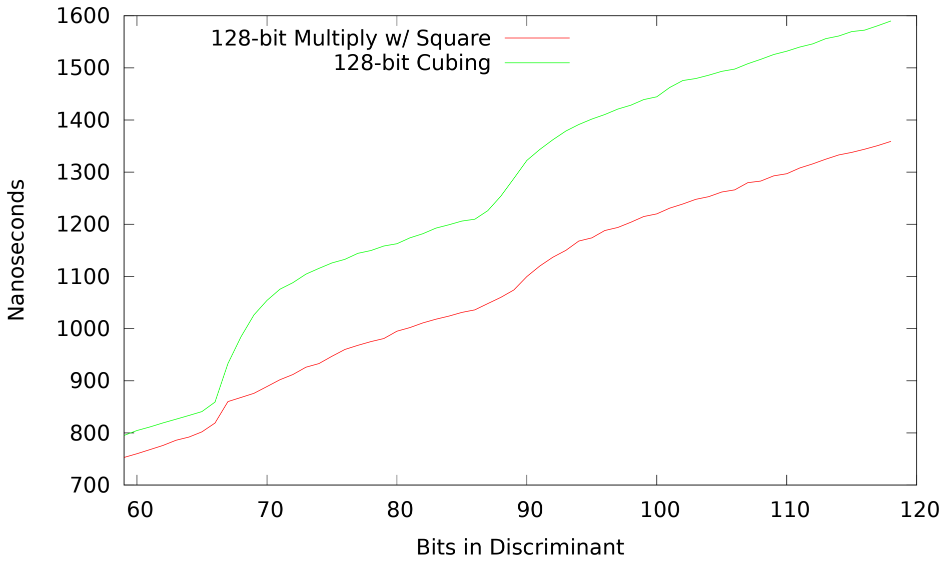


Figure 6.5: Time to compute $[\mathfrak{a}^3]$ in our 128-bit implementation.

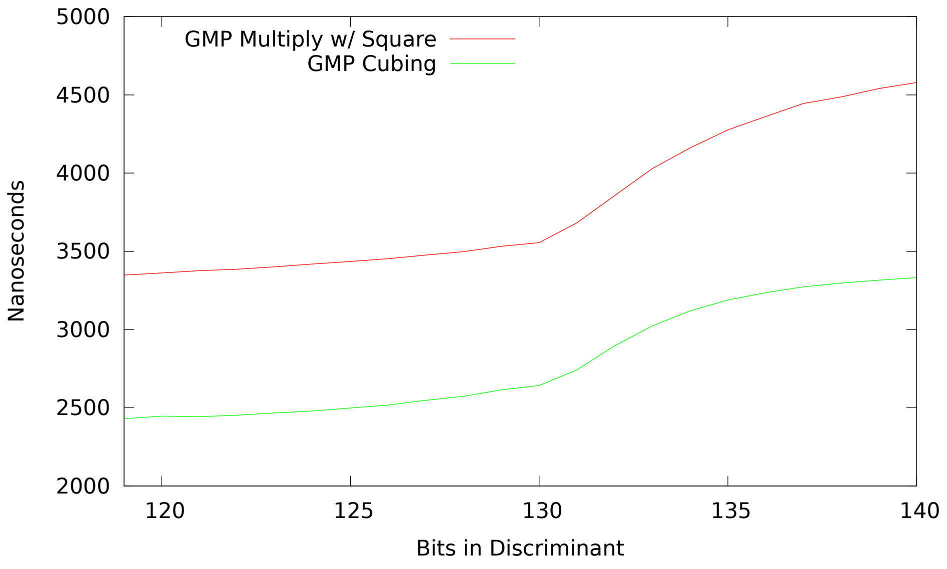


Figure 6.6: Time to compute $[\mathfrak{a}^3]$ in our GMP implementation.

Following this, we discussed specialized implementations of ideal arithmetic using 64-bit, 128-bit, and unbound arithmetic. Our 64-bit implementation is known to work correctly for negative discriminants $-2^{60} < \Delta < 0$, while our 128-bit implementation works with negative discriminants $-2^{119} < \Delta < 0$. We discussed several low-level optimizations and showed an improvement in the performance of ideal class arithmetic over our reference implementation using GMP.

Lastly, this Chapter measured the average cost of multiplication, squaring, and cubing for varying discriminant sizes. The next Chapter uses our implementation of arithmetic in the ideal class group in order to determine fast methods of exponentiation in practice. We discuss methods for exponentiating not discussed previously in this thesis – many of which take the average time to multiply, square, and cube into consideration.

Chapter 7

Exponentiation Experiments

Section 4.2 discussed the bounded primorial steps algorithm – an algorithm that finds the order of an element by exponentiating it to the product of many primes. Since this exponent is determined by a given bound, the algorithm benefits from precomputation of representations that lead to efficient exponentiation in practice. Section 4.3 introduced the SuperSPAR integer factoring algorithm, for which a bound on the group size and the order of an element lead to the factorization of an integer. Representations that lead to efficient exponentiation in practice improve the performance of the SuperSPAR factoring algorithm, as well any algorithm based on the bounded primorial steps algorithm, or one that uses exponentiation for fixed exponents.

This chapter discusses several approaches to exponentiating an ideal class representative to a large exponent, and in particular, large exponents that are the product of all primes less than some bound[1] and are known in advance. We begin by recalling exponentiation techniques from Chapter 3. These include techniques that use signed and unsigned base 2 representations, greedy right-to-left and left-to-right double base representations (for bases 2 and 3), and a tree-based approach. We also consider several extensions to these. For small exponents (16-bits or less), we are able to exhaustively compute all representations under certain constraints. This allows us to use larger exponents by partitioning the large exponent into 16-bit blocks or by using its factorization. Finally, we compare each method on a sequence of primorials to find the best method in practice.

In the previous Chapter, we discussed our implementations of ideal class arithmetic using 64-bit and 128-bit operations. For our 64-bit implementation, the largest discriminants supported are those that fit within 59-bits, and for our 128-bit implementation, the largest

[1]Such products are called *primorials* and are discussed in Section 4.2.

discriminants fit within 118-bits. These represent an upper bound on the average cost of arithmetic operations within each implementation. As such, our exponentiation experiments focus on improving the time to exponentiate assuming the average cost of operations for 59-bit and 118-bit discriminants.

7.1 Binary and Right-to-Left Non-Adjacent Form

In Sections 3.1 and 3.2 we discussed binary exponentiation and non-adjacent form exponentiation in detail. Briefly again, binary exponentiation uses the binary representation of an exponent n. The representation can be parsed from high-order to low-order or from low-order to high-order – we typically refer to this difference as left-to-right or right-to-left respectively. Using either approach, we use $\lfloor \log_2 n \rfloor$ squares and $\lfloor \log_2 n \rfloor / 2$ multiplications on average.

A non-adjacent form exponentiation uses a signed base 2 representation of the exponent such that no two non-zero terms are adjacent[2]. Similarly, when computing a non-adjacent form we can parse the exponent from left-to-right or from right-to-left. Either direction, we use $\lfloor \log_2 n \rfloor + 1$ squares and $(\lfloor \log_2 n \rfloor + 1)/3$ multiplications on average.

7.2 Right-to-Left 2,3 Chains

In Subsection 3.4.1, we described a method for computing 2,3 chains from low-order to high-order that is a natural extension of the binary representation or non-adjacent form of an exponent. In this method, we reduce the exponent n by 2 while it is even, and by 3 while it is divisible by 3. At which point either $n \equiv 1 \pmod 6$ or $n \equiv 5 \pmod 6$ and we add or subtract 1 so that n is a multiple of 6. The resulting partition of n is then reversed such that the number of squares or cubes in successive terms is monotonically increasing and we

[2]Non-adjacent form is written as $n = \prod s_i 2^i$ for $s_i \in \{0, -1, 1\}$. By "non-adjacent" we mean that $s_i \cdot s_{i+1} = 0$ for all i.

can use Algorithm 3.2 from Chapter 3 to compute the exponentiation.

Since this approach evaluates the exponent modulo 3 and may reduce the exponent by 3, efficient methods to compute $n \bmod 3$ and $n/3$ will speed the computation of the chain. Notice that $4 \equiv 1 \pmod 3$. As such, we can write n as

$$n = 4 \lfloor n/4 \rfloor + (n \bmod 4) \equiv \lfloor n/4 \rfloor + (n \bmod 4) \pmod 3$$

and then recursively write $\lfloor n/4 \rfloor \pmod 3$ the same way. This provides us with a method to quickly compute $n \bmod 3$ – we partition the binary representation of n into 2-bit blocks and sum each block modulo 4. The resulting sum s is $s \equiv n \pmod 3$. We further improve the performance of this algorithm by noting that $4^m \equiv 1 \pmod 3$. Since our target architecture (and language) has 64-bit words, we partition the binary representation into 64-bit blocks and sum each block modulo 2^{64}. We then add each 32-bit word of the resulting sum modulo 2^{32}, then each 16-bit word of the sum modulo 2^{16}, and finally each 8-bit word modulo 2^8. We look up the final answer modulo 3 from a table of 256 entries (see Algorithm 7.1).

Algorithm 7.1 Fast $n \bmod 3$ (adapted from Hacker's Delight [48]).

```
Input: $n \in \mathbb{Z}$.
Output: $n \bmod 3$.
1: $s \leftarrow 0$
2: for $i$ from 0 to $\lfloor \log_2 n \rfloor$ by 64 do
3:     $t \leftarrow \lfloor n/2^i \rfloor \bmod 2^{64}$
4:     $s \leftarrow (s + t) \bmod 2^{64}$
5: end for
6: $s \leftarrow (s + \lfloor s/2^{32} \rfloor) \bmod 2^{32}$
7: $s \leftarrow (s + \lfloor s/2^{16} \rfloor) \bmod 2^{16}$
8: $s \leftarrow (s + \lfloor s/2^{8} \rfloor) \bmod 2^{8}$
9: return $s \bmod 3$                {Lookup from a table with 256 entries.}
```

Division by 3 is relatively expensive when compared to computing the remainder. A common approach is to precompute a single word approximation of the inverse of 3, and then to use multiplication by an approximation of the inverse and then to adjust the result (see [24, 48, 37] for additional information). As the GNU Multiple Precision (GMP) library implements exact division by 3, we use this.

7.3 Windowed Right-to-Left Chains

Windowing improves the performance of right-to-left binary exponentiation and right-to-left binary GCD computations. Similarly, we use windowing to improve the performance of a right-to-left 2,3 chain. Specifically, we experimented with a window size of $2^2 3^2$. Again, while the exponent is even, we reduce it by 2, and while it is divisible by 3, we reduce it by 3. In a non-windowed variant, we add or subtract 1 to make the remainder a multiple of 6. In the windowed variant, we evaluate the exponent n modulo the window $2^2 3^2 = 36$, which gives us $n \equiv 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35 \pmod{36}$. As there are 12 different residue classes, and for each residue class we could either add or subtract 1 from n, we have 2^{12} different strategies to evaluate. For each strategy, we measured the cost to exponentiate the primorials P_{100k} for $1 \leq k \leq 50$. For 48 out of 50 of the primorials tested, the same strategy lead to the cheapest cost of exponentiation[3], which was to subtract 1 from n when $n \equiv 1, 5, 13, 17, 25, 29 \pmod{36}$ and to add 1 otherwise.

Since the windowed variant of a 2,3 chain computes $n \bmod 36$, we give a fast method for this. First write $n = 4x + r_4$ for integers x and r_4 such that $0 \leq r_4 < 4$. Then write $x = 9y + r_9$ for integers y and r_9 such that $0 \leq r_9 < 9$. Substituting the second equation into the first we have

$$\begin{aligned} n &= 4(9y + r_9) + r_4 \\ &= 36y + 4r_9 + r_4. \end{aligned}$$

Notice that $(4r_9 + r_4)$ is $n \bmod 36$ where $r_4 = n \bmod 4$ and $r_9 = \lfloor n/4 \rfloor \bmod 9$. To compute $n \bmod 9$, we point out that $64 \equiv 1 \pmod{9}$. Similar to the case of computing $n \bmod 3$, we write

$$n = 64 \lfloor n/64 \rfloor + (n \bmod 64) \equiv \lfloor n/64 \rfloor + (n \bmod 64) \pmod{9}$$

and recursively write $\lfloor n/64 \rfloor \pmod{9}$. To compute $n \bmod 9$, we partition n into blocks of

[3]For the primorial P_{200}, this strategy was the third most efficient, and for P_{500} it was the second most efficient.

6-bits (since $2^6 = 64$) and sum each 6-bit block modulo 64. We then compute the sum $s \bmod 9$. Again, since our target architecture has 64-bit machine words, we improve upon this by first partitioning n into 192-bit blocks[4] and compute an intermediate sum of each 192-bit block. We then partition the intermediate sum into 6-bit blocks and compute the final solution.

7.4 Left-to-Right 2,3 Representations and Chains

In Subsection 3.4.2 we described a greedy algorithm for computing 2,3 representations from high-order to low-order. Briefly, for a given exponent n and for $a_i, b_i \in \mathbb{Z}_{\geq 0}$ and $s_i \in \{-1, 1\}$, we compute the term $s_i 2^{a_i} 3^{b_i}$ such that $\left|n - s_i 2^{a_i} 3^{b_i}\right|$ is as small as possible. We then recurse on the result $n - s_i 2^{a_i} 3^{b_i}$. As is, this produces unchained representations, but a chain can be generated by restricting each a_i and b_i such that it is no greater than the a_{i-1} and b_{i-1} from the previous term. Placing a bound on the number of squares and cubes can also be done globally, i.e. for every a_i, b_i we have $0 \leq a_i \leq A$ and $0 \leq b_i \leq B$. When a bound is applied globally, the cost of a left-to-right chain or representation varies as the global bound varies.

Figure 7.1 shows the time to exponentiate using a precomputed left-to-right representation for an exponent that is the product of the first 1000 primes (a number with 11271 bits). The horizontal axis indicates a global bound A such that all $a_i \leq A$. A global bound B is chosen for the exponent n such that $B = \lceil \log_3(n/2^A) \rceil$. The end points of the graph correspond to a representation that uses only cubing and multiplication (on the left side) and a representation that uses only squaring and multiplication (on the right side).

[4]We use 192-bit blocks since a 64-bit machine word evenly partitions a 192-bit block and $2^{192} \equiv 1 \pmod 9$.

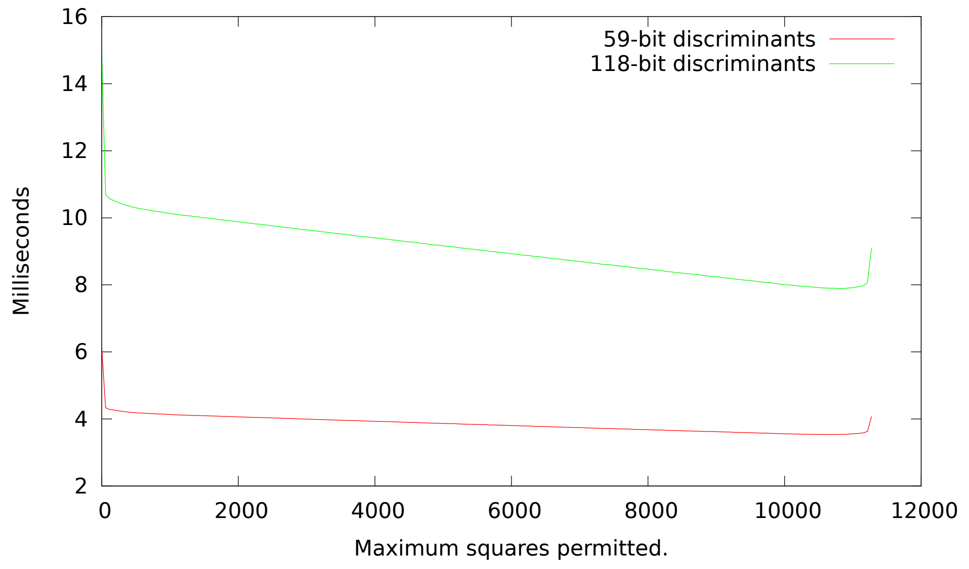


Figure 7.1: The time to exponentiate the 1000th primorial, n, while varying the maximum number of squares permitted, A. The maximum number of cubes is $B = \lceil \log_3(n/2^A) \rceil$.

In general, bounding the maximum number of squares and cubes give representations that lead to faster exponentiation in the ideal class group than representations where the number of squares or cubes is left unbound. For this particular exponent, a representation generated without a global bound takes approximately 7.3 milliseconds for a 59-bit discriminant and 17.2 milliseconds for a 118-bit discriminant. This is slower than all bounded representations for both implementations.

7.5 Greedy Pruned Trees

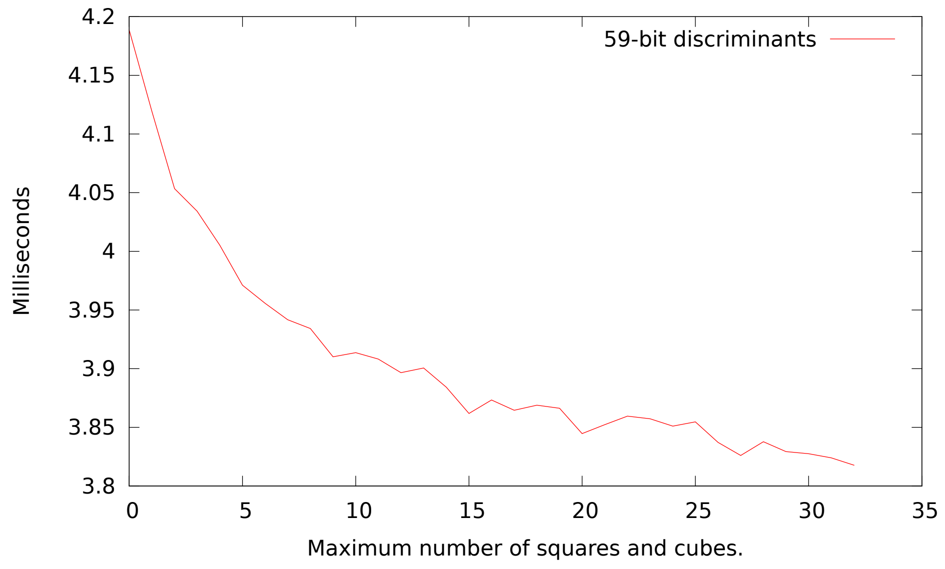
A right-to-left 2,3 chain can be generated by repeatedly reducing the exponent by 2 and 3 and then either adding or subtracting 1 and repeating this process until the exponent is 1. In the windowed variant, after reducing the exponent by 2 and 3, we had 12 residues modulo $2^2 3^2$ and this lead to 2^{12} different strategies for adding or subtracting 1 from the residue.

In Subsection 3.4.3, we discussed a tree based method where a set of at most L *partial representations* are maintained (a partial representation can be written as $n = x + \sum s_i 2^{a_i} 3^{b_i}$).

At each iteration, the x term from each partial representation generates two new elements $x-1$ and $x+1$. After reducing each new element by powers of 2 and 3, only the L smallest are kept. More formally, an element x generates new integral elements $(x \pm 1)/(2^c 3^d)$.

Here we consider two variations to the approach of maintaining the L best[5] partial representations. The first variation we consider is to generate several new nodes with integer values of the form $(x \pm 2^a 3^b)/(2^c 3^d)$, while the second variation is to include two terms such that each node generates values of the form $(x \pm 2^a \pm 3^b)/(2^c 3^d)$. Notice that the first variation includes the forms $(x \pm 1)/(2^c 3^d)$ and so tends to give representations no worse than the method suggested by Doche and Habsieger [21] (covered in Subsection 3.4.3). The assumption is that by adjusting x by more than just 1, we increase the likelihood of finding a multiple of a large $2^c 3^d$ window.

[5]We say that a partial representation is *better* when the x term is smaller, or if the x terms are equal, when the cost of the 2,3 summation is less.



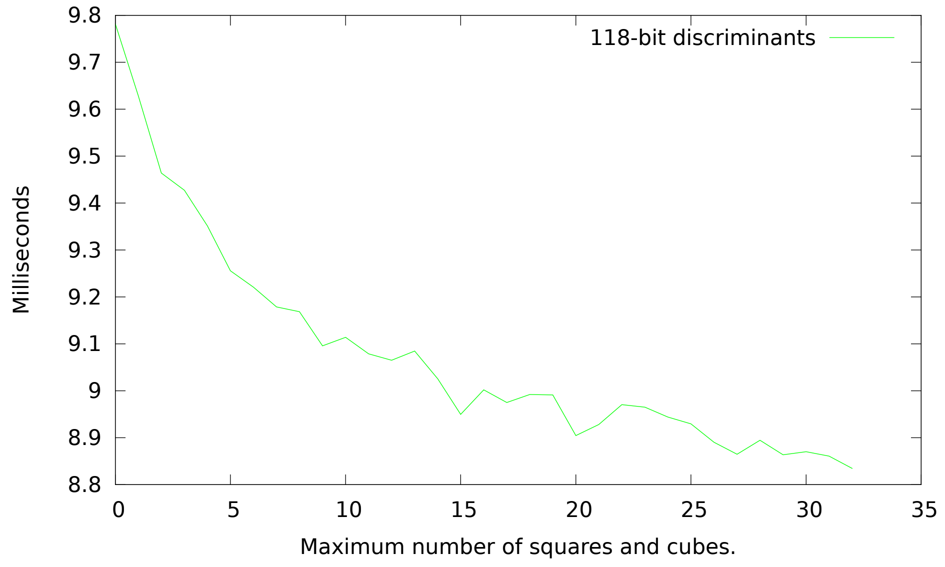


Figure 7.2: Performance of varying the bounds $a, b \leq U$ on $(x \pm 2^a 3^b)/(2^c 3^d)$ when exponentiating by the primorial P_{1000}.

For both variations, we bound a and b such that $0 \leq a \leq U$ and $0 \leq b \leq U$. Figure 7.2 shows the average time to exponentiate by the 1000th primorial as the bound U increases (using the $k = 4$ best partial representations). As U increases, computing representations using this approach quickly becomes intractable. We found that for our purposes, $U = 16$ is an acceptable trade off between the average time to exponentiate and the time to generate the 2,3 representation.

7.6 The L Best Approximations

The approach of maintaining a set of the L best partial representations of an exponent can be adapted to that of the left-to-right 2,3 representation from Subsections 3.4.2 and 7.4. For an integer x we say that 2^a3^b is a best approximation of $|x|$ when $\left||x| - 2^a3^b\right|$ is minimal. The algorithm for the left-to-right representation (Subsection 3.4.2) finds a best approximation for x and then repeats on the positive difference. However, instead of only iterating on the best approximation, each value from the set of partial representations generates new values of the form $\left||x| - 2^a3^b\right|$ (being careful to record the sign of x), and the L best partial representations are retained. In this case, we iterate b from $0 \le b \le B$ and let $a_1 = \lfloor \log_2(x/3^b) \rfloor$ and $a_2 = \lceil \log_2(x/3^b) \rceil$ bounding both $a_1, a_2 \le A$. Note that using $a_2 = a_1 + 1$ is sufficient since either $\lceil \log_2(x/3^b) \rceil = \lfloor \log_2(x/3^b) \rfloor$ or $\lceil \log_2(x/3^b) \rceil = \lfloor \log_2(x/3^b) \rfloor + 1$. We then use $\left||x| - 2^{a_1}3^b\right|$ and $\left||x| - 2^{a_2}3^b\right|$ as candidates for the new set. As before, iterating the bound on the number of squares and cubes varies the cost of the representations generated.

7.7 Additive 2,3 Chains

Imbert and Philippe [27] give a method (see Subsection 3.4.4) to compute the shortest additive strictly chained 2,3 partition, suitable for smaller integers. Such partitions do not permit subtraction and every term is strictly less than and divides all subsequent terms. They take the form

$$n = \sum_{i=0}^{k} 2^{a_i}3^{b_i}$$

for $a_i, b_i \in \mathbb{Z}_{\ge 0}$ where $2^{a_i}3^{b_i}$ divides $2^{a_j}3^{b_j}$ and $a_i < a_j$ and $b_i < b_j$ for all $i < j$.

For our purposes, we modified this algorithm to compute additive 2,3 chains that minimize the average cost of arithmetic in the ideal class group – the resulting additive 2,3 chains give a better average time for exponentiation, while they are not necessarily the shortest possible.

Let M, S, and C be the average cost to multiply, square, and cube respectively. Our modified function is as follows

$$s'(n) = \begin{cases} \min\{S + s'(n/2), C + s'(n/3)\} & \text{when } n \equiv 0 \pmod 6 \\ M + s'(n-1) & \text{when } n \equiv 1 \pmod 6 \\ S + s'(n/2) & \text{when } n \equiv 2 \pmod 6 \\ \min\{C + s'(n/3), M + S + s'((n-1)/2)\} & \text{when } n \equiv 3 \pmod 6 \\ \min\{S + s'(n/2), M + C + s'((n-1)/3)\} & \text{when } n \equiv 4 \pmod 6 \\ M + S + s'((n-1)/2) & \text{when } n \equiv 5 \pmod 6 \end{cases}$$

where $s'(1) = 0$, $s'(2) = S$, and $s'(3) = C$ are the base cases.

We also experimented with computing 2,3 strictly chained partitions that allow for both positive and negative terms. The corresponding function we used is

$$f(n) = \begin{cases} \min\{S + f(n/2), C + f(n/3)\} & \text{when } n \equiv 0 \pmod 6 \\ \min\{M + f(n-1), M + S + f((n+1)/2)\} & \text{when } n \equiv 1 \pmod 6 \\ \min\{S + f(n/2), M + C + f((n+1)/3)\} & \text{when } n \equiv 2 \pmod 6 \\ \min\{C + f(n/3), M + S + f((n-1)/2), \\ \qquad M + S + f((n+1)/2)\} & \text{when } n \equiv 3 \pmod 6 \\ \min\{S + f(n/2), M + C + f((n-1)/3)\} & \text{when } n \equiv 4 \pmod 6 \\ \min\{M + f(n+1), M + S + f((n-1)/2)\} & \text{when } n \equiv 5 \pmod 6 \end{cases}$$

again, where $f(1) = 0$, $f(2) = S$, and $f(3) = C$ are the base cases. One thing to notice is that the function s' computes a subset of the representations computed by the function f. As such, we expect the average cost to exponentiate using a representation computed by f to be no worse than the average cost to exponentiate using a representation computed by s.

7.8 Incremental Searching

For small inputs, the number of additive 2,3 chains is sufficiently reduced that we can compute all such chains in order to find the fastest. Here we consider a different approach to searching for representations – for a function generating a set of representations, we record the cheapest representation for each integer represented by the set.

We first iterate over all single term representations $2^{a_1}3^{b_1}$ for $0 \leq a_1 \leq A$ and $0 \leq b_1 \leq B$, and then all two term representations $2^{a_1}3^{b_1} \pm 2^{a_2}3^{b_2}$ for $0 \leq a_1 < a_2 \leq A$ and $0 \leq b_1 < b_2 \leq B$. In general, we compute the set of representations

$$R = R_1 \cup R_2 \cup ... \cup R_m$$

for some maximum number of terms m where

$$R_k = \left\{ \sum_{i=1}^{k} \pm 2^{a_i}3^{b_i} \;:\; 0 \leq a_1 < \cdots < a_k \leq A \text{ and } 0 \leq b_1 < \cdots < b_k \leq B \right\}.$$

We iterate over the set R and for each integer represented, we record the lowest cost representation for that integer in R.

In our experiments, we search for representations for 16-bit integers. We intially chose $A = \lceil \log_2(2^{16}) \rceil = 16$, $B = \lceil \log_3(2^{16}) \rceil = 11$, and iterated the number of terms k from 1 through 5. For representations of $k = 6$ terms, our implementation did not complete after a week of execution. We then ran our search again using $A = 18$ and $B = 12$ and found that none of our minimal representations were improved.

Since both the incremental search of this Subsection and the two functions from the previous Subsection are computationally expensive, we are only able to compute chains for small exponents. This is still useful when we consider methods that partition large exponents into smaller blocks using their binary representation, or when we consider multiple exponentiations by a list of prime powers.

7.9 Big Exponents from Small Exponents

The techniques of the previous two Subsections are computationally expensive and as such, we limit our search to representations of 16-bit integers. One way that we use such representations is to write the exponent n in 16-bit blocks as

$$n = \sum_{i=0}^{k} 2^{16i} b_i$$

where $0 \le b_i < 2^{16}$. Assuming that we can exponentiate a group element g to a 16-bit exponent b_i, Algorithm 7.2 computes the exponentiation g^n using an approach similar to a left-to-right windowed binary exponentiation.

Algorithm 7.2 16-bit Blocked Exponentiation.

Input: $n \in \mathbb{Z}, g \in G$ and a method to compute g^{b_i} for $0 \le b_i < 2^{16}$.

Output: g^n.

```
1: $R \leftarrow 1_G$
2: for $i$ from $\lceil \log_{2^{16}} n \rceil$ downto 0 do
3:     $R \leftarrow R^{2^{16}}$                                  {By repeated squaring.}
4:     $b_i \leftarrow \lfloor n / 2^{16i} \rfloor \bmod 2^{16}$
5:     $R \leftarrow R \cdot g^{b_i}$
6: end for
7: return $R$
```

Another way we can use 16-bit representations is when we know the prime factorization of the exponent n and n is the product of primes smaller than 2^{16}. Since we are interested in exponentiation by primorials (i.e. the product of the first w primes), the prime factorization is trivial. Given a primorial $P_w = \prod_{i=1}^{w} p_i$ where p_i is the ith prime, we can compute g^{P_w} as $(((g^{p_1})^{p_2})^{\cdots})^{p_w}$ using a series of w small exponentiations.

7.10 Experimental Results

One reason to improve the performance of exponentiation in the ideal class group is to improve the performance of order finding in this group. In particular, we exponentiate a random ideal class to a primorial so that the order of the resulting ideal class is likely to be coprime to our exponent.

Two of the techniques in the previous section compute g^n using a series of smaller exponentiations g^b such that $0 \leq b < 2^{16}$. So we begin by determining the best method to exponentiate using 16-bit exponents. To do so, we compute the average time to exponentiate for exponents 1 through 65535 using 59-bit and 118-bit discriminants. Table 7.1 shows the number of exponents for which each method was the fastest[6]. For each exponent, we then

Method	59-bit Discriminants	118-bit Discriminants
Left-to-Right 2,3 Representation	2536	7097
4 Best $\left\lvert \lvert x\rvert - 2^a3^b \right\rvert$	9091	7230
4 Best $(x \pm 2^a3^b)/(2^c3^d)$	47969	45468
4 Best $(x \pm 2^a \pm 3^b)/(2^c3^c)$	3333	2756
Recursive $\sum 2^a3^b$ Chains	2406	2970
Incremental Search	199	13

Table 7.1: The number of 16-bit exponents where an exponentiation technique was fastest.

normalized the time of each method relative to the best time. Table 7.2 shows the average of these normalized times. The method that maintains the 4 best partial representations of the form $(x \pm 2^a3^b)/(2^c3^d)$ was the best performer in general. However, since we were interested in precomputing 16-bit representations for use with a block exponentiation and exponentiation by a list of prime factors, we used the best representation available for each exponent.

To determine the best method to exponentiate a random ideal by a primorial, we compute the average time to exponentiate for the primorials P_{250k} for $1 \leq k \leq 100$. We categorized the different exponentiation techniques as those that use only base 2, those that generate 2,3

[6]The methods not listed in this table were not the fastest for any exponents.

Method	59-bit Discriminants	118-bit Discriminants
Binary	1.48864	1.44287
Right-to-Left Non-Adjacent Form	1.39605	1.34547
Right-to-Left 2,3 Chain	1.35869	1.37595
$2^2 3^2$ Windowed Right-to-Left 2,3 Chain	1.38676	1.37415
Left-to-Right 2,3 Representation	1.27775	1.23781
4 Best $\lvert \lvert x\rvert - 2^a 3^b\rvert$	1.19508	1.17034
4 Best $(x \pm 1)/(2^c 3^d)$	1.23152	1.22800
4 Best $(x \pm 2^a 3^b)/(2^c 3^d)$	1.03227	1.03886
4 Best $(x \pm 2^a \pm 3^b)/(2^c 3^c)$	1.37963	1.38966
Recursive $\sum 2^a 3^b$ Chains	1.28606	1.26822
Recursive $\sum \pm 2^a 3^b$ Chains	1.21295	1.18712
Incremental Search	1.19495	1.17059

Table 7.2: Normalized time to exponentiate 16-bit exponents.

chains from right-to-left, from left-to-right, that add or subtract to a partial representation and then reduce by $2^c 3^d$, and those that make use of the best 16-bit representations. We then compared the average time to exponentiate each method from a category, and finally compared the best performers of each category to determine the best performer overall.

We found that for both our 64-bit and 128-bit implementations and for all primorials tested, the method of iterating on the 4 best $\lvert \lvert x\rvert - 2^a 3^b\rvert$ approximations leads to representations with the fastest time to exponentiate. This is in contrast to the method of iterating on the 4 best partial representations $(x \pm 2^a 3^b)/(2^c 3^d)$ that lead to the best timings for 16-bit integers. Naturally, we can improve these results by iterating on the L best partial representations for $L > 4$ at the expense of longer precomputation.

Figures 7.3 and 7.4 compare binary exponentiation against right-to-left non-adjacent form representation. The non-adjacent form representation leads to faster exponentiations in all cases. Figures 7.5 and 7.6 compare the non-windowed right-to-left 2,3 chain method to the $2^2 3^2$ windowed method. The $2^2 3^2$ windowed method out performs the non-windowed method for all exponents. Figures 7.7 and 7.8 compare left-to-right 2,3 representations with that of maintaining the 4 best $\lvert \lvert x\rvert - 2^a 3^b\rvert$ approximations. In this case, maintaining the 4 best approximations performs best. Figures 7.9 and 7.10 compare the three different techniques of adding or subtracting a value to a partial representation and then reducing by a power of 2 and 3. Here, computing candidates $(x - 2^a 3^b)/(2^c 3^d)$ leads to representations that exponentiate the fastest. Figures 7.11 and 7.12 compare the two methods that rely on the best found 16-bit representations. In this case, when the factorization of the exponent is easily known, it is faster to exponentiation by the list of prime factors than it is to represent the exponent using 16-bit blocks. Finally, Figures 7.13 and 7.14 compare the best performer from each category.

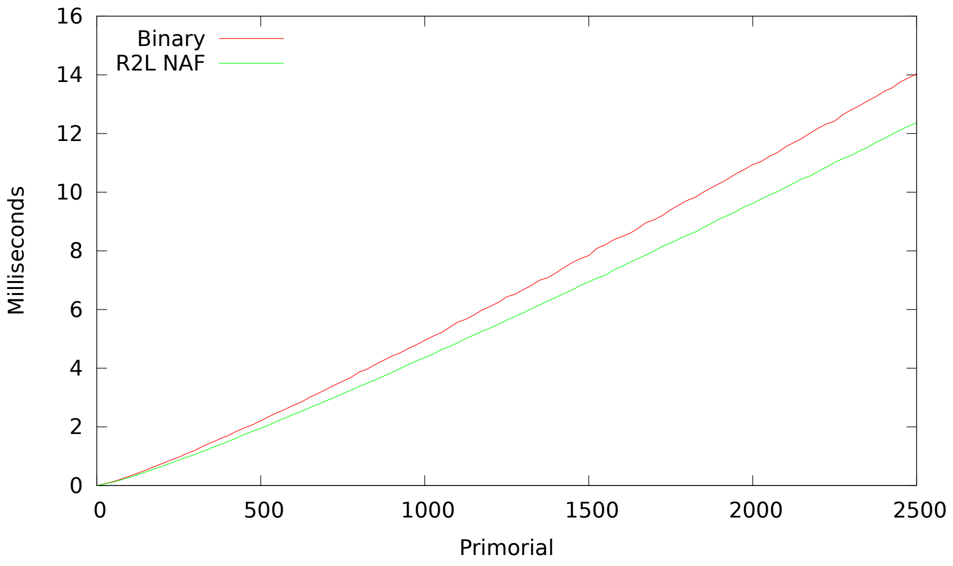


Figure 7.3: Base 2 Exponentiation (59-bit Discriminants).

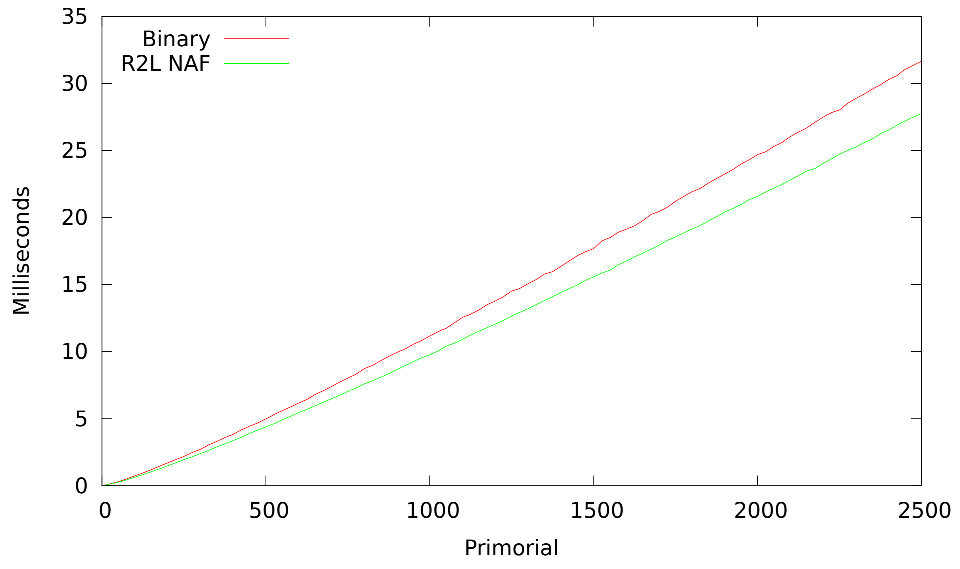


Figure 7.4: Base 2 Exponentiation (118-bit Discriminants).

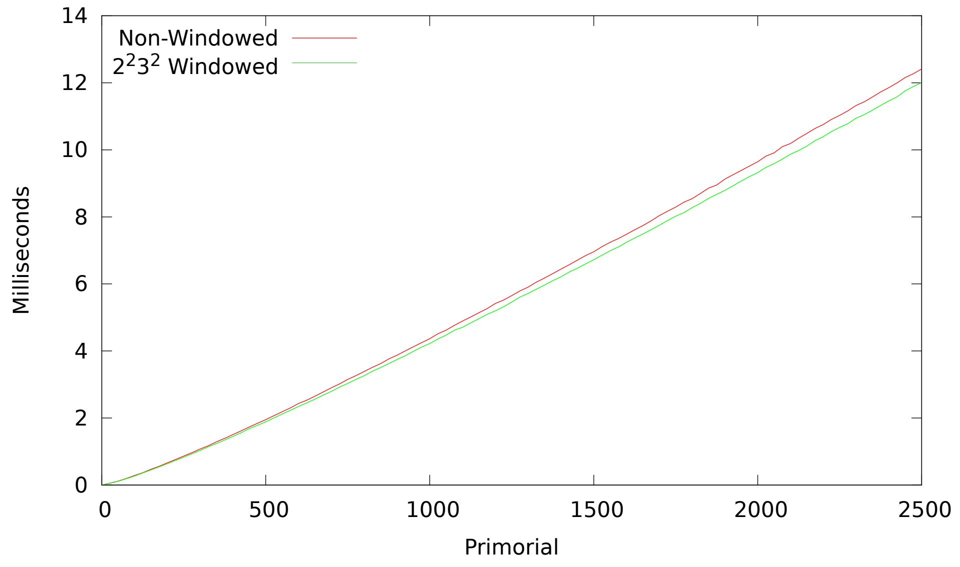


Figure 7.5: Right-to-Left 2,3 Chains (59-bit Discriminants).

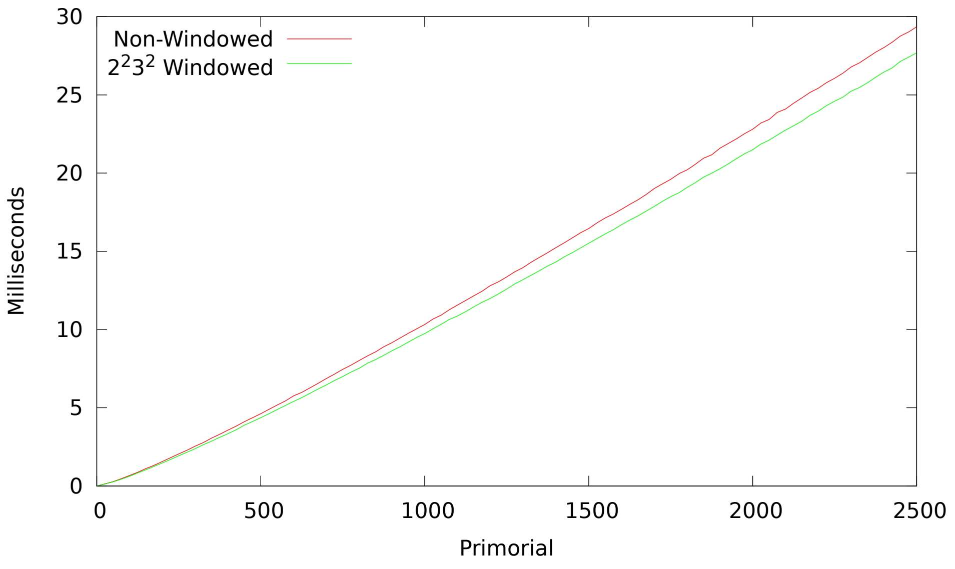
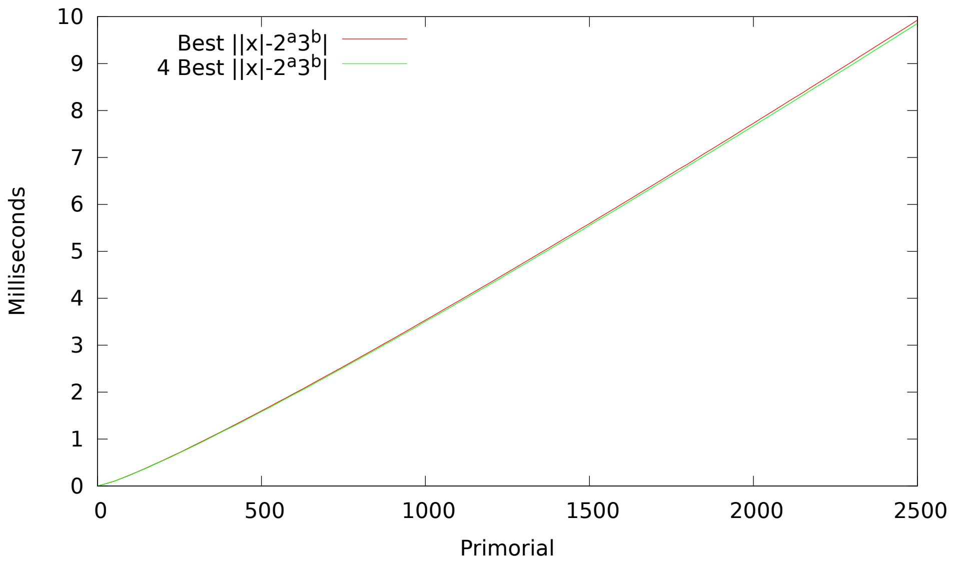


Figure 7.6: Right-to-Left 2,3 Chains (118-bit Discriminants).



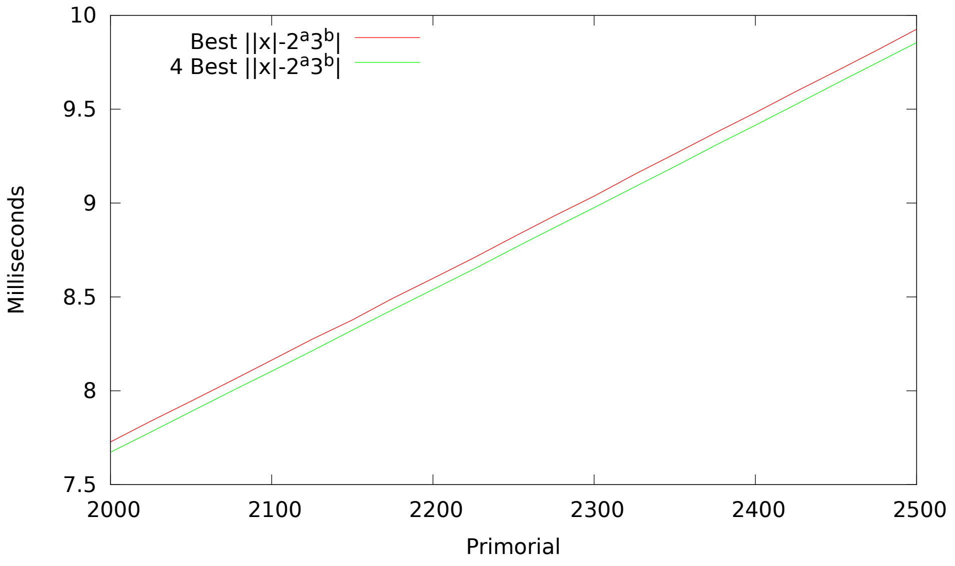
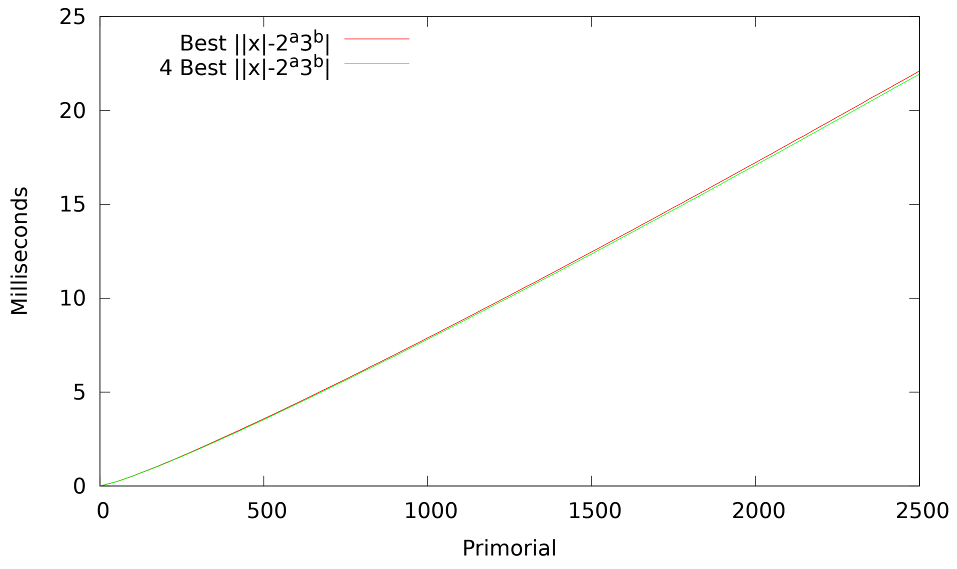


Figure 7.7: Left-to-Right 2,3 Representations (59-bit Discriminants).



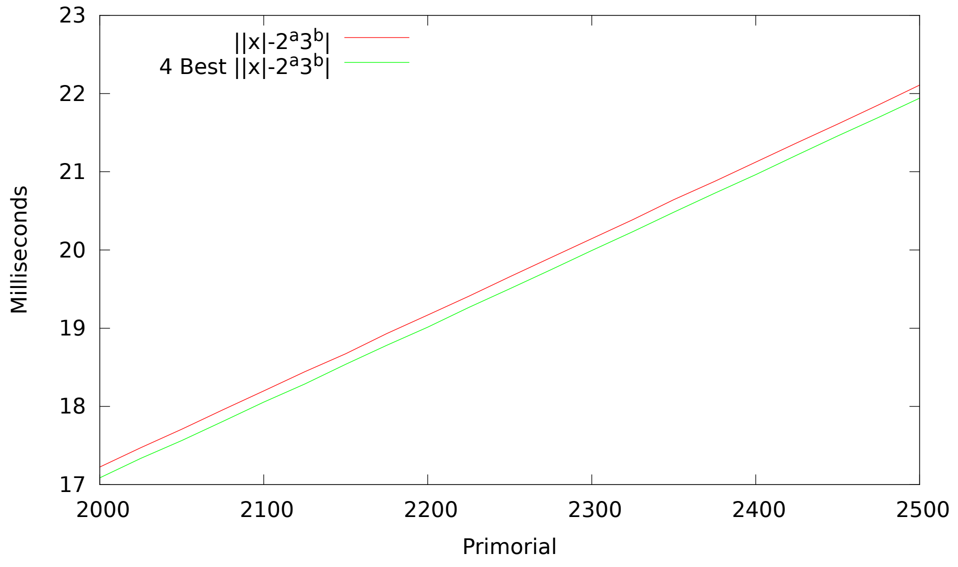
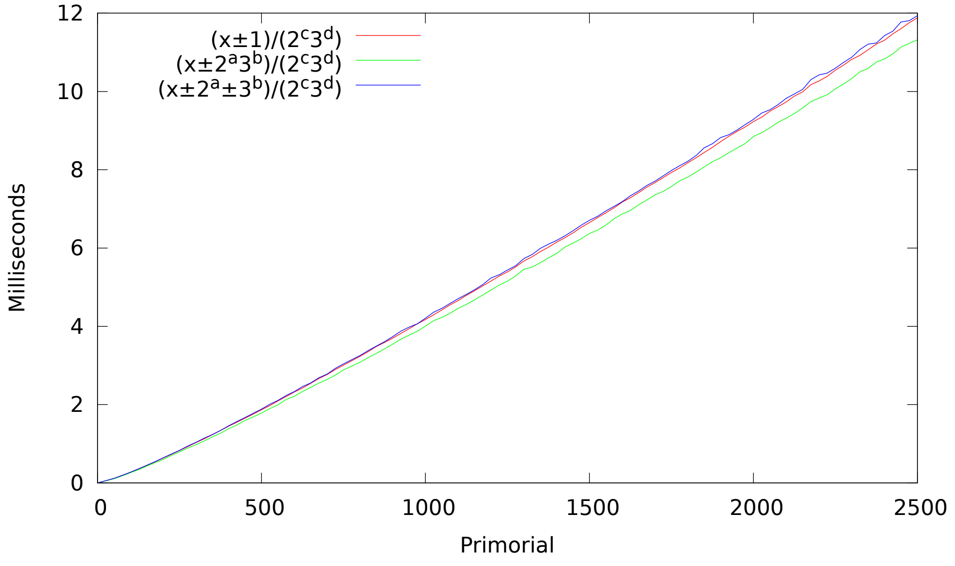


Figure 7.8: Left-to-Right 2,3 Representations (118-bit Discriminants).



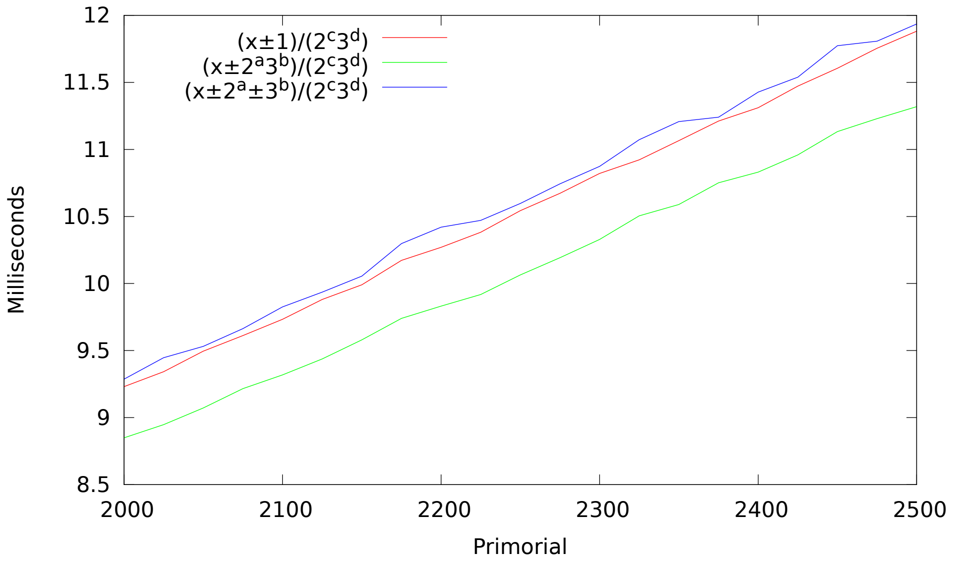
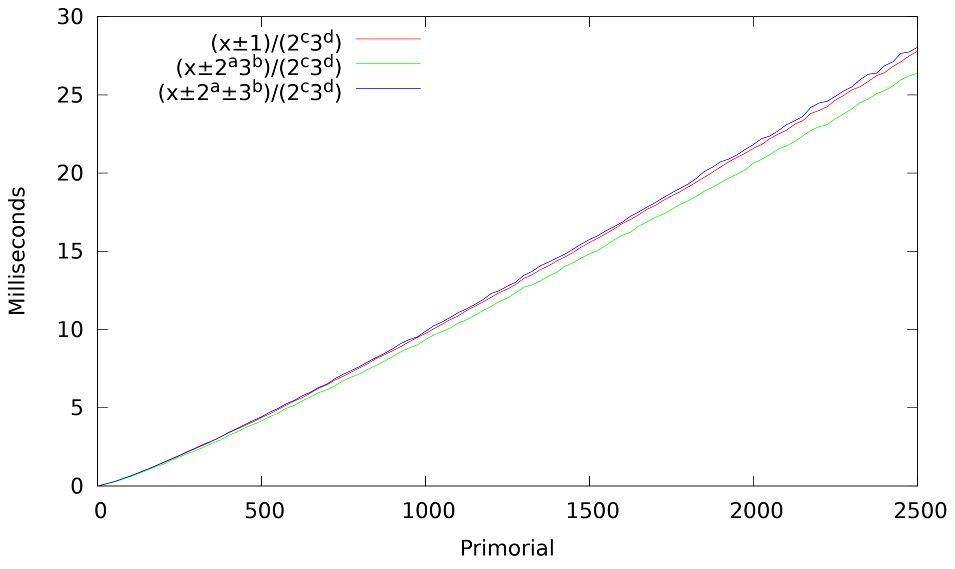


Figure 7.9: 4 Best $(x \pm \cdots)/(2^c 3^d)$ (59-bit Discriminants).



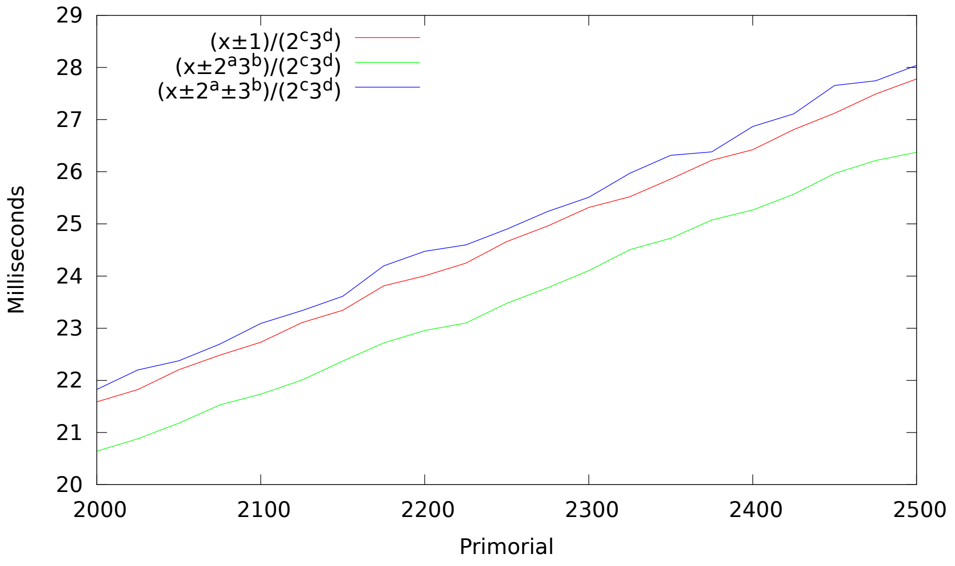


Figure 7.10: 4 Best $(x \pm \cdots)/(2^c 3^d)$ (118-bit Discriminants).

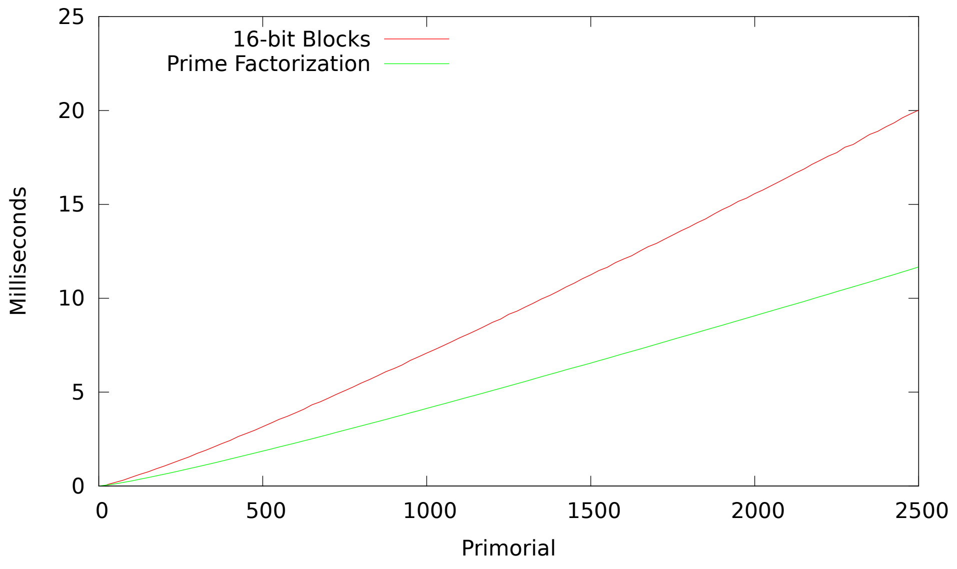


Figure 7.11: Use g^b for 16-bit b (59-bit Discriminants).

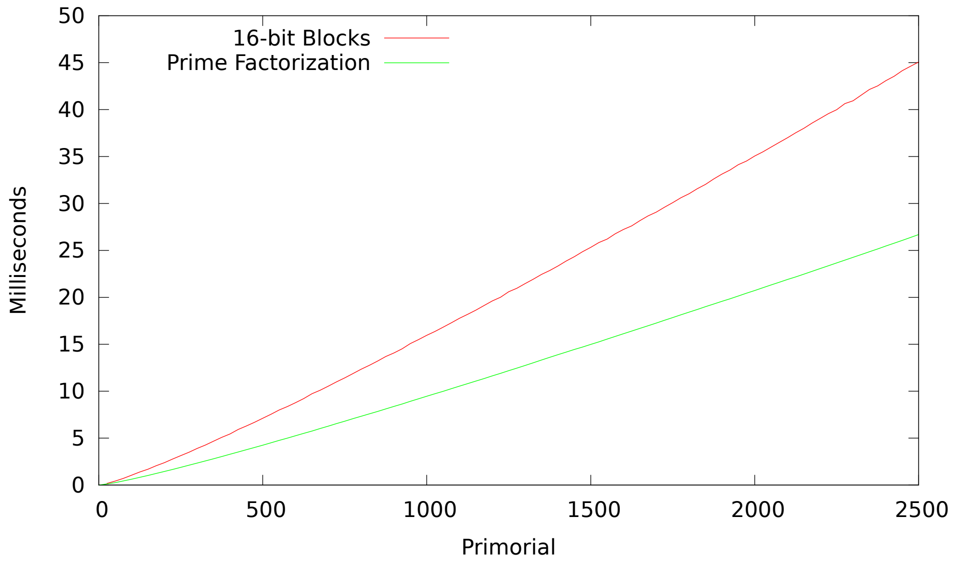


Figure 7.12: Use g^b for 16-bit b (118-bit Discriminants).

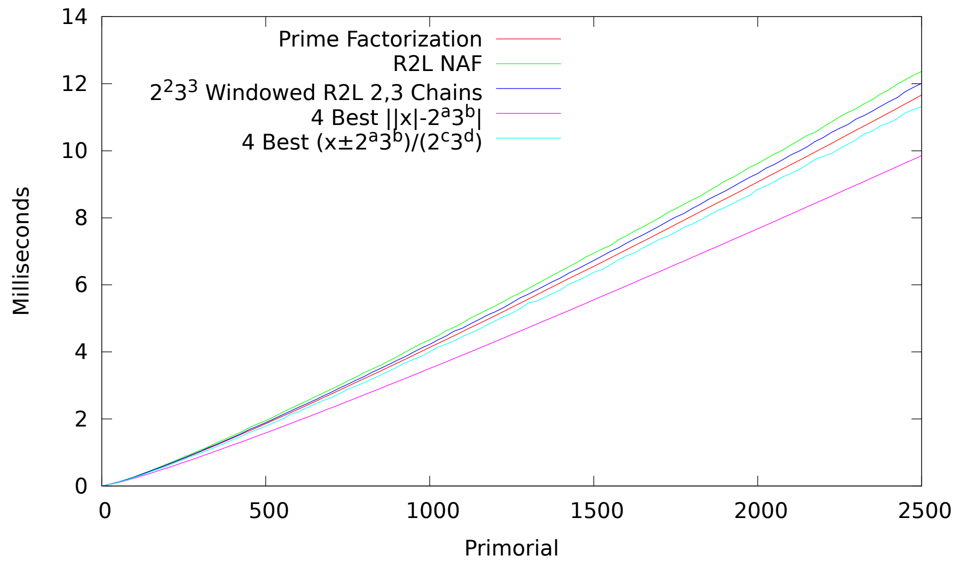


Figure 7.13: The best performers from each category (59-bit Discriminants).

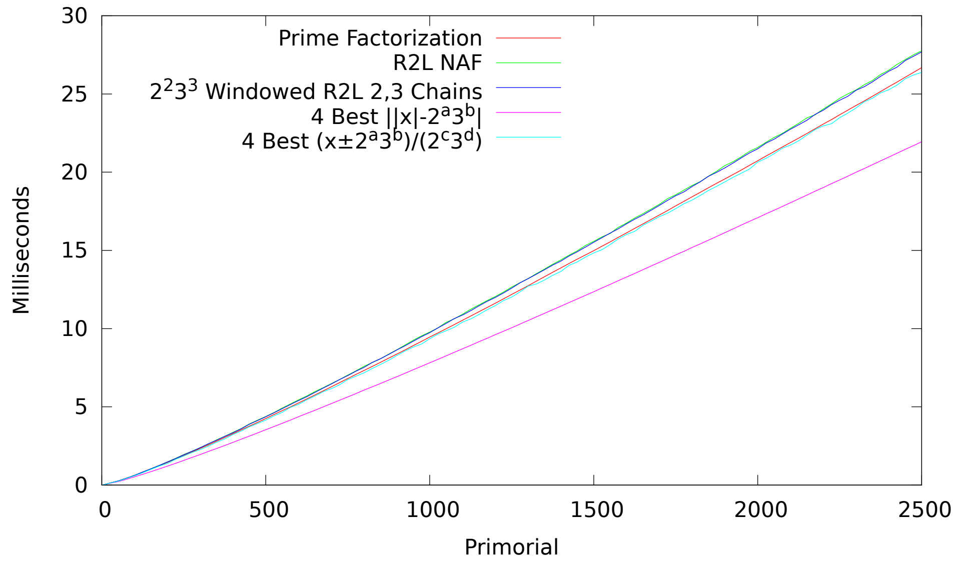


Figure 7.14: The best performers from each category (118-bit Discriminants).

7.11 Summary

This Chapter presented the approach and results used to improve exponentiation in the ideal class group of imaginary quadratic number fields. Several methods for exponentiation including novel extensions to methods for computing 2,3 chains and representations were explored. We found that for 16-bit exponents, the method of iterating on the L best partial representations $x + \sum s_i 2^{a_i} 3^{b_i}$ such that each x generates new terms of the form $(x \pm 2^a 3^b)/(2^c 3^d) \in \mathbb{Z}$ gives the fastest representation on average. For large primorial exponents, generating new terms of the form $\big||x| - 2^a 3^b\big|$ gave the fastest representations on average.

The next Chapter brings together the improvements to ideal arithmetic and exponentiation in our implementation of SuperSPAR – an algorithm with the fastest average time to factor integers n in the range $2^{54} \leq n < 2^{63}$ of the integer factoring algorithms that we tested.

Chapter 8

SuperSPAR Experiments

This Chapter discusses the experiments and results that directed our implementation of the SuperSPAR integer factoring algorithm, introduced in Section 4.3. The algorithm is based on the ideal class group, discussed in Chapter 2, and the experiments and results leading to our implementation of arithmetic in the ideal class group is discussed in Chapters 5 and 6. SuperSPAR is an adaptation of the SPAR factoring algorithm, discussed in Section 4.1. The algorithms differ in how they search for the order of a group element – SuperSPAR uses the bounded primorial steps algorithm discussed in Section 4.2 – but both algorithms first exponentiate a random ideal class to the product of many primes. Chapter 3 discusses several methods for exponentiation in generic groups and Chapter 7 discusses our experiments and results of exponentiation in the ideal class group. Practical improvements to each of these areas lead to practical improvements in our implementation of SuperSPAR.

SuperSPAR works in two stages: an exponentiation stage and a search stage. The search stage of SuperSPAR computes baby steps coprime to a multiple of a primorial. Section 8.1 discusses two techniques to find integers coprime to a primorial in a given range. As discussed in Subsection 4.2.2, for the search stage to work, the order of the element should have no factors in common with the primorial used for the search stage. Section 8.2 discusses the data and experiments used to bound the exponents of the prime factors of the exponent used in the exponentiation stage so that (with high probability) the order of the resulting ideal class will have no factors in common with the primorial used during the search stage. This Section also discusses the number of ideal classes to try in expectation for a given class group. The search stage of the algorithm requires the use of a lookup table. Section 8.3 compares two implementations of such a table. Then, to enable the discovery of bounds useful for the search stage, Section 8.4 discusses a method of generating suitable candidates. With all this in place, Section 8.5 discusses the method used to determine the exponent for the exponentiation stage and the bound for the search stage that work well in practice for integers of specific sizes. Finally, a comparison of our implementation of SuperSPAR to several public implementations of factoring algorithms is provided. We show that for random semiprime integers 50-bits or more and less than 64-bits, SuperSPAR performs the best on average of the implementations tested.

The software used to generate timing information was developed using GNU C compiler version 4.7.2 on Ubuntu 12.10 and a personal notebook with a 2.7GHz Intel Core i7-2620M CPU and 8Gb of RAM. Never more than one of the four cores was used for experiments.

8.1 Coprime Finding

The bounded primorial steps algorithm from Section 4.2 and used by the SuperSPAR factoring algorithm (Section 4.3) computes baby-steps $[\mathfrak{a}]^i$ for $1 \leq i \leq s$ where i is coprime to some primorial P_w and s is a multiple of P_w. By considering only values coprime to P_w the running time complexity of the bounded primorial steps algorithm achieves an upper bound of $O(\sqrt{M/\log\log M})$ group operations in the worst case. If an implementation has to test whether each i from 1 to P_w is coprime to P_w, the algorithm cannot achieve this. As such, the algorithm assumes a set of values coprime to P_w is globally available. Of course, one can generate such a set by testing whether $\gcd(i, P_w) = 1$ for i from 1 to P_w, but there are more efficient methods. This section discusses two such methods, namely sieving and wheeling. Additional information on each technique can be found in [16, pp.117–127] and [47, p.494].

8.1.1 Coprime Sieve

Sieving the values coprime to some primorial P_w is straightforward since the factorization $P_w = 2 \times 3 \times \cdots \times p_w$ is known. Let $[1, b]$ denote the range to be sieved. First, create a table mapping the values 1 through b to *true*. Then for each prime factor p_j of P_w, and for every multiple mp_j such that $1 \leq mp_j \leq b$, set the table entry at index mp_j to *false*. At this point, each index with a *true* value is coprime to P_w. To see this, note that an index x is *false* when there was some multiple m of a prime p_j dividing P_w such that $mp_j = x$. As such, the value of x is false if and only if x and P_w share a common factor, namely p_j.

8.1.2 Coprime Wheel

When the value b from the previous section is equal to the primorial P_w, a coprime wheel may be faster in practice. First, suppose that for some primorial P_w, the set of all integers $1 \leq x < P_w$ coprime to P_w is already known. More formally, let

$$\mathcal{C}_w = \{x \ : \ \gcd(x, P_w) = 1, 1 \leq x < P_w\}.$$

As such, there is no $x \in \mathcal{C}_w$ that is divisible by any prime p_j that divides P_w. The values $x + mP_w$ for $x \in \mathcal{C}_w$ and $m \in \mathbb{Z}$ are also coprime to P_w, and so act as a set of representatives of the integers modulo P_w that are coprime to P_w. Let $\mathcal{C}_w + mP_w$ denote the set $\{x + mP_w : x \in \mathcal{C}_w\}$. Computing

$$\bigcup_{0 \leq m < p_{w+1}} \mathcal{C}_w + mP_w$$

generates the set of all positive integers less than P_{w+1} that are coprime to P_w. Removing all multiples of p_{w+1} from this set implies that no element is divisible by a prime $p_j \leq p_{w+1}$. As such, the set

$$\mathcal{C}_{w+1} = \left[\bigcup_{0 \leq m < p_{w+1}} \mathcal{C}_w + mP_w \right] \setminus \{m' p_{w+1} : 1 \leq m' < P_w\}$$

is the set of all values $1 \leq x < P_{w+1}$ that are coprime to P_{w+1}.

The primorial $P_1 = 2$ has the set $\mathcal{C}_1 = \{1\}$ of integers coprime to 2. This acts as a base case, from which the representative set of integers coprime to primorials $P_2, P_3, ..., P_w$ are computed by recursive application of the above steps.

Our implementation of SuperSPAR iterates baby steps for consecutive integers coprime to some primorial P_w. As such, the difference between coprime integers is used instead, and the above technique is adapted to work with lists of deltas between consecutive coprime integers. Each list begins with the difference from the first coprime integer 1 (which is coprime to all integers) to the next integer coprime to some primorial P_w. Let

$$\mathcal{D}_w = d_1, ..., d_{\phi(P_w)}$$

such that $d_i = c_{i+1} - c_i$ for consecutive integers c_i and c_{i+1} coprime to P_w where $c_1 = 1$. The list $\mathcal{D}_1$ consists of the single value 2.

Algorithm 8.1 Compute deltas for P_{w+1} given deltas for P_w.

```
Input: A primorial $P_w$, the delta list $\mathcal{D}_w$, and the next prime $p_{w+1}$.
    Let $P_{w+1} = p_{w+1}P_w$ and $\phi(P_{w+1}) = (p_{w+1} - 1)\phi(P_w)$.
Output: The delta list $\mathcal{D}_{w+1}$.
 1: $i \leftarrow 1, j \leftarrow 1, c \leftarrow 1, d \leftarrow 0$
 2: while $j \le \phi(P_{w+1})$ do
 3:     $c \leftarrow c + d_i$                          {each $c$ is coprime to $P_w$}
 4:     $d \leftarrow d + d_i$
 5:     if $c \not\equiv 0 \pmod{p_{w+1}}$ then
 6:         $d'_j \leftarrow d, d \leftarrow 0, j \leftarrow j + 1$     {output $d$ when $c$ is coprime to $P_{w+1}$}
 7:     end if
 8:     $i \leftarrow i + 1$
 9:     if $i > \phi(P_w)$ then $i \leftarrow 1$ end if
10: end while
11: return $d'_1, ..., d'_{\phi(P_{w+1})}$
```

Algorithm 8.1 computes $\mathcal{D}_{w+1}$ given $\mathcal{D}_w$, P_w, and the next prime p_{w+1}. The algorithm starts with the current candidate integer, c, coprime to P_{w+1} and a delta counter $d = 0$. The algorithm cycles through the delta list $\mathcal{D}_w$ adding each element encountered to c. On each iteration, if c is not a multiple of p_{w+1}, then the delta counter d is appended to the output list $\mathcal{D}_{w+1}$ and then set to 0. Otherwise, the algorithm continues with the next delta from the input list (cycling to the beginning of the list when the end is reached). Once $\phi(P_{w+1})$ deltas have been appended to the output list, the algorithm terminates.

8.1.3 Comparison

The coprime sieve requires b bits of memory, while the coprime wheel requires $O(\phi(P_w))$ integers for the list of deltas. Table 8.1 shows the values of $\phi(P_w)$ for the first 12 primorials. The delta list for the tenth primorial, $\phi(P_{10}) = 1021870080$, requires over a billion integers. As such, the coprime sieve is preferred when the primorial is large, while the coprime wheel may be more efficient for large values of b. This is because the coprime wheel generates deltas directly, whereas each entry in the sieve must be inspected to find integers coprime to the primorial.

w	p_w	$P_w = \prod_{p \le p_w} p$	$\phi(P_w) = \prod_{p \le p_w} (p-1)$
1	2	2	1
2	3	6	2
3	5	30	8
4	7	210	48
5	11	2310	480
6	13	30030	5760
7	17	510510	92160
8	19	9699690	1658880
9	23	223092870	36495360
10	29	6469693230	1021870080
11	31	200560490130	30656102400
12	37	7420738134810	1103619686400

Table 8.1: The first 12 primorials.

SuperSPAR computes baby steps coprime to a multiple of a primorial, and so b is at least $\phi(P_w)$. This means that in practice, the algorithm is restricted to primorials that fit within the available memory. The coprime wheel is used to generate the list of coprime deltas, however, this list is precomputed and compiled directly into the bytecode of our implementation. In practice, the largest primorial used is $P_5 = 2310$ (see Section 8.5 for details).

8.2 Factorization of the Order of Ideal Classes

Subsection 4.3.1 discusses some practical considerations of our implementation of SuperSPAR. As such, this Section provides numerical evidence in support of some of those considerations. From a set of roughly 6 million ideals, the factorization of the order of each ideal was computed. Based on this factorization, a strategy of reusing a known multiple of the order of an ideal class for several ideal classes in the same group is adopted (Subsection 8.2.2). This data helped guide bounds on the exponents e_i in the product $E = \prod {p_i}^{e_i}$ used in the exponentiation stage (Subsection 8.2.1). In addition, there is evidence, at least for the integer range studied, that ideal classes from groups associated with certain multipliers are more likely to lead to a splitting of the input integer (Subsection 8.2.3).

Since this Chapter is concerned with the performance of SuperSPAR in practice, the following parameters were selected to highlight the range in which SuperSPAR is competitive with other factoring algorithms, but also in order to minimize the size of operands. Pari/GP was used to generate as large a data set as possible, but that still fit within the available memory (8Gb) and could be processed reasonably quickly. For bit sizes $n \in \{32, 40, 48, 56, 64, 72, 80\}$, roughly 250,000 unique semiprime integers $N = p \cdot q$ were generated such that p and q are prime and half the size of N, while N is n bits in size. Then for each square free multiplier $k \in \{1, 2, 3, 5, 6, 7, 10\}$, discriminants $\Delta = -kN$ or $\Delta = -4kN$ such that $\Delta \equiv 0, 1 \pmod 4$ were generated. For each corresponding ideal class group Cl_Δ, ideal class representatives $[\mathfrak{p}] \in Cl_\Delta$ with $\mathfrak{p} = [p, (b + \sqrt{\Delta})/2]$ and p prime were generated for the 5 smallest suitable values of p. Finally, for each ideal class $[\mathfrak{p}]$, the order of $[\mathfrak{p}]$, its corresponding prime factorization, and whether it lead to to a successful splitting of the integer N were recorded. This data set is used throughout the computations in the following Subsections and is denoted $\mathcal{D}$.

8.2.1 Prime Power Bound

SPAR (Section 4.1) exponentiates an ideal class $[\mathfrak{a}]$ to an exponent E where $E = \prod_{i=2}^{t} {p_i}^{e_i}$, p_i are prime, and $e_i = \max\{v : {p_i}^v \leq {p_t}^2\}$ for some appropriately chosen prime p_t [41, p.290]. In practice however, Schnorr and Lenstra recommend using smaller exponents e_i such that $e_i = \max\{v : {p_i}^v \leq p_t\}$ [41, p.293]. Here we consider bounds for the exponents e_i for use with our implementation of SuperSPAR, assuming the range in which it is a competitive integer factoring tool.

The exponentiation stage of SuperSPAR computes $[\mathfrak{b}] = [\mathfrak{a}]^{2^\ell E}$ with $\ell = \lfloor \log_2 h_\Delta \rfloor$. The search stage then computes baby steps $[\mathfrak{b}]^i$ for i coprime to some primorial P_w. However, if $\mathrm{ord}([\mathfrak{b}])$ and P_w have a common factor p, then p is not coprime to P_w and $[\mathfrak{b}]^p$ will not be added to the lookup table used by the coprime baby steps. If this is the case, the search phase is guaranteed to fail since it cannot find any $[\mathfrak{b}]^{2js}$ such that $2js \equiv 0 \pmod{p}$ in the lookup table. In order to ensure that the order of $[\mathfrak{b}]$ is coprime to E, the exponents in E would have to be chosen such that $e_i = \lfloor \log_{p_i} h_\Delta \rfloor$, however, in practice it is more efficient to choose smaller values of e_i at the risk that additional class groups are tried. For this reason, the exponent E is chosen to remove, with high probability, the factors from the order of $[\mathfrak{a}]$ that are common with the primorial P_w used by the search stage.

For each ideal in our data set $\mathcal{D}$, let the factorization of the order be represented by $\mathrm{ord}([\mathfrak{a}]) = \prod {p_i}^{e_i}$ for p_i prime. For each prime power factor 3^{e_2}, 5^{e_3}, 7^{e_4}, 11^{e_5}, 13^{e_6}, and 17^{e_7}, more than 99% of the ideals studied had either $e_2 \leq 4$, $e_3 \leq 2$, $e_4 \leq 2$, $e_5 \leq 1$, $e_6 \leq 1$, or $e_7 \leq 1$. This is captured by Table 8.2.

This is not to say that more than 99% of the ideals in the data set were such that $\mathrm{ord}([\mathfrak{a}]^{3^4 5^2 7^2 11^1 13^1 17^1})$ is coprime to $3 \times 5 \times 7 \times 11 \times 13 \times 17$, but only that $\mathrm{ord}([\mathfrak{a}]^{3^4})$ is coprime to 3, and so on. On the other hand, Table 8.3 represents the probability that an ideal class $[\mathfrak{a}]$ associated with an integer N of n bits, with order $\mathrm{ord}([\mathfrak{a}]) = \prod {p_i}^{e_i}$ for primes p_i is such

n	$e_2 = 4$	$e_3 = 2$	$e_4 = 2$	$e_5 = 1$	$e_6 = 1$	$e_7 = 1$
32	0.99598	0.99195	0.99713	0.99177	0.99419	0.99659
40	0.99594	0.99193	0.99709	0.99166	0.99404	0.99660
48	0.99593	0.99193	0.99713	0.99162	0.99406	0.99655
56	0.99593	0.99194	0.99709	0.99170	0.99404	0.99648
64	0.99584	0.99211	0.99713	0.99170	0.99412	0.99652
72	0.99586	0.99201	0.99707	0.99163	0.99415	0.99650
80	0.99580	0.99190	0.99719	0.99169	0.99404	0.99645

Table 8.2: The probability that $\operatorname{ord}([\mathfrak{a}]^{{p_i}^{e_i}})$ is coprime to p_i.

that $e_i \le \lfloor \log_{p_i} B \rfloor$ for primes $3 \le p_i \le 11$ and $e_i = 1$ for all $p_i > 11$[1]. In other words, this table represents the probability that choosing some exponent E with the above constraints implies that the ideal class $[\mathfrak{b}] = [\mathfrak{a}]^E$ will have order $\operatorname{ord}([\mathfrak{b}])$ coprime to the exponent E.

n	$B = 1$	$B = 3^2$	$B = 5^2$	$B = 3^3$	$B = 7^2$	$B = 3^4$	$B = 11^2$	$B = 5^3$
32	0.40826	0.80574	0.90863	0.93187	0.94869	0.95669	0.96418	0.97062
40	0.40693	0.80473	0.90739	0.93061	0.94735	0.95525	0.96256	0.96887
48	0.40649	0.80484	0.90720	0.93071	0.94720	0.95511	0.96246	0.96871
56	0.40598	0.80438	0.90718	0.93067	0.94724	0.95510	0.96238	0.96866
64	0.40638	0.80500	0.90722	0.93057	0.94720	0.95518	0.96243	0.96858
72	0.40624	0.80436	0.90714	0.93066	0.94734	0.95520	0.96255	0.96877
80	0.40664	0.80502	0.90738	0.93051	0.94722	0.95499	0.96228	0.96856

Table 8.3: The probability that the order of an ideal class $[\mathfrak{b}] = [\mathfrak{a}]^E$ is coprime to the product $E = \prod {p_i}^{e_i}$ for primes p_i where $e_i \le \lfloor \log_{p_i} B \rfloor$ for $3 \le p_i \le 11$, $e_i = 1$ for all $p_i > 11$, and $e_1 \le \lfloor \log_2 h_\Delta \rfloor$ for $p_1 = 2$.

While such bounds do work well in practice, the purpose of this Section is to optimize the performance of our implementation of SuperSPAR. To this end, the bound B for the exponentiation phase was iterated and the algorithm was timed in practice. Table 8.4 shows the average time to split semiprime integers[2] choosing the exponent E such that odd primes $p_i \le B$ have $e_i = \lfloor \log_{p_i} B \rfloor$ and $p_i > B$ have $e_i = 1$. The primorial and multiplier in the search phase are chosen to give good performance on average and are fixed for each integer bit size. Our implementation of SuperSPAR uses exponents with prime power bounds that

[1]For the prime 2, the exponent $e_1 \le \lfloor \log_2 h_\Delta \rfloor$ is bound by the class number since this is handle separately when searching for ambiguous ideal class.

[2]The sample set consists of 100,000 semiprime integers of each bit size, such that each integer was the product of two primes of equal size.

correspond to the best times for each bit range.

Power bound B	32 bits	40 bits	48 bits	56 bits	64 bits	72 bits	80 bits
$9 = 3^2$	0.04483	0.09538	0.24576	0.74423	2.13834	5.14941	11.81556
$25 = 5^2$	0.04469	0.09332	0.23505	0.70051	2.00290	4.82805	11.09770
$27 = 3^3$	$\underline{0.04453}$	$\underline{0.08980}$	0.22673	0.67292	1.90503	4.58491	10.51262
$49 = 7^2$	0.04550	0.09202	0.21968	0.65496	1.84011	4.42733	10.08651
$81 = 3^4$	0.04794	0.09219	$\underline{0.21840}$	0.64810	1.80854	4.32226	9.88501
$121 = 11^2$	0.04988	0.09499	0.22151	0.64957	1.79549	4.27838	9.81882
$125 = 5^3$	0.04861	0.09505	0.22084	0.64985	1.79609	4.28010	9.80192
$169 = 13^2$	0.05103	0.09783	0.22195	0.64568	1.76646	4.21067	9.60217
$243 = 3^5$	0.05126	0.09871	0.22307	$\underline{0.64527}$	$\underline{1.75882}$	4.17222	9.50603
$343 = 7^3$	0.05415	0.10083	0.22761	0.64718	1.76139	4.17266	9.47648
$625 = 5^4$	0.05966	0.10620	0.23601	0.65786	1.76363	4.13652	9.31960
$729 = 3^6$	0.06031	0.11030	0.23750	0.65964	1.76242	$\underline{4.12565}$	9.28392
$1331 = 11^3$	0.06028	0.10836	0.24391	0.66904	1.78810	4.13952	$\underline{9.28274}$
$2187 = 3^7$	0.06274	0.11096	0.25596	0.69223	1.82186	4.18447	9.34884

Table 8.4: Average time (in milliseconds) to factor semiprime integers using the exponent $E = \prod_{p_i > 2} {p_i}^{e_i}$ with $e_i = \lfloor \log_{p_i} B \rfloor$ when $p_i \le B$ and $e_i = 1$ otherwise. The lowest time for each integer range is underlined.

8.2.2 Difference between the Order of Two Ideal Classes

Suppose the search stage of SuperSPAR determines h', a multiple of the order of an ideal class $[\mathfrak{b}] = [\mathfrak{a}]^{2^\ell E}$ for $\ell = \lfloor \log_2 h_\Delta \rfloor$. Then for some other ideal class $[\mathfrak{a}']$ in the same group, there exists a set of primes $\mathcal{P}$ such that the order of $[\mathfrak{a}']^{2^\ell E}$ divides $h' \prod_{p \in \mathcal{P}} p$, where the product of the empty set is taken to be 1. Also suppose that an exponent E was chosen for the exponentiation phase such that $\operatorname{ord}([\mathfrak{a}]^E)$ is coprime to E. Since in practice our implementation of SuperSPAR does not step coprime to a primorial larger than $2 \times 3 \times 5 \times 7 \times 11$ (see Section 8.5), this Subsection assumes that the exponent E is chosen such that for each ideal class in our data set $\mathcal{D}$, the order of the ideal class $[\mathfrak{a}]^{2^\ell E}$ is coprime to $2 \times 3 \times 5 \times 7 \times 11$. Assuming the above constraints, for two ideal classes from the same group $[\mathfrak{u}], [\mathfrak{v}] \in Cl_\Delta$, Table 8.5 shows the probability that the smallest set of primes $\mathcal{P} = \{p \ : \ p \text{ is prime}, p > 11\}$ with $\operatorname{ord}([\mathfrak{v}]^{2^\ell E})$ dividing $\operatorname{ord}([\mathfrak{u}]^{2^\ell E}) \times \prod_{p \in \mathcal{P}} p$ is of a given size.

n	$\lvert\mathcal{P}\rvert = 0$	$\lvert\mathcal{P}\rvert = 1$	$\lvert\mathcal{P}\rvert = 2$	$\lvert\mathcal{P}\rvert = 3$
32	0.97804	0.02177	0.00020	0.00000
40	0.97791	0.02183	0.00026	0.00000
48	0.97785	0.02187	0.00028	0.00000
56	0.97776	0.02196	0.00028	0.00000
64	0.97779	0.02193	0.00028	0.00000
72	0.97782	0.02190	0.00027	0.00000
80	0.97781	0.02191	0.00028	0.00000

Table 8.5: If h', a multiple of the order of an ideal class $[\mathfrak{u}]$ is known, this table shows the probability that the order of the ideal class $[\mathfrak{v}]^{h'}$, for some other ideal class $[\mathfrak{v}]$ in the same group, has exactly $|\mathcal{P}|$ prime factors larger than 11.

Of the ideal class groups studied, more than 97.7% of the time, a multiple[3] of the order of an ideal class is also a multiple of the order of some other ideal class in the same group. For SuperSPAR, this means that once a multiple of the order of an ideal class is discovered, if this does not lead to a splitting of N, then with high probability, it is also a multiple of the order of some other ideal class in the same group. Rather than starting over with a different ideal class, let h' be the odd part of the multiple of the order and compute $[\mathfrak{b}]^{h'}$ for some other ideal class $[\mathfrak{b}]$. SuperSPAR then tries to find an ambiguous class by repeated squaring of $[\mathfrak{b}]^{h'}$ and, if successful, attempts to split N. This process may be repeated for several different ideal classes in the same group.

This process may be unlucky, and as Subsection 8.2.4 shows, if the algorithm is unsuccessful for more than an fixed number of ideal classes within the same class group, changing class groups by changing multipliers is beneficial.

8.2.3 Best Multipliers

As in the previous Subsection, assume that an exponent E is chosen for the exponentiation stage such that $\text{ord}([\mathfrak{a}_1]^{2^\ell E})$ is coprime to E. Also, suppose that the search stage is successful in determining h', a multiple of the order of $[\mathfrak{a}_1]^{2^\ell E} \in Cl_\Delta$. Our implementation of SuperSPAR will first attempt to split the integer N associated with the discriminant Δ by

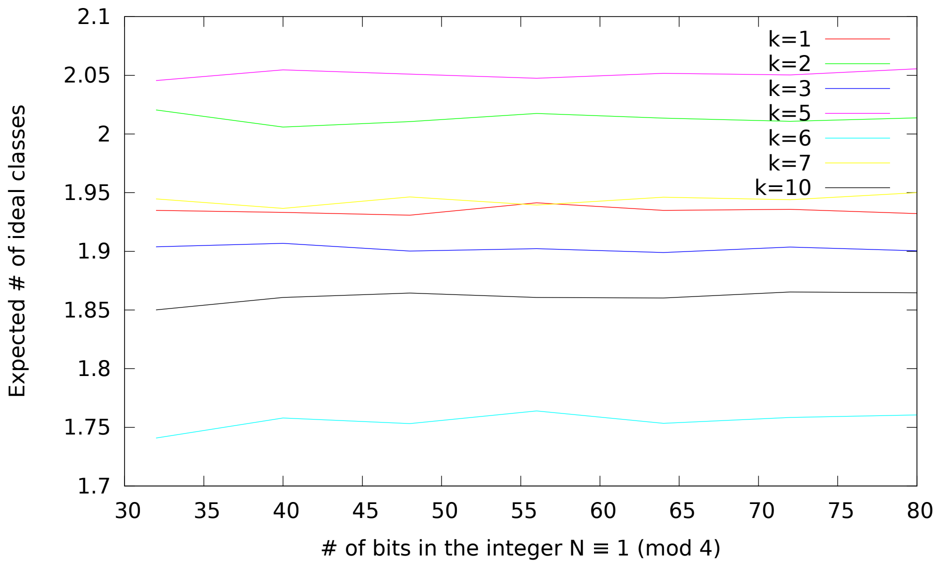
[3]Assuming that the multiple is guaranteed to remove all factors of 2, 3, 5, 7, and 11 from the order of each ideal class in the class group.

searching for an ambiguous class via repeated squaring of the ideal class $[\mathfrak{a}_1]^{Eh'}$. Failing this, the algorithm tries again by repeated squaring of the ideal classes $[\mathfrak{a}_2]^{Eh'}, [\mathfrak{a}_3]^{Eh'}, \ldots$ and so on in sequence. This Subsection uses the data set $\mathcal{D}$ to determine the expected number of ideal classes to try before a successful splitting of the integer N.

The discriminant Δ associated with an integer N and multiplier k is chosen to be either $\Delta = -kN$ when $-kN \equiv 0, 1 \pmod 4$, or $\Delta = -4kN$. As such, the data set $\mathcal{D}$ is separated into subsets for $N \equiv 1 \pmod 4$ or $N \equiv 3 \pmod 4$[4], and again for each multiplier $k \in \{1, 2, 3, 5, 6, 7, 10\}$. Figure 8.1 shows the expected number of ideal classes to try before splitting N, assuming that an appropriate exponent E for the exponentiation stage[5] is chosen and that a multiple of the order h' was found during the search stage.

[4]Notice that $N \equiv 0, 2 \pmod 4$ implies that 2 is a divisor of N and so can be easily split.

[5]Again, since our implementation of SuperSPAR does not step coprime to a primorial larger than $2 \times 3 \times 5 \times 7 \times 11$ (see Section 8.5), we assume that the exponent E for the exponentiation stage removed all factors ≤ 11 from the order of $[\mathfrak{a}_i]^E$.



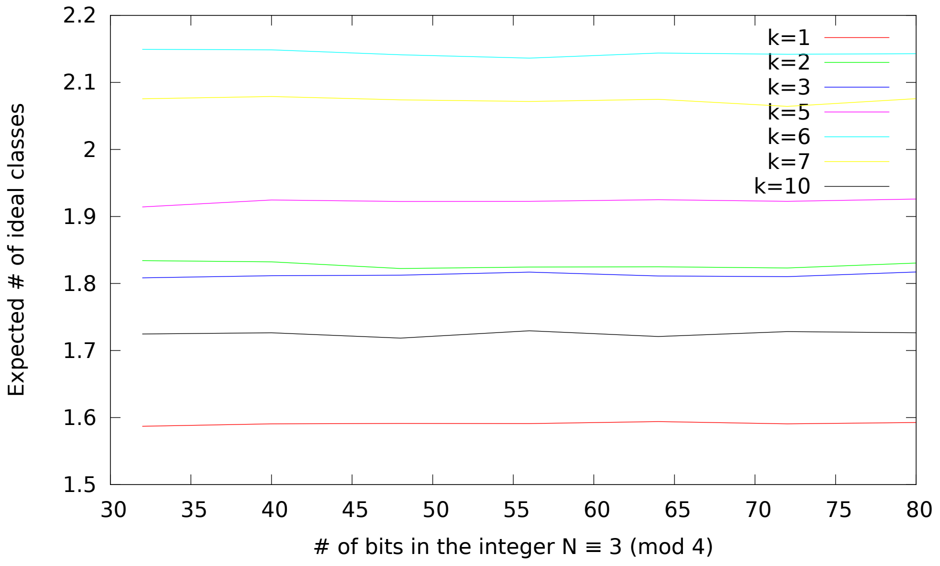


Figure 8.1: Attempts $N \equiv 1 \pmod 4$

Given this separation of the integer N and the multiplier k in our data set $\mathcal{D}$, the class groups associated with discriminants $\Delta = -kN$ or $\Delta = -4kN$, as appropriate, appear to be separate with respect to the probability that an ideal class in the group will lead to a splitting of the integer N. As such, our implementation of SuperSPAR chooses multipliers of N sequentially such that when $N \equiv 1 \pmod 4$, $k = 6, 10, 3, 1, 7, 2, 5$, and when $N \equiv 3 \pmod 4$, $k = 1, 10, 3, 2, 5, 7, 6$. In the event that the algorithm exhausts this list of multipliers

Classes/Group	32 bits	40 bits	48 bits	56 bits	64 bits	72 bits	80 bits
1	0.05570	0.12454	0.31630	0.92448	2.56007	6.55736	14.64756
2	0.04462	0.09425	0.23631	0.68485	1.92037	4.88625	11.07386
3	0.04181	0.08708	0.21465	0.62268	1.74317	4.39471	10.01309
4	0.04104	0.08418	0.20621	0.59624	1.66741	4.19481	9.55292
5	0.04080	0.08306	0.20254	0.58463	1.63373	4.09556	9.31992
6	0.04081	0.08270	0.20113	0.57836	1.61780	4.03869	9.18897
7	0.04098	0.08262	0.20026	0.57618	1.60919	4.01559	9.09742
8	0.04113	0.08266	0.20008	0.57406	1.60498	3.99565	9.05229
9	0.04130	0.08284	0.20005	0.57365	1.60082	3.98321	9.02378
10	0.04146	0.08311	0.20028	0.57390	1.60011	3.97691	9.00030
11	0.04175	0.08327	0.20067	0.57404	1.59738	3.97021	8.98048
12	0.04180	0.08348	0.20092	0.57470	1.59855	3.96747	8.97534
13	0.04200	0.08367	0.20129	0.57520	1.59944	3.96789	8.97226
14	0.04221	0.08391	0.20161	0.57583	1.60174	3.96836	8.97280
15	0.04231	0.08407	0.20208	0.57680	1.60335	3.97339	8.97848
16	0.04251	0.08431	0.20248	0.57780	1.60844	3.97845	8.97971

Table 8.6: The average time (in milliseconds) to split an integer N using no more than a fixed number of ideal classes for each class group. The lowest time for each integer range is underlined.

without successfully splitting N, square free multipliers $k > 10$ are selected in increasing order.

8.2.4 Expected Number of Ideal Classes

Figure 8.1 indicates that for most multipliers, if the search stage of the algorithm is successful in finding a multiple of the order of an ideal class, then in expectation, two ideal classes need to be tried before a successful splitting of the integer N. Although switching multipliers after at most two ideal classes does work in practice, our implementation of SuperSPAR is more efficient if many ideal classes are tried before switching multipliers and class groups. This is possibly due to the cost of the search phase of the algorithm, which is executed with each class group[6]. Table 8.6 shows the average time to split integers[7] given an upper bound

[6]This is in contrast to the exponentiation stage, which is executed for each ideal class tried.

[7]This uses the same set of semiprime integers as in Table 8.4. Again, the exponent for the exponentiation stage, and the primorial and multiplier for the search stage where chosen to give good performance on average.

on the number of ideal classes tried before switching multipliers. Our implementation of SuperSPAR bounds the number of ideal classes tried before switching class groups to the lowest time for each integer range.

8.3 Lookup Tables

The SuperSPAR Algorithm 4.2 (and more generally, the bounded primorial steps algorithm 4.1) requires a lookup table[8]. The baby steps generate a mapping from group elements $[\mathfrak{b}]^i$ to exponents i coprime to some primorial P_w and store this mapping in the lookup table. The giant steps lookup group elements $[\mathfrak{b}]^{2js}$ and $[\mathfrak{b}]^{-2js}$ from the lookup table. As such, the performance of the algorithm directly corresponds to the performance of the lookup table. This Section describes the experimental results for SuperSPAR using two different implementations of lookup tables, as well as the method used to map group elements to exponents in our implementation.

Our implementation of idea class arithmetic represents an ideal class $[\mathfrak{a}] \in Cl_\Delta$ using the triple (a, b, c) where $\mathfrak{a} = [a, (b + \sqrt{\Delta})/2]$ is a reduced representative for the ideal class and $c = (b^2 - \Delta)/4a$ (see Section 6.1). Since inversion of ideal classes is virtually free, SuperSPAR computes giant steps for ideal classes $[\mathfrak{b}]^{2js}$ and $[\mathfrak{b}]^{-2js}$, but rather than perform two table lookups, we take advantage of the way in which the inverse of an ideal class is computed. Recall form Subsection 2.5.3 that the inverse of an ideal class for a representative $[a, (b + \sqrt{\Delta})/2]$ is given by the representative $[a, (-b + \sqrt{\Delta})]$. Since $|b| = \pm\sqrt{\Delta + 4ac}$, by using the pair (a, c) for the key, our implementation is able to look up both $[\mathfrak{b}]^{2sj}$ and $[\mathfrak{b}]^{-2js}$ using a single table lookup. However, once a giant step finds a corresponding $[\mathfrak{b}]^i$ in the table, both the exponents $2js - i$ and $2js + i$ must be tested to determine which one is a multiple of the order of $[\mathfrak{b}]$. Figure 8.2 shows the advantage of performing a single lookup for each giant step over two lookups per giant step[9], even when this requires extra exponentiations

[8]The lookup table maps group elements $[\mathfrak{b}]^i$ to exponents i.

[9]The method proposed here is to use the pair (a, b) for the hash key. This distinguishes between $[\mathfrak{b}]^{2js}$

once a candidate for a multiple of the order is found.

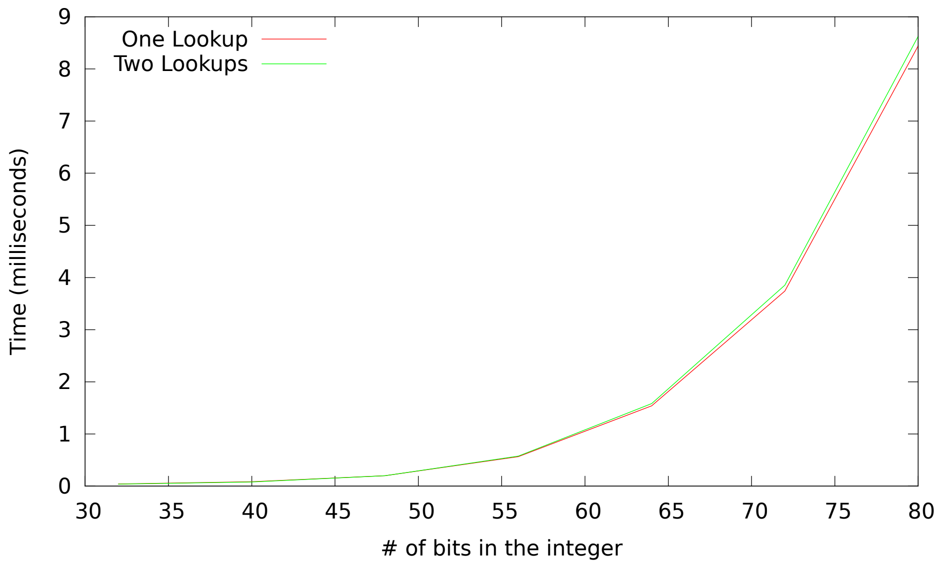


Figure 8.2: Average time to split an integer either by using a single lookup for each giant step, with exponentiation to verify a multiple of the order, or two lookups for each giant step, but without the need to verify a multiple of the order.

In our implementation, the lookup table is implemented as a hash table with 32-bit keys and 32-bit values (both as unsigned integers). Our implementation maps the pair (a, c) associated with an ideal class to a 32-bit hash key by computing

$$\text{hash}_{32}(a, c) = (2654435761 \times (2654435761a + c)) \bmod 2^{32}.$$

The multiplier 2654435761 was chosen because it is the largest prime less than $2^{32} \times (\sqrt{5} - 1)/2$, and $(\sqrt{5} - 1)/2$ has been shown by Knuth [32, Section 6.4] to have good scattering properties[10]. Since the number of baby steps is a function of the size of the integer to be factored (see Section 8.5), the maximum number of entries in the hash table is known at initialization. We found that a table of 2^k slots for the smallest k such that $2^k \geq 3m\phi(P_2)$,

and $[\mathfrak{b}]^{-2js}$. As such, both must be looked up during the giant steps. Then when some $[\mathfrak{b}]^i = [\mathfrak{b}]^{2js}$ or $[\mathfrak{b}]^i = [\mathfrak{b}]^{-2js}$ is found, a multiple of the order is known.

[10]Other multipliers were also tried but had little impact on performance.

where $m\phi(P_w)$ is the number of baby steps, worked well in practice[11]. Using a power of 2 for the number of slots has the added benefit that once a hash key is computed, the corresponding slot is found by using a binary $\texttt{and}_2$ operation. However, regardless of the hash function used, multiple elements may hash to the same slot. Two methods of collision resolution are considered here[12].

8.3.1 Chaining with List Heads

The first method is chaining with list heads (see [15, Subsection 11.2]). The idea is for the hash table to consist of 2^k slots, such that each slot operates as a linked list, but that the head of the linked lists are separate from the tails. Two areas of memory are used: one for the heads, and the other for the tails (also known as the overflow). In the head, each slot consists of the 32-bit value for a specified key, as well as the 32-bit hash key itself (since multiple keys may resolve to the same slot). A special pair of constants are used to indicate that a slot is unoccupied, e.g. (0xAAAAAAAA, 0x55555555). The overflow area consists of an array of no less than 2^k entries, each entry consisting of the 32-bit value for a specified hash key, the 32-bit hash key itself, and an index into the overflow area of the next node in the list, if any. A special constant, e.g. 0xFFFFFFFF, is used to indicate the end of list. The first 2^k entries in the overflow area are reserved and correspond to the second node in the linked list of each slot. To perform a lookup, the hash key resolves to a slot (using $\text{hash}_{32}(a, c) \bmod 2^k$) and the list is traversed until either the specified hash key or the end of the list is found. To insert or update, again, the list is traversed until either the specified hash key is found, at which point an update is performed, or the end of list is found. If the end of list is found, the next available entry in the overflow area is set appropriately and appended to the end of the list.

[11]Different multiples of the number of baby steps were tried, as well as setting the number of slots to a prime near some multiple of the number of baby steps. There was little difference in performance, with the exception of a table having too few slots (resulting in an insertion failing), or a table having an excessive number of slots (and table initialization dominated).

[12]Each method was selected for cache coherency properties (see [15, Subsection 11.2] and [33]).

8.3.2 Open Addressing

The second method of collision resolution considered is open addressing, and in particular, we implement the same probing function as in CPython [33]. In this method, each slot consists of a 32-bit hash key, as well as the 32-bit value associated with that hash key. Any hash key can occupy any slot, and a special pair of constants are used to indicate that a slot is unoccupied, e.g. (0xAAAAAAAA, 0x55555555). When an element is hashed, the table is probed at slot indices $s_0, s_1, ...$ generated by a probing function until a slot is found where either the hash key occupying the slot is the same as the hash key for the element in question, or the slot is unoccupied. Our implementation defines probe indices using

$$\begin{aligned} s_0 &= \text{hash}_{32}(a, b) \bmod 2^k \\ s_i &= \left(5s_{i-1} + 1 + \left\lfloor \text{hash}_{32}(a, b)/2^{5i} \right\rfloor\right) \bmod 2^k. \end{aligned}$$

8.3.3 Chaining vs. Open Addressing

Figure 8.3 shows the average time to split semiprime integers of the specified size using the collision resolution methods described above. In this context and for each integer range tested, open addressing for collision resolution performs better.

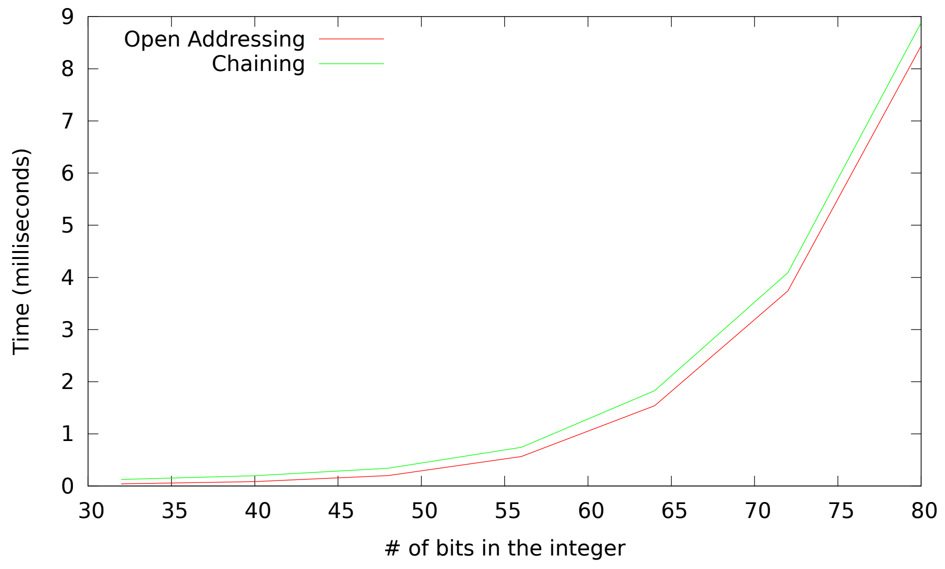


Figure 8.3: The average time to split an integer using either open addressing or chaining with list heads for collision resolution in a hash table.

8.4 Search Bounds

Theoretically, SuperSPAR takes the number of baby steps and giant steps proportional to the largest prime, p_t, used in the exponent of the exponentiation stage, such that $p_t \le N^{1/2r}$, p_t is as large as possible, and $r = \sqrt{\ln N / \ln \ln N}$ (see Section 4.3). The idea is for the search stage and the exponentiation stage to use at most $O(p_t)$ group operations. However, by choosing the number of baby steps and giant steps independently from the exponent used in the exponentiation stage, SuperSPAR performs better in practice. The algorithm takes baby steps coprime to a multiple of some primorial. One could evaluate the performance of all multiples of primorials up to a certain bound, but this is more work than is necessary. This section discusses the method used by our implementation to generate bounds useful for searching. These bounds are later evaluated empirically in Section 8.5.

The success of the search stage depends on the largest exponent $2js$ generated by the giant steps – we will refer to this as the *search range*. The idea here is to generate a set $\mathcal{S}$ of primorial and multiplier pairs used as candidates for the baby step bound s. For each pair, let δ be a function from some multiple m of the primorial P_w to the total number of baby steps and giant steps taken during the search stage of the algorithm,

$$\delta(m, w) = 2m\phi(P_w). \tag{8.1}$$

Notice we take $m\phi(P_w)$ baby steps plus $m\phi(P_w)$ giant steps. Each giant step is of size $2mP_w$, so let θ be a function that computes the exponent of the final giant step, i.e. the search range,

$$\theta(m, w) = 2m^2\phi(P_w)P_w. \tag{8.2}$$

Theorem 8.4.1. For the pair (m_i, w_i), there does not exist a pair (m_j, w_j) with $m_i \neq m_j$ or $w_i \neq w_j$ such that both $\delta(m_i, w_i) = \delta(m_j, w_j)$ and $\theta(m_i, w_i) = \theta(m_j, w_j)$.

Proof. By contradiction, suppose there exists (m_i, w_i) and (m_j, w_j) with $m_i \neq m_j$ or $w_i \neq w_j$ such that $\delta(m_i, w_i) = \delta(m_j, w_j)$ and $\theta(m_i, w_i) = \theta(m_j, w_j)$. Let $w_i < w_j$. Then by Equation 8.1

$$\begin{aligned} &2m_i\phi(P_{w_i}) = 2m_j\phi(P_{w_j}) \\ \Rightarrow &\frac{m_i}{m_j} = \frac{\phi(P_{w_j})}{\phi(P_{w_i})} \end{aligned}$$

and by Equation 8.2

$$\begin{aligned} &2{m_i}^2\phi(P_{w_i})P_{w_i} = 2{m_j}^2\phi(P_{w_j})P_{w_j} \\ \Rightarrow &2m_j\phi(P_{w_j})m_iP_{w_i} = 2{m_j}^2\phi(P_{w_j})P_{w_j} && \{\text{Substituting from above.}\} \\ \Rightarrow &m_iP_{w_i} = m_jP_{w_j} \\ \Rightarrow &\frac{m_i}{m_j} = \frac{P_{w_j}}{P_{w_i}}. \end{aligned}$$

Therefore

$$\frac{\phi(P_{w_j})}{\phi(P_{w_i})} = \frac{P_{w_j}}{P_{w_i}}.$$

However, this is only possible when $w_i = w_j$ and then for $\delta(m_i, w_i) = \delta(m_j, w_j)$ and $\theta(m_i, w_i) = \theta(m_j, w_j)$ to be true, $m_i = m_j$ must also be true. □

With this out of the way, the set $\mathcal{S}$ consists of pairs (m, w) such that for all (m', w') either

$$\theta(m', w') < \theta(m, w) \text{ or } \delta(m', w') > \delta(m, w).$$

In other words, the set $\mathcal{S}$ consists of the pairs (m, w) such that for all other pairs (m', w'), either the search range $\theta(m', w')$ is not as large, or the total number of steps $\delta(m', w')$ is greater. The set $\mathcal{S}$ is defined as

$$\mathcal{S} = \{(m, w) : \text{for all } (m', w'),\ \text{either } \theta(m', w') < \theta(m, w) \text{ or } \delta(m', w') > \delta(m, w)\} \tag{8.3}$$

and is infinite. When a bound B on the total number of steps $\delta(m, w)$ is given, a subset $\mathcal{S}_B \subset \mathcal{S}$ is defined as

$$\mathcal{S}_B = \{(m, w) : (m, w) \in \mathcal{S} \text{ and } \delta(m, w) \le B\} \tag{8.4}$$

and Algorithm 8.2 can be used to generate such a set.

Algorithm 8.2 Compute baby step bound candidates.

```
Input: A bound $B$ on the total number of steps $\delta(m, w)$.
Output: The set of candidate pairs $\mathcal{S}$ (Equation 8.3).
 1: generate the set $\mathcal{T} = \{(m, w) : \delta(m, w) \le B\}$
 2: define an ordering on the set $\mathcal{T}$ using
      $(m_i, w_i) < (m_j, w_j) \Leftrightarrow \begin{cases} \delta(m_i, w_i) < \delta(m_j, w_j) \\ \delta(m_i, w_i) = \delta(m_j, w_j) \text{ and } \theta(m_i, w_i) > \theta(m_j, w_j). \end{cases}$
 3: let $(m_1, w_1), (m_2, w_2), ..., (m_n, w_n)$ be the list of elements generated by sorting the set $\mathcal{T}$
    in ascending order
 4: $\mathcal{S}_B \leftarrow \{\}$
 5: $(m, w) \leftarrow (m_1, w_1)$
 6: for $i = 2$ to $n$ do
 7:    if $\theta(m_i, w_i) > \theta(m, w)$ then
 8:       $\mathcal{S}_B \leftarrow \mathcal{S}_B \cup \{(m, w)\}$
 9:       $(m, w) \leftarrow (m_i, w_i)$
10:    end if
11: end for
12: $\mathcal{S}_B \leftarrow \mathcal{S}_B \cup \{(m, w)\}$
13: return $\mathcal{S}_B$
```

First the algorithm generates all pairs (m, w) such that $\delta(m, w) \leq B$. There is a finite number of these pairs, since there are a finite number of primorials no larger than B, and for a given w there are $\lfloor B/2\phi(P_w) \rfloor$ possible values of m. The algorithm then sorts these pairs in ascending order by the total number of steps $\delta(m, w)$, breaking ties by sorting in descending order of the search range $\theta(m, w)$. The first pair in the list is chosen as a candidate (m, w) for the set $\mathcal{S}_B$. This pair is always in the solution set since by Equation 8.3 and the ordering imposed on the list, all other pairs either take more steps, or an equal number of steps, but have a smaller search range. The algorithm then iterates over the remaining pairs, and the search range of each pair is compared with that of the candidate pair. If the search range is greater, then the candidate pair is output to the set $\mathcal{S}_B$ and the current pair becomes the next candidate pair. The correctness of this follows from the fact that pairs in the list are monotonically increasing by the total number of steps, and successive candidate pairs are strictly increasing in their search range. As such, when the candidate pair (m, w) is compared with the pair (m_i, w_i) from the list, if the search range of the list pair is less than that of the candidate pair, the the list pair uses at least as many steps, but does not search as far, and therefore is not a member of the set $\mathcal{S}_B$. Otherwise, when the list pair has a larger search range, this implies that it uses more steps (since ties are broken by sorting in descending order of search range), and the candidate pair is guaranteed to be a member of the set $\mathcal{S}_B$. This holds since all the pairs remaining in the list use more steps, and all the previous pairs from the list either had a smaller search range, or were rejected because they required more steps.

As an example, the set $\mathcal{S}_{512}$ restricted to pairs using no more than 512 steps, and ordered according to Algorithm 8.2, is

$$\begin{aligned}\mathcal{S}_{512} = \{&(1,1),(1,2),(3,1),(2,2),(5,1),(3,2),(1,3),(5,2),(6,2),(7,2),(2,3),(9,2),\\ &(10,2),(11,2),(3,3),(14,2),(15,2),(4,3),(18,2),(19,2),(5,3),(23,2),(1,4),\\ &(7,3),(8,3),(9,3),(10,3),(11,3),(2,4),(13,3),(14,3),(15,3),(16,3),(17,3),\\ &(3,4),(20,3),(21,3),(22,3),(23,3),(4,4),(26,3),(27,3),(28,3),(29,3),(5,4)\}.\end{aligned}$$

The number of steps for each corresponding pair is

$$\begin{aligned}&2,4,6,8,10,12,16,20,24,28,32,36,40,44,48,56,60,64,72,76,80,92,96,112,128,144,\\ &160,176,192,208,224,240,256,272,288,320,336,352,368,384,416,432,448,464,480,\end{aligned}$$

and the search range, i.e. the value of the largest exponent generated by the giant steps, for each corresponding pair is

$$\begin{aligned}&4,24,36,96,100,216,480,600,864,1176,1920,1944,2400,2904,4320,4704,5400,7680,\\ &7776,8664,12000,12696,20160,23520,30720,38880,48000,58080,80640,81120,94080,\\ &108000,122880,138720,181440,192000,211680,232320,253920,322560,324480,349920,\\ &376320,403680,504000.\end{aligned}$$

This technique of generating candidate bounds for the search phase of SuperSPAR is used in the next section where we search for an exponent to use in the exponentiation stage and a corresponding bound for the search stage that perform well in practice for integers of various sizes.

8.5 Empirical Search for Exponent and Step Count

In order to split integers of a fixed size, two parameters remain to be determined for our implementation of SuperSPAR. The first is the largest prime used in the exponent $E = \prod {p_i}^{e_i}$ for the exponentiation stage, and the second is a multiple of a primorial, mP_w, for use with the search stage. This Section begins by graphically displaying the timing trends to split random semiprime integers of three different bit sizes when the largest prime in the exponent E or the bound on the search phase is iterated. Based on these trends, an algorithm is proposed to find values that work well in practice.

In selecting the exponent E for the exponentiation stage, our implementation uses the results of Chapter 7. Section 7.6 introduces the L best approximations technique for generating 2,3 representations of an integer, for which Section 7.10 shows that this method performs best in practice when exponentiating an ideal class to the product of many prime numbers. This is the method used in our implementation of SuperSPAR. In practice, for a given exponent, the bound L was chosen to be $L = 2^k$ for some value k. The bound was repeatedly doubled and an L best approximation was computed for a given exponent until the cost of exponentiating an ideal class to that particular exponent did not change between iterations. For the exponents tested in this section, the bound was $L \leq 2048$. Representations for the exponents used here were precomputed and available in memory to the running application.

When selecting a multiple of a primorial for the search stage, candidates were selected from the list generated by Algorithm 8.2 in Section 8.4. For the purposes here, the candidate list was bound such that no candidate used more than 16384 total steps for the search stage.

To indicate the effect of iterating the largest prime in the exponent E and the index of the search bound, three sets of 10,000 random semiprime integers $N = p \cdot q$ were generated for p and q prime and half the size of N. The three sets consist of integers of 48, 56, and 64 bits. The largest prime in the exponent was iterated from 13 to 947, and the search bound index was iterated from the first index up to the 120$^{\text{th}}$ index. Figures 8.4, 8.5, and 8.6 show the average time to split integers as the largest prime in the exponent is iterated for 48, 56, and 64-bit integers. Figures 8.7, 8.8, and 8.9 show the average time when the search bound index is iterated for the same sets of integers. Finally, Figure 8.10 shows the best average time of all search bounds tested when the largest prime in the exponent is iterated, and Figure 8.11 shows the best average time of all exponents tested when the search bound index is iterated.

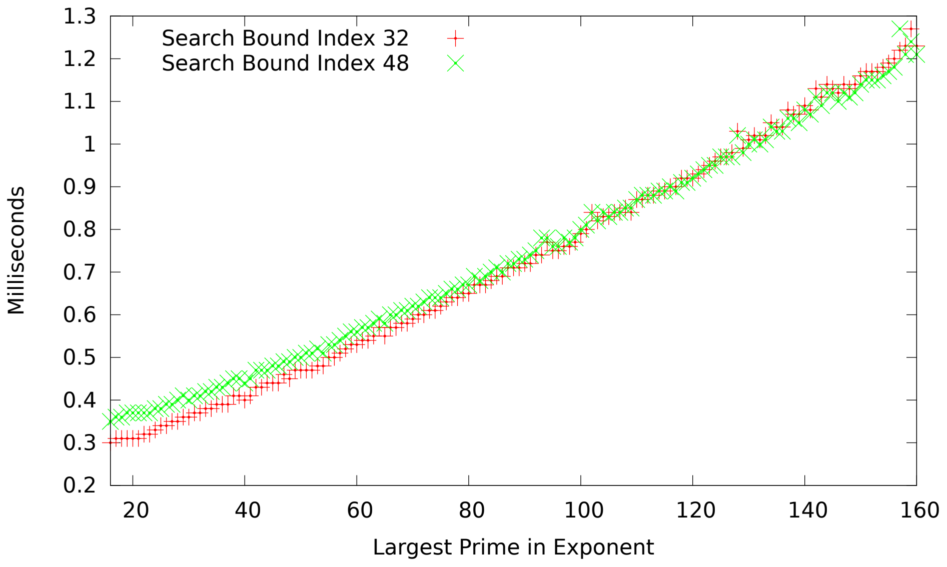


Figure 8.4: The average time to split 48-bit semiprime integers when the largest prime in the exponent $E = \prod {p_i}^{e_i}$ is iterated for a fixed search bound.

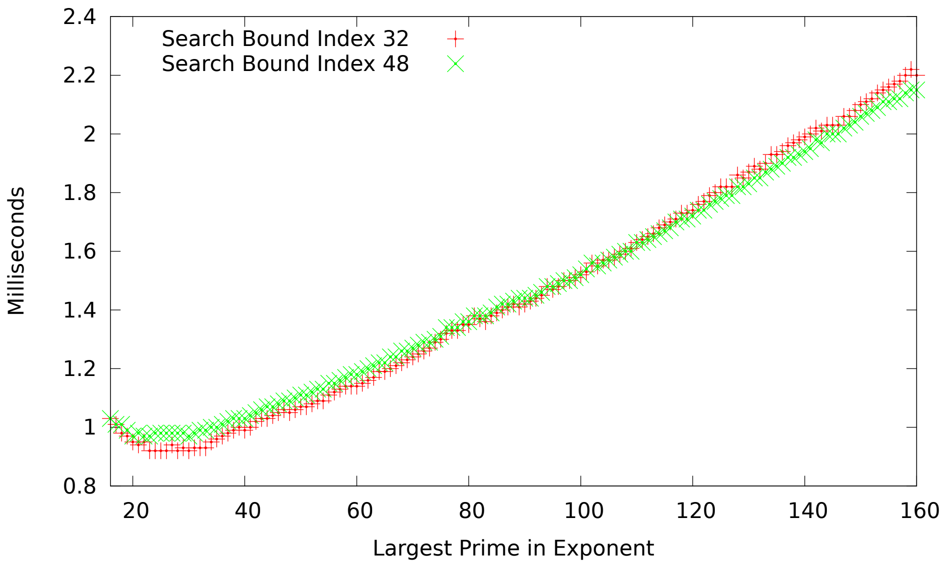


Figure 8.5: Average time to split 56-bit semiprime integers when the largest prime in the exponent $E = \prod {p_i}^{e_i}$ is iterated for a fixed search bound.

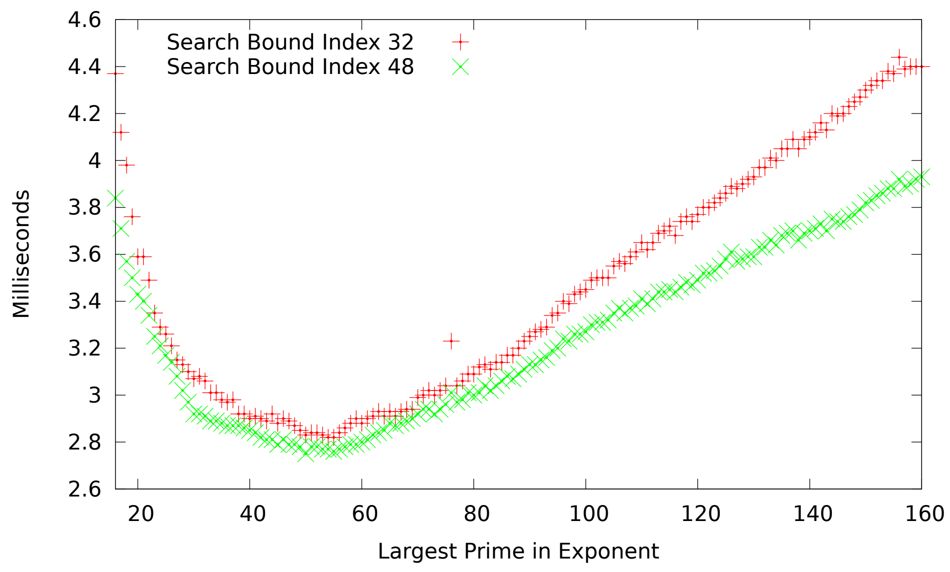


Figure 8.6: Average time to split 64-bit semiprime integers when the largest prime in the exponent $E = \prod {p_i}^{e_i}$ is iterated for fixed search bound.

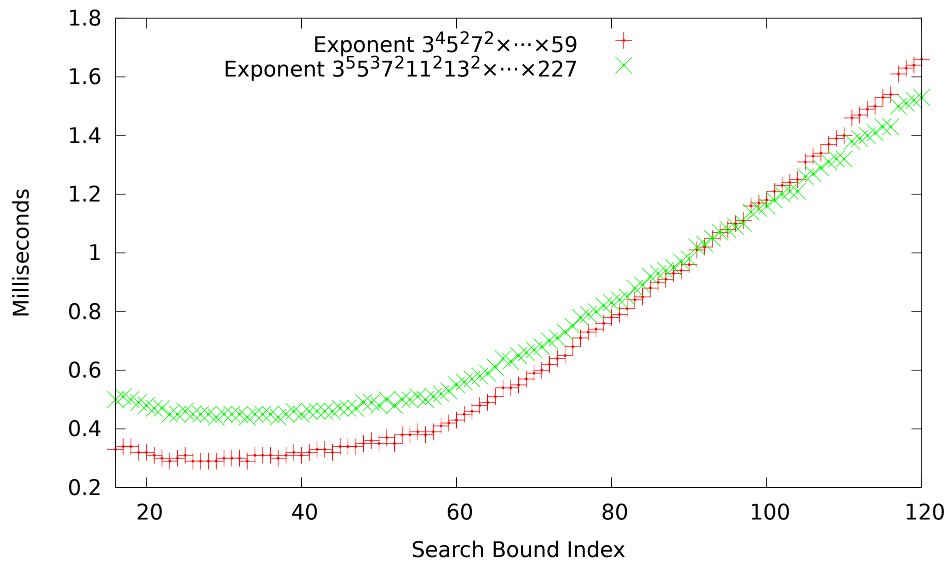


Figure 8.7: Average time to split 48-bit semiprime integers when the search bound index is iterated for fixed exponent.

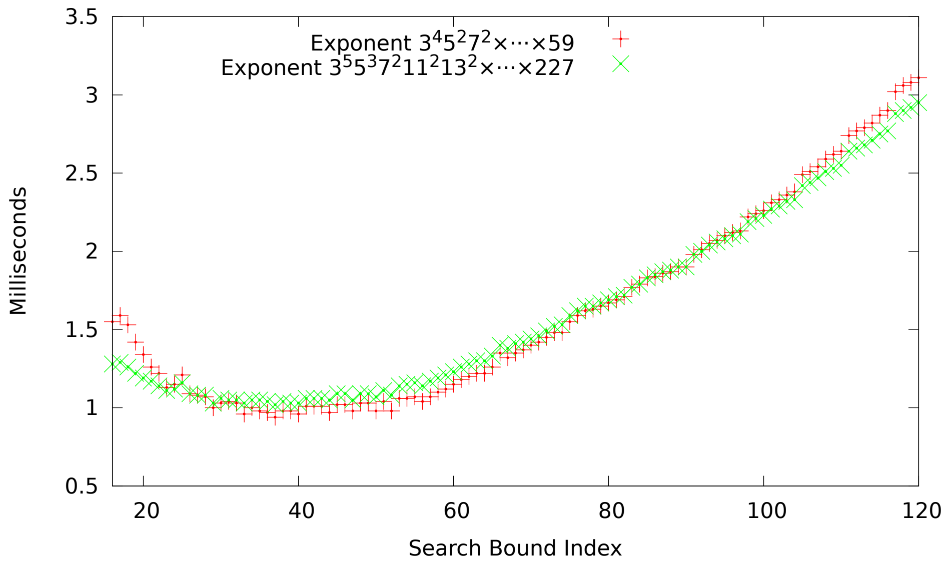


Figure 8.8: Average time to split 56-bit semiprime integers when the search bound index is iterated for fixed exponent.

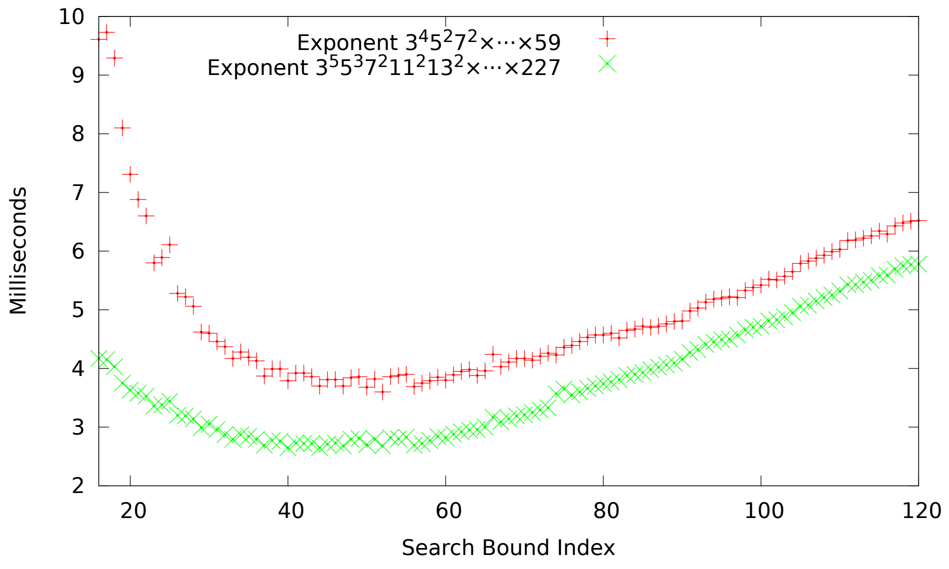


Figure 8.9: Average time to split 64-bit semiprime integers when the search bound index is iterated for fixed exponent.

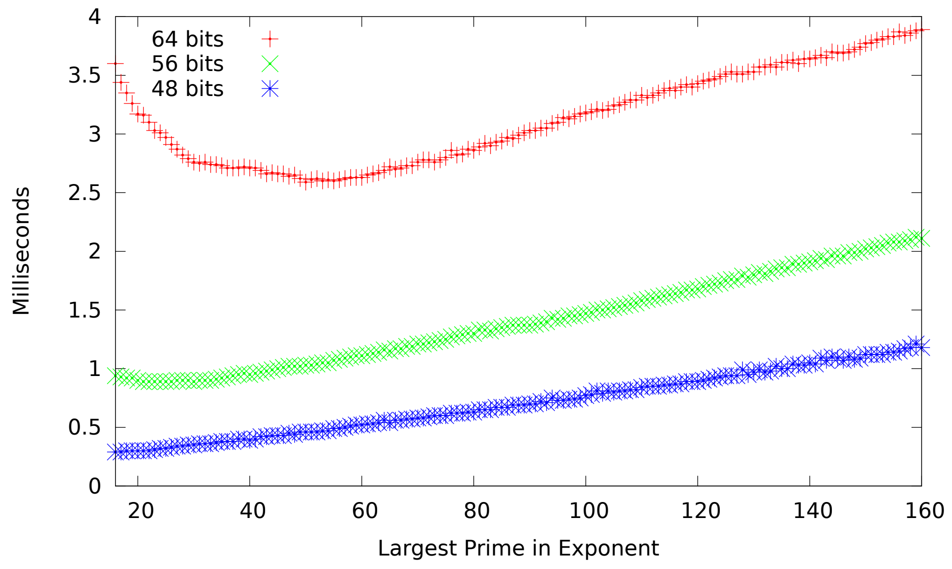


Figure 8.10: The best average time of all search bounds tested when the largest prime in the exponent $E = \prod p_i^{e_i}$ is iterated.

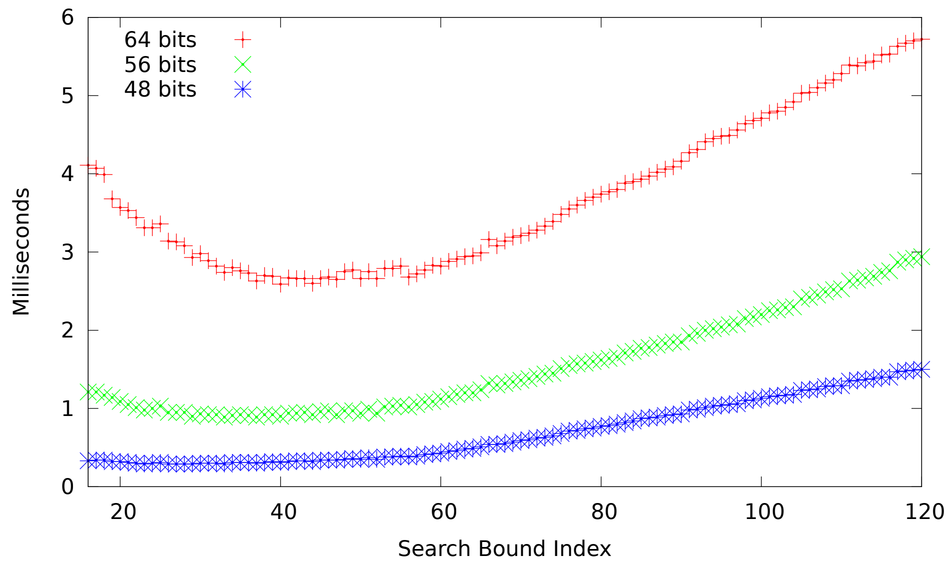


Figure 8.11: The best average time of all exponents tested when the search bound is iterated.

8.5.1 Searching a Noisy Curve

The information in the above figures is noisy, which may be partly due to the inaccuracies inherit in timing very short operations. Even so, these figures demonstrate that when one variable is fixed and the other is iterated, that the time to split an integer first generally decreases and then generally increases. Furthermore, Figures 8.10 and 8.11 show that when one variable is iterated and the other is taken to give the minimum, that the time also first generally decreases and then generally increases.

To find values for the exponentiation stage and search stage that work well in practice, one could iterate all suitable exponents E and multiples of primorials mP_w, but that would conceivably take a long time[13] for even a small sample set of integers. The Figures in the previous section suggest a more efficient approach, given by Algorithm 8.3. Using a more efficient approach also allows us to use a larger sample of integers than would be possible otherwise.

Algorithm 8.3 Determine some x such that $f(x)$ is suitably small where $f(x)$ is the average time to split integers using SuperSPAR with one free variable.

```
Input: A function $f(x)$ corresponding to the average time to split an integer,
    a search range $[x_{\min}, x_{\max}]$,
    and a bound $k$ within which to linear search.
Output: $x \in [x_{\min}, x_{\max}]$ such that $f(x)$ is suitably small.
 1: {– reduce by 1/3rd each iteration –}
 2: $(x_{\text{lo}}, x_{\text{hi}}) \leftarrow (x_{\min}, x_{\max})$
 3: while $x_{\text{hi}} - x_{\text{lo}} > k$ do
 4:     $x_\ell \leftarrow \lfloor (x_{\text{hi}} - x_{\text{lo}})/3 \rfloor + x_{\text{lo}}$
 5:     $x_h \leftarrow \lfloor 2(x_{\text{hi}} - x_{\text{lo}})/3 \rfloor + x_{\text{lo}}$
 6:     if $f(x_\ell) \le f(x_h)$ then
 7:         $x_{\text{hi}} \leftarrow x_h$
 8:     else
 9:         $x_{\text{lo}} \leftarrow x_\ell$
10:     end if
11: end while
12: {– linear search –}
13: $(x, y) \leftarrow (x_{\text{lo}}, f(x_{\text{lo}}))$        {$(x, y)$ represent smallest $f(x)$ encountered.}
14: $x_{\text{lo}} \leftarrow x_{\text{lo}} + 1$
15: while $x_{\text{lo}} \le x_{\text{hi}}$ do
16:     if $f(x_{\text{lo}}) < y$ then $(x, y) \leftarrow (x_{\text{lo}}, f(x_{\text{lo}}))$ end
17:     $x_{\text{lo}} \leftarrow x_{\text{lo}} + 1$
18: end while
19: return $x$
```

[13]The improved method proposed here took approximately 1 day to run on a set of 4,000 random semiprime integers for bits sizes 16, 18, ..., 100. See Table 8.7 for the results.

Suppose the exponent E for the exponentiation stage is fixed. Candidate search bounds mP_w are chosen from the list of search bounds $\mathcal{S}_{16384}$ generated by Algorithm 8.2 such that no candidate uses more than 16384 steps. Let x (with subscripts) denote indices into the candidate list, and $f(x)$ denote the average time to split integers for the exponent E and search bound at index x from the list $\mathcal{S}_{16384}$. Initially, let x_{lo} take the minimum search index and x_{hi} take the maximum search index. Then sample the time to split integers at one third and two third the value between x_{lo} and x_{hi}. If the time associated with the one third mark is higher, the first third of the interval is thrown away and the Algorithm recursively computes using the remaining two thirds. If the time associated with the two third mark is higher, the last third is thrown away and the Algorithm recursively computes using the first two thirds. Assuming the tendency of the timings to first decrease and then increase as the free variable increases, the third removed at each iteration should contain values generally larger than the minimum in the remaining two thirds. Since timings are noisy, when the interval $[x_{\text{lo}}, x_{\text{hi}}]$ is sufficiently small, the Algorithm simply performs a linear search in order to find the $x \in [x_{\text{lo}}, x_{\text{hi}}]$ that gives the best time. This is not guaranteed to be the best time possible for the exponent E, however, this method works well in practice.

Assuming that Algorithm 8.3 computes some search bound that is near the best possible for a given exponent for the exponentiation stage, Figure 8.10 indicates that the same algorithm can be adapted to search for the exponent for the exponentiation stage. In this case, the variable x is associated with the exponent used, and the function f first computes a suitable search bound (using Algorithm 8.3), and then returns the average time to split integers for that exponent and search bound. This way, the search for suitable values for the exponentiation stage and search stage are computed by nested applications of Algorithm 8.3.

Table 8.7 shows the values used for the exponentiation and search stage in practice for various sized integers[14]. The range of exponents for the exponentiation stage was from a

[14]For each bit size, 4,000 random semiprime integers $N = p \cdot q$ were generated. We emphasize that this

Bit Size	Largest Prime in $E = \prod {p_i}^{e_i}$	Search Bound $s = mP_w$	Total Steps	Average Time (milliseconds)
16	11	$120 = 4P_3$	62	0.17992
20	11	$36 = 6P_2$	22	0.21529
24	11	$36 = 6P_2$	22	0.01728
28	11	$90 = 3P_3$	46	0.02461
32	11	$150 = 5P_3$	78	0.03475
36	17	$240 = 8P_3$	126	0.05341
40	17	$420 = 2P_4$	190	0.07951
44	23	$630 = 3P_4$	286	0.12786
48	47	$630 = 3P_4$	286	0.19711
52	53	$1050 = 5P_4$	478	0.32283
56	89	$840 = 4P_4$	382	0.55058
60	149	$1260 = 6P_4$	574	0.93604
64	173	$1260 = 6P_4$	574	1.51579
68	263	$2310 = 1P_5$	958	2.36646
72	347	$1680 = 8P_4$	766	3.52871
76	467	$2310 = 1P_5$	958	5.42861
80	727	$3360 = 16P_4$	1534	8.53706
84	859	$4620 = 2P_5$	1918	11.97196
88	1033	$4620 = 2P_5$	1918	18.00593
92	1597	$6090 = 29P_4$	2782	29.14281
96	1861	$9240 = 4P_5$	3838	40.02095
100	2753	$7140 = 34P_4$	3262	57.97719

Table 8.7: Values for the largest prime used in the exponent $E = \prod {p_i}^{e_i}$ for the exponentiation phase, and the baby step bound mP_w used for the search stage.

largest prime of 11 in the exponent to a largest prime of 2753. The range for search bounds was given by the set $\mathcal{S}_{16384}$. Algorithm 8.3 was configured to switch to a linear search when the size of the range was ≤ 8. Notice that the largest primorial used for search bounds is P_5, which justifies our approach to bounding the values e_i in the exponent $E = \prod {p_i}^{e_i}$ for values of $i \leq 5$.

set is different from the set of semiprime integers used in Section 8.6 so as to avoid training SuperSPAR on the same set of integers used for comparison with other factoring algorithms.

8.6 Comparison to Other Factoring Implementations

To demonstrate the performance of our implementation of SuperSPAR, several factoring implementations were timed, namely Pari/GP [6], Msieve [5], GMP-ECM [2], YAFU [7], Flint [1], Maple [4], and a custom implementation of SQUFOF [23] adapted from the source code of Pari/GP.

For bit sizes 16, 18, ..., 100, sets of 10,000 random semiprime integers $N = p \cdot q$ for p and q prime and half the size of N were generated and written to disk. The file format was ASCII with one integer per line. For each factoring implementation, either this file was converted to an implementation specific format so that all the integers could be factored in batch, or, if a C programming interface was provided, a program was written to load the set of integers and use the library directly[15]. The hardware platform was a personal notebook with a 2.7GHz Intel Core i7-2620M CPU and 8Gb of memory. The CPU has four cores, only one of which was used during timing experiments. The operating system was 64-bit Ubuntu 12.10. When possible, the most recent version of each factoring implementation was used and built from source using the GNU C compiler version 4.7.2. Timings include forking the process, reading and parsing the test set, and factoring all the integers in the set. The timings do not include the generation of the semiprime integers or the conversion to the implementation specific batch file.

Figures 8.12 through 8.16 were chosen to emphasize different features of the performance of SuperSPAR. Figure 8.12 shows the performance of each factoring implementation for the complete range of integer sizes timed – visually, SuperSPAR is not particularly competitive for integers much larger than 90-bits. Figure 8.13 zooms in on the range of integers 44-bits to 72-bits. This shows that SQUFOF quickly becomes impractical for integers larger than 70-bits, and that Maple, Msieve, and GMP-ECM do not perform as efficiently as the other implementations for integers in the range 44-bits to 72-bits. This also shows that SuperSPAR

[15]In the case of Pari/GP, Flint, SQUFOF, and SuperSPAR, C programming libraries were provided. Msieve, GMP-ECM, YAFU, and Maple were scripted.

is highly competitive below 64-bits. Figure 8.14 shows the 5 best performing implementations for integers in the range of 44-bits to 68-bits. Figure 8.15 zooms in on the left of this image for integers in the range 44-bits to 58-bits. This shows the same 5 implementations. For integers between 44-bits and around 50-bits, the custom implementation of SQUFOF is the fastest performing, but as the integer size grows, SQUFOF takes longer more quickly. For integers around 50-bits in size, SuperSPAR is typically the fastest performing implementation of the implementations tested. Finally, Figure 8.16 zooms in on the right part of Figure 8.14. This shows the 3 best performing implementations for this range, and the point at which the performance of SuperSPAR decreases and YAFU is better performing. This occurs for integers around 64-bits in size.

Table 8.8 shows the average time in milliseconds to factor integers for each bit size given a particular implementation. The best performing implementation for integers of a given size is underlined. Timings were only recorded for implementations and integer sizes that took less than 100 milliseconds on average. In the case of SQUFOF, this was for integers 74-bits in size and less. Inexplicably, for integers of size 24-bits, 28-bits, and 42-bits, Flint did not complete the test set before crashing. Similarly, Msieve crashed for all sets of integers larger than 84-bits. This table shows that for integers in the range of 50-bits to 62-bits, SuperSPAR performs the fastest on average.

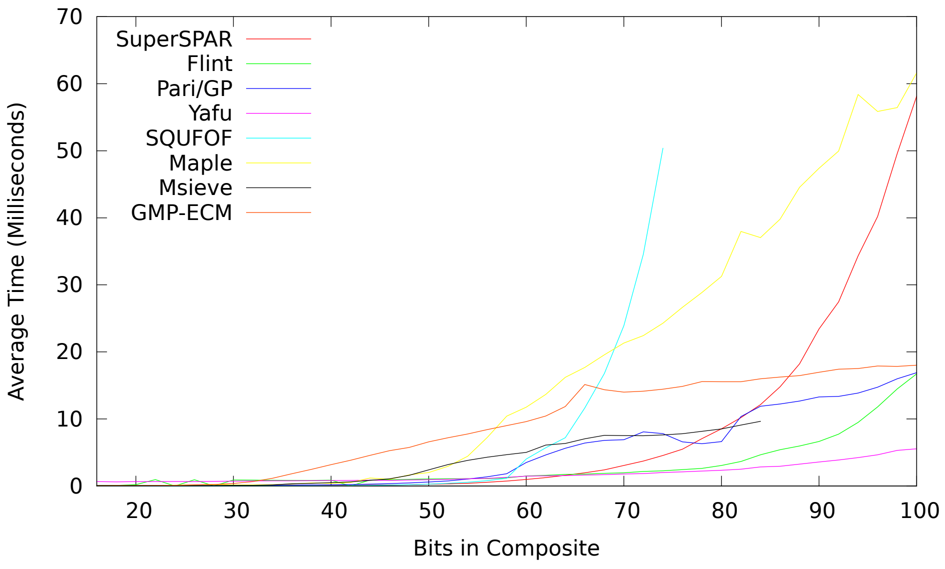


Figure 8.12: The performance of each factoring implementation for integers 16-bits to 100-bits. SuperSPAR appears to be competitive at less than 70-bits.

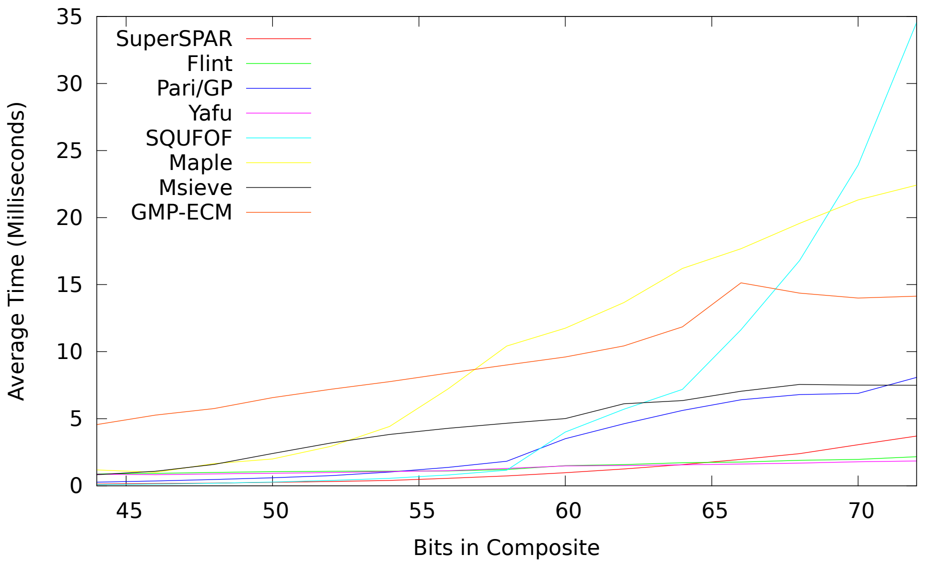


Figure 8.13: The performance of each factoring implementation for integers 44-bits to 72-bits. In this range, Maple, Msieve, and GMP-ECM do not appear to be competitive.

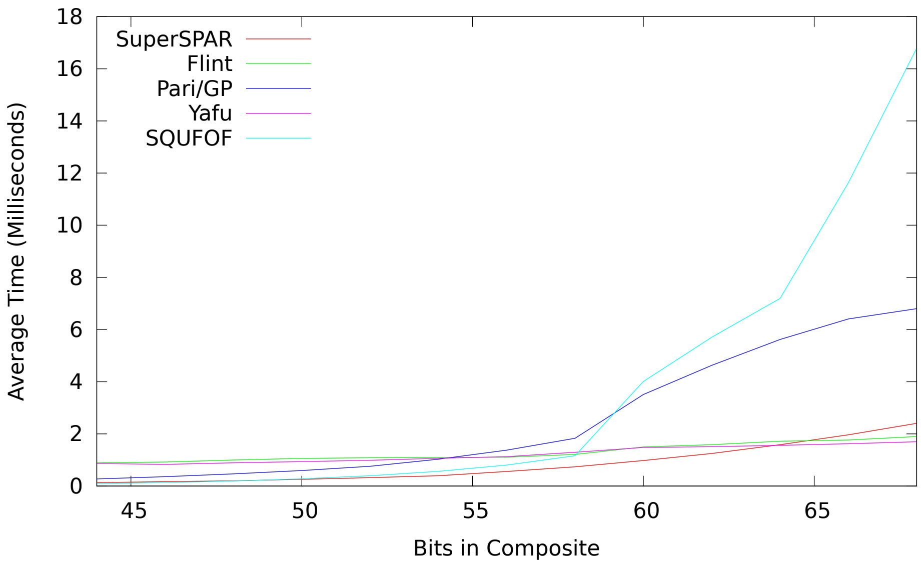


Figure 8.14: The 5 best performing factoring implementations for integers in the range 44-bits to 68-bits. This range shows that SuperSPAR is the fastest performing implementation for some integer sizes.

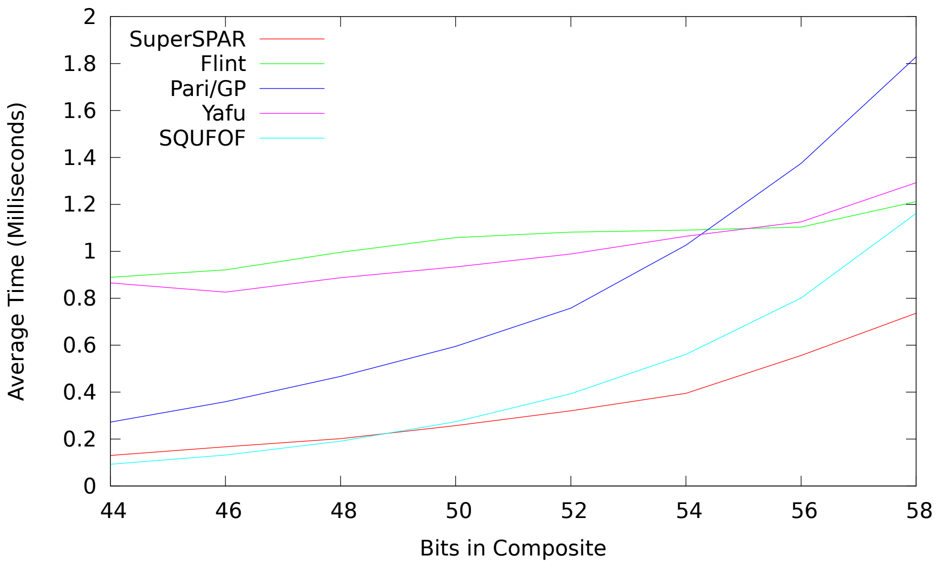


Figure 8.15: The 5 best performing factoring implementations for integers in the range 44-bits to 58-bits. This focuses the range on the lower half of Figure 8.14. Here SQUFOF grows faster than SuperSPAR and at integers around 50-bits in size, SuperSPAR is the best performing implementation.

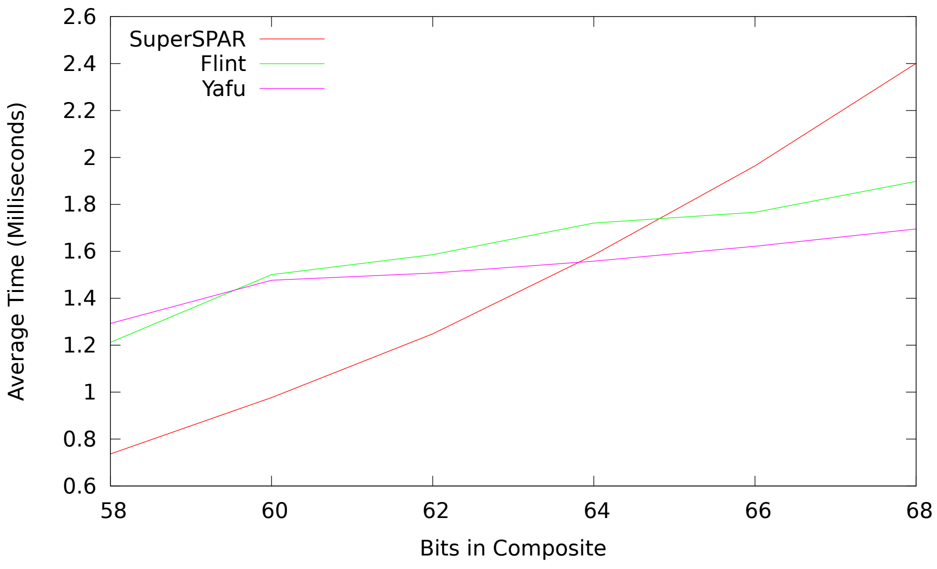


Figure 8.16: The 3 best performing factoring implementations for integers in the range 58-bits to 68-bits. This focuses the range on the upper half of Figure 8.14 and demonstrates that around integers 64-bits in size, YAFU performs better than SuperSPAR.

Bits	ECM	Flint	Maple	Msieve	Pari/GP	SQUFOF	SSPAR	Yafu
16	0.0270	0.0378	0.0505	0.0799	0.0065	0.0008	0.0097	0.6524
18	0.0337	0.0774	0.0920	0.0815	0.0070	0.0010	0.0116	0.6082
20	0.0473	0.1994	0.0637	0.0812	0.0085	0.0018	0.0128	0.6492
22	0.0660	0.9614	0.0795	0.0820	0.0086	0.0021	0.0165	0.6469
24	0.0946	failed	0.1205	0.0829	0.0127	0.0028	0.0195	0.6779
26	0.1740	0.9406	0.1340	0.0832	0.0180	0.0040	0.0221	0.6569
28	0.2235	failed	0.2380	0.0883	0.0261	0.0056	0.0265	0.6975
30	0.3783	0.8982	0.1544	0.0914	0.0824	0.0077	0.0311	0.7193
32	0.6537	0.8725	0.1641	0.1003	0.0957	0.0110	0.0365	0.7511
34	1.1481	0.8591	0.2044	0.1642	0.1199	0.0158	0.0465	0.7827
36	1.8327	0.8310	0.2822	0.3351	0.1357	0.0222	0.0548	0.7661
38	2.4831	0.8327	0.4612	0.4004	0.1610	0.0313	0.0662	0.8022
40	3.1906	0.8796	0.3906	0.4883	0.1870	0.0461	0.0821	0.8167
42	3.8457	failed	0.5226	0.6174	0.2205	0.0648	0.1045	0.8439
44	4.5650	0.8890	1.1850	0.8271	0.2722	0.0928	0.1298	0.8655
46	5.2680	0.9210	0.9994	1.0838	0.3591	0.1320	0.1671	0.8263
48	5.7561	0.9963	1.6464	1.5946	0.4670	0.1911	0.2014	0.8873
50	6.5731	1.0584	2.0015	2.4111	0.5947	0.2741	0.2573	0.9338
52	7.2033	1.0819	2.9428	3.1965	0.7578	0.3929	0.3202	0.9886
54	7.7635	1.0901	4.4271	3.8279	1.0259	0.5608	0.3949	1.0640
56	8.4054	1.1036	7.2331	4.2903	1.3752	0.8010	0.5563	1.1253
58	9.0041	1.2117	10.4179	4.6656	1.8292	1.1622	0.7365	1.2925
60	9.6012	1.5008	11.7576	5.0153	3.5080	4.0100	0.9769	1.4769
62	10.4339	1.5859	13.6654	6.1142	4.6261	5.7092	1.2482	1.5075
64	11.8548	1.7206	16.2116	6.3498	5.6207	7.1933	1.5846	1.5577
66	15.1356	1.7662	17.6785	7.0451	6.4084	11.6313	1.9639	1.6214
68	14.3670	1.8983	19.5723	7.5541	6.8028	16.7912	2.4011	1.6952
70	13.9973	1.9687	21.3196	7.5087	6.8940	23.9112	3.0578	1.7895
72	14.1343	2.1680	22.4251	7.4943	8.0791	34.5667	3.7133	1.8536
74	14.4356	2.2741	24.2755	7.6182	7.8113	50.3791	4.5587	2.0003
76	14.8602	2.4442	26.6470	7.8022	6.5805	–	5.4914	2.0998
78	15.5668	2.6173	28.8623	8.1577	6.2996	–	7.0521	2.2202
80	15.5548	3.0537	31.2528	8.5141	6.6235	–	8.5300	2.3407
82	15.5577	3.6557	37.9693	9.0961	10.3569	–	10.2062	2.5122
84	15.9824	4.6584	37.0573	9.6379	11.8881	–	12.1335	2.8428
86	16.2545	5.4168	39.7901	failed	12.2243	–	14.7879	2.9365
88	16.4600	5.9574	44.5510	failed	12.6767	–	18.2133	3.2695
90	16.9574	6.6372	47.3801	failed	13.2897	–	23.4263	3.5713
92	17.4196	7.7319	49.9509	failed	13.3701	–	27.4630	3.8687
94	17.5219	9.4851	58.3808	failed	13.8622	–	34.3230	4.2393
96	17.9056	11.7830	55.8692	failed	14.7439	–	40.1884	4.6538
98	17.8311	14.4835	56.4315	failed	15.9800	–	49.5837	5.3058
100	18.0168	16.7292	61.6214	failed	16.9010	–	58.1393	5.5532

Table 8.8: The average time (in milliseconds) to factor integers of a given size for a particular implementation.

Chapter 9

Future Work

The work of this thesis is to improve exponentiation in the ideal class group of imaginary quadratic number fields, with an application to integer factoring. This lead to practical improvements when computing the extended GCD for bounded integers (Chapter 5) as well as improvements to ideal class arithmetic for bounded discriminants (Chapter 6). Chapter 7 lead to practical performance improvements when exponentiating an ideal class with bounded discriminant to a large primorial. Finally, this thesis revisits the SPAR factoring algorithm using the contributions to ideal class arithmetic and exponentiation in the context of the primorial steps algorithm. Section 8.6 compares our implementation of SuperSPAR to several integer factoring libraries to show that the performance improvements of this thesis lead to SuperSPAR being the fastest implementation for integers in the range of 54-bits to 64-bits (TODO).

For the work of this thesis to be most useful to the future work of others, the source code for the libraries used throughout is available online, and the hope is for eventual inclusion into common mathematical packages such as Pari/GP, Sage, and Dr. Michael J. Jacobson, Jr.'s algorithmic number theory library.

- A library for 128-bit arithmetic, extended GCD computations, generic group exponentiation, and 2,3 representations.

  `https://github.com/maxwellsayles/liboptarith`

- Ideal class arithmetic library, specialized for discriminants bound by 59-bits, 118-bits, and unbound.

  `https://github.com/maxwellsayles/libqform`

- Our implementation of the SuperSPAR integer factoring library.

`https://github.com/maxwellsayles/libsspar`

The work presented in this thesis is by no means exhaustive. Sections 9.1, 9.2, and 9.3 contain suggestions for future work in ideal class arithmetic, exponentiation, and integer factoring respectively.

9.1 Ideal Arithmetic

The practical improvements to arithmetic in the ideal class group are based on the Algorithms for computing reduced (or almost reduced) representatives for multiplication (Subsection 2.5.5), squaring (Subsection 2.5.6), and cubing (Subsection 2.5.7). While these Algorithms are certainly faster as the size of the discriminant grows, future work could include a comparison of the implementation in this thesis with an implementation of the basic ideal class multiplication presented in Subsection 2.5.4. The idea would be to optimize an implementation as well as make improvements to the ideal reduction algorithm from Subsection 2.5.1. Ideal reduction is similar to the standard Euclidean Algorithm, as such, future work might apply several of the approaches used for computing the extended GCD to that of ideal reduction.

Additional techniques for computing the extended GCD can be explored. A relatively straightforward approach is to apply windowing to the left-to-right binary GCD that performed well for 32-bit to 64-bit integers. Binary GCD computations favour bit shifting over multiplication and division since bit shifting is faster. In groups where squaring and cubing are fast, an interesting combination to explore would be a right-to-left 2,3 GCD, similar to the right-to-left 2,3 chain of Section 7.2.

With future improvements to basic ideal class arithmetic, additional comparisons to other implementations would be useful, such as to Pari/GP and Sage. Finally, one could study practical improvements to other types of ideal arithmetic, such as the class group of real quadratic fields or function fields.

9.2 Exponentiation

The ideal class exponentiation experiments of Chapter 7 assume that the exponents are primorials and that representations can be precomputed. Future work could include a study of the time to generate 2,3 representations against the time to exponentiation using such representations. Our expectation is that representations that lead to faster exponentiations also take longer to generate, and that the rate at which the time to exponentiate improves is slower than the rate at which the time to generate the representation grows. Along this line, one could also rigorously analyse the expected cost to exponentiate using representations generated by a particular technique, or one could analyse the cost of generating representations for each of the techniques described.

The L best approximations technique of Section 7.6 generated 2,3 representations for large primorials that worked well in practice. This algorithm iterated on the L smallest partial representations. Future work could consider other heuristics on which to prune candidates, such as approximating the cost of the complete chain based on the partial chain and retaining the L best approximate costs.

For the techniques of Chapter 7, the cost associated with exponentiating shows general trends as the size of the primorial grows. However, for exponent N and exponent $N+1$, the cost can vary considerably. Interesting and useful work would be to provide upper bounds (as a function of N) on how much the cost can vary as the exponent increases by a fixed amount.

Finally, in this thesis, we only consider double base number systems using bases 2 and 3. Future work should consider other bases. This would involve additional research with ideal arithmetic to determine the benefit of direct methods for computing $[\mathfrak{a}]^5$, $[\mathfrak{a}]^7$, and so on, for an ideal class $[\mathfrak{a}]$. Other open areas are multiple base number systems, i.e. number systems where an integer is expressed as the sum and difference of powers of several coprime bases $N = \sum_i \left(s_i \prod_j {p_j}^{e_{i,j}} \right)$.

9.3 Super^{2}SPAR

Practical improvements in this thesis to ideal class arithmetic and to exponentiation also lead to improvements in the SuperSPAR integer factoring algorithm. Future work in either area will naturally contribute to future improvements to SuperSPAR. There are, however, many open research areas that could lead to direct practical improvements to SuperSPAR.

Parameters in our implementation were chosen to work well in practice. For a given discriminant associated with the integer to be factored, there is only a probability that the integer N will be split. Often many different multipliers for the discriminant are tried before a successful splitting of N. Future work would include a study of these multipliers, and more formal work would include bounding the probability that a specific number of multipliers are used. Subsection 8.2.3 showed that for $N \bmod 4$ different multipliers were associated with a different number of ideal classes to try in expectation before a splitting of N. Studying the behaviour of multipliers may be useful in the parallelization of SuperSPAR – simply, the algorithm could run on several multiplier in parallel. One possible highly parallel platform for consideration would be an implementation of SuperSPAR for GPUs.

There are many open questions surrounding the running time of SuperSPAR. Incomplete investigations show that the majority of integers only require a single multiplier before a successful splitting of the integer, however, a small number of integers require a very large number of multipliers. These few *hard* numbers tend to skew the average running time. Future work would include quartile timings and 5-number summaries of samples of integers to be split. Additional work could include more rigorous analysis of the median asymptotic complexity of SuperSPAR. Not necessarily related to SuperSPAR would be a theoretical analysis of the factorization of the order of ideal classes, such as the probabilities of certain divisors of the order.

The study of ideal class arithmetic, exponentiation, and our implementation of Super-SPAR given in this thesis was guided by practice. SPAR is theoretically capable of larger interger factorizations, and so is SuperSPAR. Interesting future work would be to generate much larger exponents that would be stored on disk. A method of computing 2,3 representations with low space requirements (such as right-to-left 2,3 chains of Section 7.2) could be used to exponentiate an ideal by a primorial stored on disk. Since the bounded primorial steps algorithm requires a large amount of memory, an alternative Pollard-Brent recursion as suggested by Schnorr and Lenstra [41] would be space efficient and may be able to take steps coprime to the exponent used. More generally, the bounded primorial steps algorithm can be used to compute discrete logarithms, and there are many open questions as to the difficulty of the discrete log problem in the ideal class group of imaginary quadratic number fields.

Bibliography

[1] Flint 2.3. `http://www.flintlib.org/`. Accessed: 2013-04-10.

[2] GMP-ECM 6.4.4. `http://ecm.gforge.inria.fr/`. Accessed: 2013-04-10.

[3] GNU Multiple Precision (GMP) Library. `http://gmplib.org/`. Accessed: 2013-04-10.

[4] Maple 13. `http://www.maplesoft.com/`. Accessed: 2013-04-10.

[5] Msieve 1.5.1. `http://msieve.sourceforge.net/`. Accessed: 2013-04-10.

[6] Pari/GP 2.5.1. `http://pari.math.u-bordeaux.fr/`. Accessed: 2013-04-10.

[7] YAFU (Yet Another Factoring Utility) 1.33. `http://yafu.sourceforge.net/`. Accessed: 2013-04-10.

[8] E. Bach and J.O. Shallit. *Algorithmic Number Theory: Efficient Algorithms*. Number 1 in Foundations of Computing. Mit Press, 1996.

[9] Valérie Berthé and Laurent Imbert. Diophantine approximation, Ostrowski numeration and the double-base number system. *Discrete Mathematics and Theoretical Computer Science*, 11(1):153–172, 2009.

[10] Richard P. Brent. An improved Monte Carlo factorization algorithm. *BIT*, 20(2):176–184, 1980.

[11] Mathieu Ciet, Marc Joye, Kristin Lauter, and Peter L. Montgomery. Trading inversions for multiplications in elliptic curve cryptography. *Des. Codes Cryptography*, 39(2):189–206, May 2006.

[12] Mathieu Ciet and Francesco Sica. An analysis of double base number systems and a sublinear scalar multiplication algorithm. *Mycrypt*, 3715:171–182, 2005.

[13] H. Cohen and G. Frey, editors. *Handbook of elliptic and hyperelliptic curve cryptography.* Chapman & Hall/CRC, 2006.

[14] H. Cohn. *Advanced Number Theory.* Dover Books on Mathematics. Dover Publications, 1980.

[15] Thomas H. Cormen, Clifford Stein, Ronald L. Rivest, and Charles E. Leiserson. *Introduction to Algorithms.* McGraw-Hill Higher Education, 2nd edition, 2001.

[16] R.E. Crandall and C. Pomerance. *Prime Numbers: A Computational Perspective.* Springer, 2001.

[17] V. Dimitrov and T. Cooklev. Hybrid algorithm for the computation of the matrix polynomial $I + A + \cdots + A^{N-1}$. *IEEE Transactions on Circuits and Systems – I: Fundamental Theory and Applications*, 42(7), July 1995.

[18] V. Dimitrov and T. Cooklev. Two algorithms for modular exponentiation using nonstandard arithmetics. *IEICE Trans. Fundamentals*, E78-A(1), January 1995.

[19] V. Dimitrov, K.U. Järvinen, M.J. Jacobson, W.F. Chan, and Z. Huang. Provably sublinear point multiplication on Koblitz curves and its hardware implementation. *IEEE Transaction on Computers*, 57(11), November 2008.

[20] V. S. Dimitrov, L. Imbert, and P. K. Mishra. Fast elliptic curve point multiplication using double-base chains, 2005.

[21] Christophe Doche and Laurent Habsieger. A tree-based approach for computing double-base chains. In *ACISP*, pages 433–446, 2008.

[22] Albrecht Fröhlich and Martin Taylor. *Algebraic Number Theory (Cambridge Studies in Advanced Mathematics)*, volume 27. Cambridge University Press, 1993.

[23] Jason E. Gower and Samuel S. Wagstaff Jr. Square form factorization. *Math. Comput.*, 77(261):551–588, 2008.

[24] Torbjörn Granlund and Peter L. Montgomery. Division by invariant integers using multiplication. In *In Proceedings of the SIGPLAN '94 Conference on Programming Language Design and Implementation*, pages 61–72, 1994.

[25] L.K. Hua and P. Shiu. *Introduction to Number Theory*. Springer London, Limited, 2012.

[26] L. Imbert, M.J. Jacobson, and A. Schmidt. Fast ideal cubing in imaginary quadratic number and function fields. *Advanced in Mathematics of Communications*, 4(2):237–260, 2010.

[27] Laurent Imbert and Fabrice Philippe. Strictly chained (p,q)-ary partitions. *Contributions to Discrete Mathematics*, 5(2), 2010.

[28] K. Ireland and M.I. Rosen. *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics. Springer, 1990.

[29] M.J. Jacobson. *Subexponential Class Group Computation in Quadratic Orders*. Berichte aus der Informatik. Shaker, 1999.

[30] M.J. Jacobson, R.E. Sawilla, and H.C. Williams. Efficient ideal reduction in quadratic fields. *International Journal of Mathematics and Computer Science*, 1:83–116, 2006.

[31] M.J. Jacobson and H.C. Williams. *Solving the Pell Equation*. CMS books in mathematics. Springer, 2009.

[32] Donald E. Knuth. *The art of computer programming, volume 3: (2nd ed.) sorting and searching*. Addison Wesley Longman Publishing Co., Inc., Redwood City, CA, USA, 1998.

[33] Andrew Kuchling. Python's dictionary implementation: Being all things to all people. In Andy Oram and Greg Wilson, editors, *Beautiful Code: Leading Programmers Explain How They Think*, pages 293–318. O'Reilly Media, 2008.

[34] D.H. Lehmer. Euclid's algorithm for large numbers. *American Mathematical Monthly*, 45(4):227–233, April 1938.

[35] Jr. H.W. Lenstra and Carl Pomerance. A rigorous time bound for factoring integers. *Journal of the American Mathematical Society*, 5(3), July 1992.

[36] Nicolas Méloni and M. Anwar Hasan. Elliptic curve scalar multiplication combining Yao's algorithm and double bases. In *Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '09, pages 304–316, Berlin, Heidelberg, 2009. Springer-Verlag.

[37] Niels Möller and Torbjörn Granlund. Improved division by invariant integers. *IEEE Transactions on Computers*, 60(2):165–175, 2011.

[38] J. M. Pollard. A monte carlo method for factorization. *BIT Numerical Mathematics*, 15:331–334, 1975.

[39] S. Ramachandran. Numerical results on class groups of imaginary quadratic fields. Master's thesis, University of Calgary, Canada, 2006.

[40] George W. Reitwiesner. Binary arithmetic. *Advances in Computers*, 1:231–308, 1960.

[41] C.P. Schnorr and Jr. H.W. Lenstra. A Monte Carlo factoring algorithm with linear storage. *Mathematics of computation*, 43(167), July 1984.

[42] Jeffrey Shallit and Jonathan Sorenson. Analysis of a left-shift binary GCD algorithm. *Journal of symbolic computation*, 17:473–486, 1994.

[43] D. Shanks. Class number, A theory of factorization and genera. In *Symp. Pure Math.*, volume 20, pages 415–440, Providence, R.I., 1971. AMS.

[44] D. Shanks. On Gauss and composition I, II. *Proc. NATO ASI on Number Theory and Applications*, pages 163–179, 1989.

[45] J. Stein. Computational problems associated with racah algebra. *Journal of Computational Physics*, 1(3):397–405, February 1967.

[46] A.V. Sutherland. *Order computations in generic groups.* PhD thesis, M.I.T., 2007.

[47] A.V. Sutherland. A generic approach to searching for Jacobians. *Mathematics of computation*, 78(265):485–507, january 2009.

[48] Henry S. Warren. *Hacker's Delight.* Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002.