The Sieve Re-Imagined: Integer Factorization Methods

by

Jennifer Smith

A research paper
presented to the University of Waterloo
in partial fulfillment of the
requirement for the degree of
Master of Mathematics
in
Computational Mathematics

Supervisor: Prof. Kevin Hare

Waterloo, Ontario, Canada, 2012

I hereby declare that I am the sole author of this report. This is a true copy of the report, including any required final revisions, as accepted by my examiners.

I understand that my report may be made electronically available to the public.

Abstract

In this paper, I explain the Quadratic Sieve, its Multiple Polynomial variation, the Number Field Sieve, and give some worked examples of the afore-mentioned algorithms. Using my own Maple implementation of the Quadratic Sieve, I explore the effect of altering one of the parameters of the Quadratic Sieve algorithm, with respect to both time and success rate.

Acknowledgements

Many people have contributed to my success this year. First of all, I would like to thank my family for all of their support. My mother was always willing to lend an ear and tell me to treat myself to a glass of wine. My father's sympathy was less frequent, but he was always encouraging me to do my best. My brother's good advice was never-ending, but it was always comforting. Their constant faith in my abilities has meant a lot to me this year.

I would like to thank my supervisor for being so generous with his time and knowledge. I also appreciate his willingness to accommodate my constant need for schedules. I feel that I accomplished a lot with this project, and I definitely would not have liked to do it alone.

I want to thank Anthea Dunne for all that she does. Handling administrative matters in a new place can be tricky, but she was always so helpful!

Many thanks to Alfred Menezes for letting me sit in on his Applied Cryptography class, even though it was full. With a waiting list. His lectures were always very engaging, and I very much enjoyed the course.

Dedication

This is dedicated to my parents. Without their love and support I would not be able to factor integers.

Table of Contents

List of Tables vii

List of Figures viii

1 Introduction 1

2 The Quadratic Sieve 3

2.1 The Algorithm . . . 3

2.2 A Nice Example . . . 5

2.2.1 Hensel Lifting . . . 7

2.3 Summary . . . 11

3 Extending to Multiple Polynomials 13

3.1 The Algorithm . . . 13

3.2 Example . . . 15

3.3 Summary . . . 17

4 The Number Field Sieve 18

4.1 The Algorithm . . . 18

4.2 The Second "Mini"-Vector . . . 21

4.3 The Third "Mini"-Vector . . . 24

4.4 Summary . . . 28

5 The Experiment 29

6 Conclusion 32

References 34

List of Tables

2.1 Potential B-Smooth Numbers 5
2.2 Sieving by 2. 9
2.3 Sieving by powers of 3. 9
2.4 Sieving by powers of 7. 10
2.5 Sieving by 13. 10
2.6 Sieving 12

3.1 Potential B-Smooth Numbers 16
3.2 Smooth Numbers 16

4.1 Make Third Mini- Vectors: Part 1. 26
4.2 "Mini"-Vector Corresponding to $a - b\sigma$ 27

List of Figures

5.1 Experimental Results. 30

Chapter 1

Introduction

In 1903, F. Cole successfully factored the Mersenne number $n = 2^{67} - 1$ using the naive factoring method [11]. Mersenne conjectured that this number was prime, but no one had been able to factor it until Cole [1]. It took Cole three years of Sundays to find all seven prime factors and was a great achievement at the time; he received a standing ovation after presenting his findings to his colleagues [8]. Today, Maple's *ifactor* function can do this in 0.047 seconds (July 27, 2012).

Since 1903, we have had two major developments that have pushed integer factoring capabilities to where they stand today. First is the success of the computer, which allows for quick efficient factoring for many numbers. Next, is the introduction of the RSA Encryption Scheme by Rivest, Shamir, & Adleman in 1977, which bases its whole security on the assumption that factoring larger integers is a difficult problem. This generated significant interest in factoring integers and has led to the development of many new algorithms. Thus, mathematicians have studied integer factoring methods as an interesting problem in its own right, as well as to test security for the RSA scheme.

In 1982, Pomerance introduced the Quadratic Sieve (QS), a highly successful method for factoring large numbers [12]. It uses the idea that for any odd prime p, there are two square roots of 1 in $\mathbb{Z}_p$, namely ± 1. A composite number, n, with k distinct prime factors, can be written as a product of primes, say $n = p_1 \cdots p_k$. Then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$ and there are two choices for the square root of 1 in every $\mathbb{Z}_{p_i}$. The Chinese Remainder Theorem tells us that there are 2^k square roots of 1 in $\mathbb{Z}_n$. For example, the square roots of 1 in $\mathbb{Z}_{15}$ are 1, -1, 4, and $-4 = 11$. Note that these correspond to the pairs $(1, 1)$, $(-1, -1)$, $(1, -1)$, and $(-1, 1)$ in $\mathbb{Z}_3 \times \mathbb{Z}_5$, respectively.

We notice from the example that two of the square roots of 1 in $\mathbb{Z}_{15}$ are still ± 1. This is true for all composite numbers n. More interestingly, the other square roots of 1 can be used to factor n [3]. Indeed, finding an integer x with $x^2 \equiv 1 \pmod{n}$ and $x \not\equiv \pm 1$

$(\text{mod } n)$ is the same as finding x such that $0 \equiv x^2 - 1 \equiv (x-1)(x+1) \pmod{n}$. Equivalently, the greatest common divisor (GCD) of $x-1$ or $x+1$ with n is non-trivial. Since $x \pm 1 < n$, we have that n cannot divide either $x+1$ or $x-1$, so part of n must divide $x-1$ and part must divide $x+1$. Continuing the example from before, we have $4^2 \equiv 11^2 \equiv 1 \pmod{15}$. Further, we find that $\gcd(4+1, 15) = 5$ and $\gcd(4-1, 15) = 3$. Similarly, $\gcd(11+1, 15) = 3$ and $\gcd(11-1, 15) = 5$.

This would work just as well by replacing 1 with any other square. If we find x, y such that $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv \pm y \pmod{n}$, then we can factor n. In this case, n divides $(x-y)(x+y)$, but n divides neither $(x+y)$ nor $(x-y)$ [14]. If we look at $\mathbb{Z}_{15}$ again, we find that $2^2 \equiv 7^2 \pmod{15}$ with $2 \not\equiv \pm 7 \pmod{15}$. We see that $\gcd(7-2, 15) = 5$ and $\gcd(7+2, 15) = 3$, and we have factored 15.

The QS is a method to find x and y with the property that $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv \pm y \pmod{n}$ by sieving for smooth numbers over evaluations of quadratic polynomials. The Number Field Sieve (NFS) uses this same idea, but goes about finding x and y a bit differently from the Quadratic Sieve. An early version of the NFS was introduced by Pollard in 1988 as a method for factoring numbers which are close to prime powers. For example, Mersenne numbers like $n = 2^{67} - 1$. It was Lenstra who made it applicable for general composites in 1990, when the name was changed to the Number Field Sieve.

We present a description and example of the Quadratic Sieve in Chapter 2. We extend the Quadratic Sieve method by using Multiple Polynomials in Chapter 3. In Chapter 4, we give an overview of the Number Field Sieve and in Chapter 5, we discuss experiments performed with a Maple implementation of the Quadratic Sieve to explore the optimal length of values to sieve in order to perform the algorithm quickly and correctly. Our last chapter contains some concluding remarks.

Chapter 2

The Quadratic Sieve

2.1 The Algorithm

To factor n, we need to find x and y such that $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv \pm y \pmod{n}$. The following procedure outlines how the Quadratic Sieve goes about doing this [3, 7].

1. Generate B-Smooth Numbers

   Choose an integer B and let $\mathcal{B} = \{p_j : p_j \text{ prime}, p_j \leq B, \}$ where we have indexed the primes and p_j is the j^{th} element in $\mathcal{B}$. We call $\mathcal{B}$ a *factor base*. Note that there is another criterion for a prime p_j to be in $\mathcal{B}$, but that will be explained shortly. The recommended value for B is $\exp(\frac{1}{2}(\ln n \ln\ln n)^{1/2})$, but a smaller value usually works.

   Find a sequence of integers z_i such that $z_i^2 - n$ is a product of primes in $\mathcal{B}$. If $z_i^2 - n$ factors in such a way, we call it *B-smooth*. Disregard any pairs $(z_i,\ z_i^2 - n)$ where $z_i^2 - n$ does not factor over $\mathcal{B}$. If $z_i^2 - n$ factors is B-smooth, write $z_i^2 \equiv \prod_{j=1}^{\ell} p_j^{\alpha_{i,j}} \pmod{n}$, where each $p_j \in \mathcal{B}$, the number of primes in the factor base is ℓ, and $\alpha_{i,j} \in \mathbb{Z}$.

   The technique used to find such a sequence of z_i is by way of a sieve, which will be discussed later.

2. Linear Algebra

   Write the exponents of each z_i as vectors, $v_i = (\alpha_{i,1}, \ldots, \alpha_{i.\ell})$, where the j-th component corresponds the j-th prime in $\mathcal{B}$, and take each vector modulo 2. That is to say, make an exponent vector for each z_i and then take each coordinate modulo 2. Find a linear dependency in these vectors and form a set I of the indices of these linearly dependent vectors.

3. Construct x and y such that $x^2 \equiv y^2 \pmod{n}$

   Let $x = \prod_{i \in I} z_i \pmod{n}$ and let $y = \prod_{j=1}^{\ell} p_j^{1/2 \sum_{i \in I} \alpha_{i,j}} \pmod{n}$. Note that $x^2 \equiv y^2 \pmod{n}$ and that y is B-smooth.

4. GCD

   Compute $\gcd(x - y, n)$. If n is a product of k distinct prime factors, the probability that $\gcd(x - y, n)$ results in a factor of n is one minus the probability that the GCD is ± 1:

$$1 - 2/2^k = \left(2^{k-1} - 1\right)/2^{k-1}.$$

If x is near a multiple of $\sqrt{n}$, then x^2 will be small modulo n, and is more likely to be B-smooth [7]. Therefore, we can use a variation of the Sieve of Eratosthenes to sieve the sequence of x^2 for x in an interval near $\sqrt{n}$ [14]. If, instead of crossing the numbers off, as usual in the Sieve of Eratosthenes, one divides x^2 by each prime in $\mathcal{B}$ and its powers, then all B-smooth numbers in the interval are reduced to 1. Sieving is very quick, so this is an efficient method of producing B-smooth numbers.

Let $Q(z) = (z + \lfloor \sqrt{n} \rfloor)^2 - n$. Sieving $Q(z)$ for smooth values relies on the fact that for a prime p with $p | Q(z_0)$, we also have $p | Q(z_0 + kp)$ for all integers k. Finding z_0 simply requires solving the congruence $Q(z) = (z + \lfloor \sqrt{n} \rfloor)^2 - n \equiv 0 \pmod{p}$, or equivalently $(z + \lfloor \sqrt{n} \rfloor)^2 \equiv n \pmod{p}$. Note that solving this congruence requires $\left(\frac{n}{p}\right) = 1$, where $\left(\frac{n}{p}\right)$ is the Legendre Symbol. Therefore, we make the adjustment to the above procedure that all primes p in the factor base $\mathcal{B}$ must have $\left(\frac{n}{p}\right) = 1$.

We see that $Q(z)$ is a square modulo n for every value of z. We are actually looking for a sequence $\{z_i\}_{i \in I}$ such that $\prod_{i \in I} Q(z_i)$ is a square. In other words, we want a sequence $\{z_i\}_{i \in I}$ such that $y^2 = \prod_{i \in I} Q(z_i)$ for some y. Then, we let $x = \prod_{i \in I} (z_i + \lfloor \sqrt{n} \rfloor)$ and we have found x and y such that $x^2 \equiv y^2 \pmod{n}$. There is a good chance that $x \not\equiv \pm y \pmod{n}$, in which case we can use x and y to factor n.

To further speed up the process, we include -1 in the factor base. If we use an interval *centred* at $z = 0$, instead of just looking at numbers starting there, then we generate many more possible B-smooth numbers [3]. To accommodate this, we label -1 as the "zero-th item" in the factor base and include a "zero-th coordinate" in the exponent vector.

z	$(z+25)^2 - 667$	Factoring	Exponent Vector	Exponent Vector Modulo 2
-7	-343	$-1 \cdot 7^3$	(1,0,0,3,0)	(1,0,0,1,0)
-6	-306	$-1 \cdot 2 \cdot 3^2 \cdot 17$	Not Applicable	Not Applicable
-5	-267	$-1 \cdot 3 \cdot 89$	Not Applicable	Not Applicable
-4	-226	$-1 \cdot 2 \cdot 113$	Not Applicable	Not Applicable
-3	-183	$-1 \cdot 3 \cdot 61$	Not Applicable	Not Applicable
-2	-138	$-1 \cdot 2 \cdot 3 \cdot 23$	Not Applicable	Not Applicable
-1	-91	$-1 \cdot 7 \cdot 13$	(1,0,0,1,1)	(1,0,0,1,1)
0	-42	$-1 \cdot 2 \cdot 3 \cdot 7$	(1,1,1,1,0)	(1,1,1,1,0)
1	9	3^2	(0,0,2,0,0)	(0,0,0,0,0)
2	62	$2 \cdot 31$	Not Applicable	Not Applicable
3	117	$3^2 \cdot 13$	(0,0,2,0,1)	(0,0,0,0,1)
4	174	$2 \cdot 3 \cdot 29$	Not Applicable	Not Applicable
5	233	233	Not Applicable	Not Applicable
6	294	$2 \cdot 3 \cdot 7^2$	(0,1,1,2,0)	(0,1,1,0,0)
7	357	$3 \cdot 7 \cdot 17$	Not Applicable	Not Applicable

Table 2.1: Potential B-Smooth Numbers

2.2 A Nice Example

Let $n = 667$, and let us choose $B = 13$. Then the factor base is $\mathcal{B} = \{-1, 2, 3, 7, 13\}$, since $\left(\frac{n}{5}\right) \neq 1$ and $\left(\frac{n}{11}\right) \neq 1$. According to the procedure above, the first step is to generate relations, or pairs $(z, Q(z))$, where $Q(z) = (z + \lfloor\sqrt{n}\rfloor)^2 - n = (z+25)^2 - 667$. Table 2.1 shows a list of some potential B-smooth numbers. The factorizations listed in the third column of the table are for illumination of the next step. In practice we do not factor these numbers directly; we use a sieve to identify B-smooth numbers. Columns 4 and 5 give the exponent vectors, when applicable. In many cases, there is a prime factor > 13. These values will not be considered. We will return to the sieving process shortly.

Now that we have identified our B-smooth numbers, we can go to the Linear Algebra step. For each value z_i, we find exponents $\alpha_{i,0}, \cdots, \alpha_{i,4}$ such that $(z_i+25)^2 - 667 = (-1)^{\alpha_{i,0}} (2)^{\alpha_{i,1}} (3)^{\alpha_{i,2}} (7)^{\alpha_{i,3}} (13)^{\alpha_{i,4}}$. We make each sequence of exponents, $\alpha_{i,0}, \cdots, \alpha_{i,4}$, into a vector where the "zero-th" element corresponds to -1, the first exponent corresponds to 2, etc. These vectors are shown in column 4 of Table 2.1. Taking the list of exponent vectors modulo 2, as shown in column 5 of Table 2.1, we make each vector a column in a matrix and we get the following matrix:

$$A = \begin{array}{c} \\ p{=}{-1} \\ 2 \\ 3 \\ 7 \\ 13 \end{array} \begin{array}{c} \begin{array}{cccccc} z{=}{-7} & -1 & 0 & 1 & 3 & 6 \end{array} \\ \left[\begin{array}{cccccc} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{array}\right] \end{array}.$$

Note that the columns of A correspond to the exponent vectors listed in Table 2.1, column 5. The column labels on the top are actually the corresponding z value and the row labels along the left are the corresponding element of the factor base $\mathcal{B}$. We include both for easy referencing. One particular solution to $Aw = 0$ is $w = (0, 1, 1, 1, 1, 1)^T$. If we look at $\vec{w} = (0, 1, 1, 1, 1, 1)^T$, the non-zero entries correspond to exponent vectors which are linearly dependent; in this case, the corresponding z values are $z = -1$, 0, 1, 3, and 6. We will to use these B-smooth numbers to try to factor n.

Our goal now is to construct x and y such that $x^2 \equiv y^2 \pmod{n}$ and $x \not\equiv \pm y \pmod{n}$. From the Linear Algebra stage, our z values of interest are $z_2 = -1$, $z_3 = 0$, $z_4 = 1$, $z_5 = 3$, and $z_6 = 6$, so we make our index set $I = \{2, 3, 4, 5, 6\}$. Let $x = \prod_{i \in I} (z_i + 25)$ and let $y = \prod_{j=1}^{\ell} p_j^{1/2 \sum_{i \in I} \alpha_{i,j}}$. Then

$$\begin{aligned} x(z) &= 24 \cdot 25 \cdot 26 \cdot 28 \cdot 31 \\ &\equiv 33 \pmod{667}, \text{ and} \end{aligned}$$

$$\begin{aligned} y(z) &= 2^{2/2} \cdot 3^{6/2} \cdot 7^{4/2} \cdot 13^{2/2} \\ &= 2^1 \cdot 3^3 \cdot 7^2 \cdot 13^1 \\ &\equiv 381 \pmod{667}. \end{aligned}$$

Note that to calculate y, we simply add up the exponent vectors in Table 2.1, column 4 that correspond to our z_i for $i \in I$, and raise each prime in $\mathcal{B}$ to its corresponding exponent vector. After this, we take the square root. In practice, we make a slight alteration to speed this process up. The exponents $\sum_{i \in I} \alpha_{i,j}$ are always even by construction. In particular, the exponent on -1 is even, and hence we may drop this term when constructing y. Therefore, we can add up the original exponent vectors, divide each element by 2, and then raise each prime to its corresponding vector component.

We find that $x^2 \equiv y^2 \equiv 422 \pmod{667}$ and $33 \equiv x \not\equiv \pm y \equiv \pm 381 \pmod{667}$.

Our last step is the GCD stage. Taking the greatest common divisor gives $\gcd(x - y, n) = \gcd(33 - 381, 667) = 23$. Finally, $667/23 = 29$ and we have completely factored $667 = 23 \cdot 29$.

2.2.1 Hensel Lifting

Now, let us go back and look at sieving the sequence $(z+25)^2 - 667$ in more detail. Looking back at Table 2.1, we can see that -1 divides $(z+25)^2 - 667$ for $z \leq 0$. Therefore, if $z \leq 0$, we divide $(z+25)^2 - 667$ by -1. We start the sieving process by performing modular arithmetic with the primes in the factor base. Then we sieve with the prime powers via *Hensel Lifting*.

We will begin with 2, as it is the first prime in our factor base. First, we expand $Q(z) = (z+25)^2 - 667 = x^2 + 50x - 42$, and then simplify modulo 2.

$$\begin{aligned} Q(z) &\equiv 0 \pmod 2 \\ (z+25)^2 - 667 &\equiv 0 \pmod 2 \\ z^2 + 50z - 42 &\equiv 0 \pmod 2 \\ z^2 &\equiv 0 \pmod 2. \end{aligned}$$

From this, we get a polynomial f such that $f(z) \equiv 0 \pmod 2$. In this case, $f(z) = z^2$ and its only root modulo 2 is 0. Then $(z+25)^2 - 667$ is divisible by 2 only when $z \equiv 0 \pmod 2$. We are not able to lift this to higher powers of 2 because $f'(0) \equiv 0 \pmod 2$ [6].

Next, we do the same thing with 3:

$$\begin{aligned} z^2 + 50z - 42 &\equiv 0 \pmod 3 \\ z^2 + 2z &\equiv 0 \pmod 3 \\ z(z+2) &\equiv 0 \pmod 3. \end{aligned}$$

Then $(z+25)^2 - 667$ is divisible by 3 when $z \equiv 0$ or $1 \pmod 3$. Now, $f(z) = z(z+2)$, so the roots are 0 and 1 and $f'(z) = 2z + 2$. Since $f'(0) = 2 \not\equiv 0 \pmod 3$ and $f'(1) \equiv 1 \not\equiv 0 \pmod 3$, we can lift both solutions to solutions modulo 9 [6].

To lift our solution modulo 9, let $z_1 = 0 + 3k_1$ and $w_1 = 1 + 3\ell_1$ (hence, z_1 and w_1 are our solutions modulo 9). We will attempt to solve for integers k_1 and ℓ_1 by substituting z_1 and w_1 into our polynomial $z^2 + 50z - 42 \equiv 0 \pmod 9$. This gives:

$$\begin{aligned} (0+3k_1)^2 + 50(0+3k_1) - 42 &\equiv 0 \pmod 9 \\ 6k_1 - 6 &\equiv 0 \pmod 9 \\ k_1 &= 1 \end{aligned}$$

$$\begin{aligned} (1+3\ell_1)^2 + 50(1+3\ell_1) - 42 &\equiv 0 \pmod 9 \\ 12\ell_1 &\equiv 0 \pmod 9 \\ \ell_1 &= 0. \end{aligned}$$

Therefore, if $z \equiv 0$ or $1 \pmod 3$, then $3|Q(z)$ and if $z \equiv 3$ or $1 \pmod 9$, then $9|Q(z)$. The roots are equivalent to $z = 3 + 9k_2 \pmod{27}$ and $z = 1 + 9\ell_2 \pmod{27}$ and we can repeat the process.

$$\begin{aligned} (3+9k_2)^2 + 50(3+9k_2) - 42 &\equiv 0 \pmod{27} \\ 18k_2 - 18 &\equiv 0 \pmod{27} \\ k_2 &= 1 \end{aligned}$$

$$\begin{aligned} (1+9\ell_2)^2 + 50(1+9\ell_2) - 42 &\equiv 0 \pmod{27} \\ 9\ell_2 + 9 &\equiv 0 \pmod{27} \\ \ell_2 &= -1. \end{aligned}$$

We find that $27|Q(z)$ when $z \equiv 12$ or $19 \pmod{27}$, but our interval is too small to allow this so we will only sieve our sequence with 3 and 3^2, and we stop lifting.

We interpret the Hensel Lifting as follows:

- If $z \equiv 12$ or $19 \pmod{27}$, then 27 divides $(z+25)^2 - 667$.
- If $z \not\equiv 12$ or $19 \pmod{27}$, but we have that $z \equiv 1$ or $3 \pmod 9$, then 9 is the highest power of 3 that divides $(z+25)^2 - 667$.
- If $z \not\equiv 12$ or $19 \pmod{27}$ and $z \not\equiv 1$ or $3 \pmod 9$, but $z \equiv 0$ or $1 \pmod 3$, then 3 is highest power of 3 that divides $(z+25)^2 - 667$.

When sieving, we divide $(z+25)^2 - 667$ by the highest power of 3 that we are able to.

Similarly, we find that $7|Q(z)$ when $z \equiv 0$ or $6 \pmod 7$, $49|Q(z)$ when $z \equiv 6$ or $4 \pmod{49}$, and $343|Q(z)$ when $z \equiv 300$ or $336 \pmod{343}$. Looking at powers of 13, we find that $13|Q(z)$ for $z \equiv 12$ or $3 \pmod{13}$ and we cannot lift any higher.

We are now ready to sieve our sequence. Tables 2.2 - 2.5 show the process of sieving. First, we sieve by -1. Recall that earlier we found that $(z+25)^2 - 667 < 0$ when $z \leq 0$, so we divide these values by -1. Next, Table 2.2 shows the process of sieving $Q(z)$ by powers of 2 after factors of -1 have been divided out. We use the results in column 4 to sieve by powers of 3 in Table 2.3. Table 2.4 shows sieving the results of Table 2.3 being sieved by powers of 7. Finally, Table 2.5 shows sieving the results of sieving Table 2.4 by 13. Throughout this process we see that by the time we sieve by a prime $p \in \mathcal{B}$, we have already sieved by all elements $q \in \mathcal{B}$ with $q < p$.

z	$z \pmod 2$	Before Sieving by 2	After Sieving
-7	1	343	343
-6	0	306	153
-5	1	267	267
-4	0	226	113
-3	1	183	183
-2	0	138	69
-1	1	91	91
0	0	42	21
1	1	9	9
2	0	62	31
3	1	117	117
4	0	174	87
5	1	223	223
6	0	294	147
7	1	357	357

Table 2.2: Sieving by 2.

z	$z \pmod 3$	$z \pmod 9$	$z \pmod{27}$	Before Sieving by 3	After Sieving
-7	2	2	20	343	343
-6	0	3	21	153	17
-5	1	4	22	267	89
-4	2	5	23	113	113
-3	0	6	24	183	61
-2	1	7	25	69	23
-1	2	8	26	91	91
0	0	0	0	21	7
1	1	1	1	9	1
2	2	2	2	31	31
3	0	3	3	117	13
4	1	4	4	87	29
5	2	5	5	223	223
6	0	6	6	147	49
7	1	7	7	357	119

Table 2.3: Sieving by powers of 3.

z	$z \pmod 7$	$z \pmod{49}$	$z \pmod{343}$	Before Sieving by 7	After Sieving
-7	0	42	336	343	1
-6	1	43	337	17	17
-5	2	44	338	89	89
-4	3	45	339	113	113
-3	4	46	340	61	61
-2	5	47	341	69	23
-1	6	48	342	91	13
0	0	0	0	7	1
1	1	1	1	1	1
2	2	2	2	31	31
3	3	3	3	13	13
4	4	4	4	29	29
5	5	5	5	223	223
6	6	6	6	49	1
7	0	7	7	119	17

Table 2.4: Sieving by powers of 7.

z	$z \pmod{13}$	Before Sieving by 13	After Sieving
-7	6	1	1
-6	7	17	17
-5	8	89	89
-4	9	113	113
-3	10	61	61
-2	11	23	23
-1	12	13	1
0	0	1	1
1	1	1	1
2	2	31	31
3	3	13	1
4	4	29	29
5	5	223	223
6	6	1	1
7	7	17	17

Table 2.5: Sieving by 13.

At the end of the sieving process, we find that the B-smooth values have indeed been reduced to 1, and we can easily identify B-smooth numbers.

The entire sieving process is summarized Table 2.6. The elements of our factor base and their prime powers are listed in the first column. The first row is values of z and the second row is values of $Q(z)$. A dash indicates when $Q(z)$ is not divisible by the corresponding element listed in the first column. Therefore, a dash signals that the value of $Q(z)$ remains unchanged. If $Q(z)$ is divisible by the corresponding number in the first column, then we divide that number out and continue sieving with the number in brackets. For example, working our way down the column corresponding to $z = 7$, we find that 357 is not divisible by -1 or 2. It is divisible by 3, so we divide 3 out and use 119 to sieve further. At the end, we scan each column and if a 1 appears in the brackets, then we know the corresponding $Q(z)$ values is smooth.

2.3 Summary

Factoring $n = 667 = 23 \cdot 29$ was a lot of work, so let's go over what we did. We chose an integer B which was smaller than the recommended value. Then, we built our factor base consisting of -1 and all prime number $\leq B$ with $\left(\frac{n}{p}\right) = 1$. We let $Q(z) = (z + \lfloor\sqrt{n}\rfloor)^{1/2} - n$ and we used Hensel Lifting to identify B-smooth numbers and create our exponent vectors. Then, we found a linear dependency among all of our exponent vectors. We multiplied all of the quadratic residues, $(z + \lfloor\sqrt{n}\rfloor)$, from this linear dependence together modulo n to create x and used the original exponent vectors to create y. This gave us x and y such that

$$x^2 \equiv \prod_{i \in I}(z_i + \lfloor\sqrt{n}\rfloor)^2 \pmod{n} \text{ and } y^2 \equiv \prod_{i \in I} Q(z_i) \pmod{n},$$

where $x^2 \equiv y^2 \pmod{n}$. Finally, we took $\gcd(x - y, n)$ as our factor of n.

	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7
	-343	-306	-267	-226	-183	-138	-91	-42	9	62	117	174	223	294	357
-1	$-1 \cdot 343$	-1(306)	-1(267)	-1(226)	-1(183)	-1(138)	-1(91)	-1(42)	–	–	–	–	–	–	–
2	–	2(153)	–	2(113)	–	2(69)	–	2(21)	–	2(31)	–	2(87)	–	2(147)	–
3	–	–	3(89)	–	3(61)	3(23)	–	3(7)	–	–	–	3(29)	–	3(49)	3(119)
9	–	9(17)	–	–	–	–	–	–	9(1)	–	9(13)	–	–	–	–
7	–	–	–	–	–	–	7(13)	7(1)	–	–	–	–	–	–	7(17)
49	–	–	–	–	–	–	–	–	–	–	–	–	–	49(1)	–
343	343(1)	–	–	–	–	–	–	–	–	–	–	–	–	–	–
13	–	–	–	–	–	–	13(1)	–	–	–	13(1)	–	–	–	–

Table 2.6: Sieving

Chapter 3

Extending to Multiple Polynomials

3.1 The Algorithm

Using the polynomial $Q(z) = (z - \lfloor\sqrt{n}\rfloor)^2 - n$ to generate B-smooth numbers gives us the desired result. However, as z moves away from 0, the values $Q(z)$ grow quickly as z grows [3]. The larger z gets, the less likely $Q(z)$ is to have only small prime factors. This can be troublesome if many B-smooth numbers are needed. To get around this problem, Davis and Holdrige [4] and Montgomery, via a personal correspondence, see Pomerance [13], extended the quadratic sieve to use multiple polynomials to generate B-smooth numbers.

Ideally, we want to find other polynomials $P(z)$ that have the same properties as $Q(z)$. Recall that $Q(z) = (z - \lfloor\sqrt{n}\rfloor)^2 - n$. The first important property of $Q(z)$ is that the right-hand side is a square modulo n. We would like the right-hand side of $P(z)$ to also be a square modulo n. Furthermore, by sieving for B-smooth values of $Q(z)$, we can find some values of $Q(z)$ that multiply together to produce a square. We want to be able to do the same with $P(z)$ and sieve for B-smooth values.

The following is adapted from Crandall and Pomerance [3].

Let a, b, and c be integers with $b^2 - ac = n$ and let $f(z) = az^2 + 2bz + c$. Then

$$\begin{aligned} af(z) &= a^2z^2 + 2abz + ac \\ &= (az + b)^2 - \left(b^2 - ac\right) \\ &= (az + b)^2 - n \\ &\equiv (az + b)^2 \pmod{n}. \end{aligned}$$

Taking $P(z) = af(z)$ gives us that the right-hand side of $P(z)$ is a square modulo n. If we choose a to be a square times a B-smooth number and z such that $f(z)$ is B-smooth,

then we can find a sequence $\{z_i\}_{i\in J}$ such that $\prod_{i\in J} P(z_i)$ is a square. Then we can let $y^2 = \prod_{i\in J} P(z_i)$ and $x = \prod_{i\in J} (az_i + b)$ and we will have $x^2 \equiv y^2 \pmod{n}$. We check that $x \not\equiv \pm y \pmod{n}$ and carry on as before.

The point of this is to keep values of $P(z)$ small so they're more likely to be B-smooth. If we look at $P(z)$ on the interval $[-n, n]$, we see that $P(z) = (az + b)^2 - n$ is a parabola. We want to minimize the parabola on our interval to keep the values as small as possible. Moreover, it would be nice to bound the parabola on the interval so that we can be assured of having small values of $P(z)$.

We are not going to look at the whole interval $[-n, n]$; it is too large. Instead, we will look at values of z on some sub-interval, say $[-M, M]$ for $M < n$, and we want to minimize and bound $P(z)$ on this interval. Since a is positive, our parabola opens upwards on $[-n, n]$, with the minimum occuring at $z = -b/a$. If we take $|b| \leq \frac{1}{2}a$, then $-n \leq (az + b)^2 - n \leq \left(az + \frac{1}{2}a\right)^2 - n = a^2\left(z + \frac{1}{2}\right)^2 - n$, and we have bounded our parabola.

Since $-n \leq P(z) \leq a^2\left(z + \frac{1}{2}\right)^2 - n$ for $z \in [-M, M]$ and $f(z) = P(z)/a$, we can bound $f(z)$: we have $-n/a \leq f(z) \leq a(M + \frac{1}{2})^2 - n/a$ with the maximum of $f(z)$ occuring at $z = M$. Since a is a fixed value, it suffices to minimize $f(z)$ when trying to minimize $P(z)$. Furthermore, it will be easier to minimize $f(z)$ now that we have bounded it. We set the absolute values of the bounds to be approximately equal, $n/a \approx |a(M + \frac{1}{2})^2 - n/a|$. We find that we require $a \approx \sqrt{2n}/M$ for $f(z)$ to be bounded by $\left(M\sqrt{n}\right)/\sqrt{2}$.

The easiest choice of a is p^2 for some $p \approx \sqrt{2n}/M$. However, if we look at $af(z) = (az + b)^2 - n$ and take it modulo p, we have $0 \equiv (az + b)^2 - n \pmod{p}$, or $n \equiv (az + b)^2 \pmod{p}$. Therefore, we require $\left(\frac{n}{p}\right) = 1$ for our choice of p.

After we have our M and our a, we can get our b. Using the equation $b^2 - ac = n$, we can solve the congruence $b^2 \equiv n \pmod{a}$. There are two solutions for b, so we take the one with $|b| \leq \frac{1}{2}a$. Then we can solve $c = \left(b^2 - n\right)/a$ to obtain all three coefficients of our polynomial $f(z)$.

To summarize, we have the following procedure:

1. Construct $f(z)$

   Choose an integer M such that $[-M, M]$ is the interval to be sieved and find a prime $p \approx \sqrt{2n}/M$ with $\left(\frac{n}{p}\right) = 1$. Take $a = p^2$ and solve $b^2 \equiv n \pmod{a}$ for $|b| \leq \frac{1}{2}a$. Then let $c = \left(b^2 - n\right)/a$. The polynomial is $f(z) = az^2 + bz + c$.

2. Generate B-Smooth Numbers

   Find a sequence of integers z_i such that $f(z_i) = az_i^2 + bz_i + c$ is is B-smooth. Disregard any pairs $(z_i,\ f(z_i))$ where $f(z_i)$ does not factor over $\mathcal{B}$ and write $f(z_i) \equiv \prod_{j=1}^{\ell} p_j^{\beta_{i,j}} \pmod{n}$, where each $p_j \in \mathcal{B}$, the number of primes in the factor base is ℓ, and $\alpha_{i,j} \in \mathbb{Z}$.

3. Linear Algebra

   Write the exponents of each z_i as vectors, $v_i = (\beta_{1,i}, \ldots, \beta_{\ell,i})$, where the j-th component corresponds the j-th prime in $\mathcal{B}$, and take each vector modulo 2. Make each vector a column in a matrix and append this matrix onto A, the matrix from the basic Quadratic Sieve. Find a linear dependency in all the vectors and form index sets I and J, where I holds all the indices of the linearly dependent vectors which correspond to the polynomial $Q(z)$, and J holds all the indices of the linearly dependent vectors corresponding to the polynomial $f(z)$.

4. Construct x and y such that $x^2 \equiv y^2 \pmod{n}$

   Let

$$x = \left(\prod_{i\in I} (z_i + \lfloor\sqrt{n}\rfloor)\right)\left(\prod_{i\in J} (az_i + b)\right) \pmod{n} \text{ and}$$
$$y = \left(p^{\sum_{i\in J} i}\right)\left(\prod_{j=1}^{\ell} p_j^{1/2(\sum_{i\in I}\alpha_{i,j} + \sum_{i\in J}\beta_{i,j})}\right) \pmod{n}.$$

   Note that x^2 is a new square that factors over $\mathcal{B}$.

5. GCD

   Compute $\gcd(x - y, n)$.

3.2 Example

Let us pretend that we were unlucky in our factoring of $n = 667$ and try to generate more B-smooth numbers. If we let $M = 2$, then we can take $p = 17 \approx \sqrt{2 \cdot 667}/2$ and $a = 289$. Then $b^2 \equiv 667 \equiv 89 \pmod{289}$, so $b \equiv \pm 49 \pmod{289}$ and we can take $b = 49$. Let $c = (49^2 - 667)/289 = 6$. Our polynomial is $f(z) = 289z^2 + 49z + 6$ and $P(z) = af(z) \equiv (289z + 49)^2 - 667 = 146z^2 + 154z - 267$. We obtain the potential B-smooth numbers listed in Table 3.1. Of these, we obtain the smooth number in Table 3.2. Notice that we did not include the potential B-smooth number corresponding to $z = 2$ since our original factor base does not include the prime number 5.

z	$f(z)$	Factoring
-2	1064	$2^3 \cdot 7 \cdot 19$
-1	246	$2 \cdot 3 \cdot 41$
0	6	$2 \cdot 3$
1	344	$2^3 \cdot 43$
2	1260	$2^2 \cdot 3^2 \cdot 5 \cdot 7$

Table 3.1: Potential B-Smooth Numbers

z	$af\,(z) \pmod n$	Factoring	Exponent Vector	Exponent Vector Modulo 2
0	6	$2 \cdot 3$	(0,1,1,0,0)	(0,1,1,0,0)

Table 3.2: Smooth Numbers

We can add this vector to our matrix A and obtain the matrix:

$$C = \begin{array}{c} \\ p{=}{-1} \\ 2 \\ 3 \\ 7 \\ 13 \end{array} \begin{array}{c} \begin{array}{cccccccc} Q(z)\text{: } z{=}{-7} & -1 & 0 & 1 & 3 & 6 & f(z)\text{: } z{=}0 \end{array} \\ \left[\begin{array}{cccccccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{array}\right] \end{array}$$

Note that the column indices reference the corresponding z value and the row indices reference the corresponding element in $\mathcal{B}$. The first six columns are from our matrix A, which correspond to our original z values of $z_1 = -7$, $z_2 = -1$, $z_3 = 0$, $z_4 = 1$, $z_5 = 3$, & $z_6 = 6$, and the polynomial $Q(z)$, and the last column of C corresponds to our new B-smooth number from the polynomial $f(z)$, which has $z_7 = 0$. To find a linear dependency, we solve $Cw = 0$. One solution is $\vec{w} = (0, 0, 0, 0, 0, 1, 1)^T$. The non-zero entries correspond to $z_6 = 6$ from our old polynomial $Q(z)$, and $z_7 = 0$ from our new polynomial, $f(z)$. This gives two new index sets, $I = \{6\}$ from the polynomial $Q(z)$ and $J = \{7\}$ from the polynomial $f(z)$. We will try and use these B-smooth numbers to factor n.

Let

$$\begin{aligned} x &= \prod_{i \in I}(z_i + \lfloor\sqrt{n}\rfloor) \prod_{j \in J}(az_j + b) \\ &= \prod_{i \in I}(z_i + 25) \prod_{j \in J}(289z_j + 49) \\ &= 31 \cdot 49 \\ &\equiv 185 \pmod{667} \end{aligned}$$

$$\begin{aligned} y &= a^{1/2} \cdot 2^{\alpha_{i,1}/2} \cdot 3^{\alpha_{i,2}/2} \cdot 7^{\alpha_{i,3}/2} \cdot 13^{\alpha_{i,4}/2} \\ &= 17^{2/2} \cdot 2^{2/2} \cdot 3^{2/2} \cdot 7^{2/2} \cdot 13^{0/2} \\ &= 17 \cdot 2 \cdot 3 \cdot 7 \\ &\equiv 47 \pmod{667}. \end{aligned}$$

Then $x^2 = y^2 \equiv 52 \pmod{667}$ but $x \not\equiv \pm y \pmod{667}$. Then $\gcd(185 - 47, 667) = \gcd(138, 667) = 23$, and we have split n.

3.3 Summary

Using all of the work we did in the basic Quadratic Sieve (except the actual factors of n), we chose a new interval we wanted to sieve, $[-M, M]$. We let $p \approx \sqrt{2n}/M$ be a prime with $(\frac{n}{p}) = 1$, and let $a = p^2$. Solving $b^2 \equiv n \pmod{a}$ for $|b| \leq \frac{1}{2}a$ and letting $c = (b^2 - n)/a$, we constructed the polynomial $f(z) = az^2 + bz + c$. Then, we sieved our interval $[-M, M]$ for values of $f(z)$ that were B-smooth and created our new exponent vectors. After adding the new exponent vectors to our matrix A, we had a new linear dependency in our new matrix. We multiplied all the roots of our quadratic residues, $(z + \lfloor\sqrt{n}\rfloor)$ and $(az + b)$, from our linear dependence together modulo n to form x, and used the original exponent vectors to create y. Finally, we had that $\gcd(x - y, n)$ was a proper divisor of n.

Chapter 4

The Number Field Sieve

4.1 The Algorithm

Currently, the Number Field Sieve is the fastest factoring algorithm available for integers over 130 digits, while the Quadratic Sieve works well for integers with fewer than 100 digits [13]. This is due to the fact that the Quadratic Sieve algorithm is conjectured to have a complexity of $L(n) = \exp((1+o(1))\sqrt{\ln n \ln\ln n})$ where as the Number Field Sieve is conjectured to have a complexity of $\exp\left(((64/9)^{1/3}+o(1))(\ln n)^{1/3}(\ln\ln n)^{2/3}\right)$ [3]. Even with the alterations to speed up the basic Quadratic Sieve, the Number Field Sieve is faster in the worst-case.

The following is adapted from Crandall and Pomerance [3].

In the Quadratic Sieve, we noticed that the right-hand side of $Q(z) = (z - \lfloor\sqrt{n}\rfloor)^2 - n$ is always a square modulo n. More specifically, it is a small quadratic residue modulo n when we have a sequence centred at $\lfloor\sqrt{n}\rfloor$, and we can use Hensel Lifting to quickly identify smooth values on the left-hand side. The Number Field Sieve uses this general idea, but instead of using small quadratic residues, we will simply use small numbers and perform the linear algebra stage with each side of the congruence.

Let m be an integer, σ be an algebraic number, and ϕ be a homomorphism such that $\phi : \mathbb{Z}[\sigma] \to \mathbb{Z}_n$ with $\phi(\sum_{i=1}^{d-1} a_i\sigma^i) = \sum_{i=1}^{d-1} a_i m^i \pmod{n}$ for any integers a_i and a positive integer d. We will show how to construct m, σ, and ϕ later.

We are searching for a set $\mathcal{S} \subseteq \{(a,b) \in \mathbb{Z}\times\mathbb{Z} | \gcd(a,b) = 1\}$ such that

$$\begin{aligned} \gamma^2 &= \prod_{(a,b)\in\mathcal{S}} (a - b\sigma), \text{ for some } \gamma \in \mathbb{Z}[\sigma] \text{ and} \\ x^2 &= \prod_{(a,b)\in\mathcal{S}} (a - bm), \text{ for some } x \in \mathbb{Z}_n. \end{aligned}$$

Then we will have

$$x^2 \equiv \textstyle\prod_{\mathcal{S}}(a - bm) \equiv \prod_{\mathcal{S}} \phi(a - b\sigma) \equiv \phi(\prod_{\mathcal{S}}(a - b\sigma)) \equiv \phi(\gamma^2) \equiv \phi(\gamma)^2 \equiv y^2 \pmod{n},$$

and we can try and factor n by taking the $\gcd(x - y, n)$.

We start by generating an irreducible polynomial. First, we choose a small integer d, usually $d \approx \left(\frac{3 \ln n}{\ln \ln n}\right)^{1/3}$, and let $m = \lfloor n^{1/d} \rfloor$. Then we write n as follows:

$$n = m^d + c_{d-1}m^{d-1} + \cdots + c_0$$

with $c_i \in [0, m - 1]$. We have just generated a polynomial $f(z) = z^d + c_{d-1}z^{d-1} + \cdots + c_0$ that has the property that $f(m) \equiv 0 \pmod{n}$. We can already see that f is monic. If f is not irreducible, then $f(z) = g(z)h(z)$ for some non-trivial polynomials g, $h \in \mathbb{Z}[z]$ and $n = f(m) = g(m)h(m)$. Thus, if f is not irreducible, we can find a non-trivial factorization of n. If f is irreducible, then we proceed with the Number Field Sieve.

Let σ be some root of f. Then, $\mathbb{Z}[\sigma]$ is equivalent to the ring $\mathbb{Z}[z]/(f(z))$, which is indeed a ring since f is irreducible. Elements of the ring are of the form $a_0 + a_1\sigma + \cdots + a_{d-1}\sigma^{d-1}$ where $a_0, \ldots, a_{d-1} \in \mathbb{Z}$. Then, our homomorphism is $\phi : \mathbb{Z}[\sigma] \to \mathbb{Z}_n$ which sends an element $a_0 + a_1\sigma + \cdots + a_{d-1}\sigma^{d-1}$ to $a_0 + a_1m + \cdots + a_{d-1}m^{d-1}$ in $\mathbb{Z}_n$.

Note that ϕ is indeed a homomorphism. Let $\chi : \mathbb{Z}[z] \to \mathbb{Z}_n$ be a group homomorphism such that any element in $\mathbb{Z}[z]$ gets evaluated at m and reduced modulo n. Now, we know that there is a natural, surjective homomorphism ψ where $\psi : \mathbb{Z}[z] \to \mathbb{Z}[z]/(f(z))$. Since $f(m) = n \equiv 0 \pmod{n}$, we have that $(f(z))$ is in $ker(\chi)$. Then, the Fundamental Theorem of Homomorphisms tells us that there exists a unique homomorphism $\phi : \mathbb{Z}[z]/(f(z)) \to \mathbb{Z}_n$ such that $\chi = \phi \cdot \psi$ [5].

Looking back at our polynomial f, we want to put it in a more useful form, the reason for which is explained in the next section. We do the following:

$$\begin{aligned} f(z) &= (z - \sigma_1) \cdots (z - \sigma_d) \\ f(a/b) &= (a/b - \sigma_1) \cdots (a/b - \sigma_d) \\ &= b^{-d}(a - b\sigma_1) \cdots (a - b\sigma_d). \end{aligned}$$

Let $F(a,b) = b^d f(a/b) = (a - b\sigma_1)\cdots(a - b\sigma_d)$ and let $G(a,b) = a - bm$. This gives us two new polynomials of two variables, a and b.

What we really want, is to find a set $\mathcal{S}$ of co-prime pairs (a,b) such that:

1. $\prod_{(a,b)\in\mathcal{S}} G(a,b)$ is a square in $\mathbb{Z}_n$,
2. $\prod_{(a,b)\in\mathcal{S}} F(a,b)$ is a square in $\mathbb{Z}$,
3. $\prod_{(a,b)\in\mathcal{S}}(a - b\sigma)$ is a square in $\mathbb{Z}[\sigma]$.

Note that $x^2 \equiv \prod_{(a,b)\in\mathcal{S}} G(a,b) \pmod{n}$ and $\gamma^2 = \prod_{(a,b)\in\mathcal{S}}(a - b\sigma)$. We further require that $\prod_{(a,b)\in\mathcal{S}} F(a,b)$ is a square in $\mathbb{Z}$; otherwise, $\prod_{(a,b)\in\mathcal{S}}(a - b\sigma)$ would not be square in $\mathbb{Z}[\sigma]$. This will be explained in the next section.

In the Quadratic Sieve method, we used the notion of smooth values to find potential relations (a,b). We will use the same idea here. We require that all of $G(a,b)$, $F(a,b)$, and $(a - b\sigma)$ are B-smooth. As we'll see in the next section, $(a - b\sigma)$ is B-smooth if $F(a,b)$ is B-smooth. Therefore, it suffices to sieve $F(a,b)$ and $G(a,b)$ for smooth values.

Although we only need to sieve $F(a,b)$ and $G(a,b)$ for B-smooth values, we still require that all three products are squares. Therefore, it makes sense to have three separate parts to the exponent vector for (a,b) that we are making. We will make three "mini"-exponent vectors, relating to each of $G(a,b)$, $F(a,b)$, and $(a - b\sigma)$, and then concatenate them together before finding our linear dependency modulo 2 in the Linear Algebra stage. This will ensure that all three products will be squares simultaneously.

Leaving off some of the details for right now, the general idea of the Number Field Sieve can be summarized by the following procedure:

1. Generate Relations

   Let $B \approx \exp(8/9)^{1/3}\ln n)^{1/3}(\ln\ln n)^{2/3}$ be an integer and let
   $\mathcal{B} = \{p_j : p_j \text{ prime}, p_j \le B\}$, where we have indexed the primes with p_j being the j^{th} prime starting from 2. Include $-1 \in \mathcal{B}$ as the "zero-th" element. This $\mathcal{B}$ is our factor base. Note that like in the Quadratic Sieve, a smaller value of B usually works.

   Choose a small, positive integer $d \approx \left(\frac{3\ln n}{\ln\ln n}\right)^{1/3}$ and let $m = \lfloor n^{1/d} \rfloor$. Write $n = m^d + c_{d-1}m^{d-1} + \cdots + c_0$, where $c_j \in [0, m-1]$, and let $f(z) = z^d + c_{d-1}z^{d-1} + \cdots + c_0$. Let $F(a,b) = b^d f(a/b)$ and $G(a,b) = a - bm$. Make $\mathcal{S}'$, a set of co-prime, integer

pairs (a_i, b_i) such that $F(a_i, b_i)$ and $G(a_i, b_i)$ are each products of primes in $\mathcal{B}$. If $F(a_i, b_i)$ or $G(a_i, b_i)$ factors in such a way, we call it *B-smooth* and we call the pairs $(a_i, b_i) \in \mathcal{S}'$ *relations*. Disregard any pairs (a_i, b_i) where both $F(a_i, b_i)$ and $G(a_i, b_i)$ do not factor over $\mathcal{B}$.

2. Linear Algebra

   Make three "mini"-exponent vectors corresponding to $G(a, b)$, $F(a, b)$, and $(a - b\sigma)$. We will call the first mini-vector $\overrightarrow{v}_{G(a,b)} = (\rho_{(a,b),0}, \cdots, \rho_{(a,b),k})$ where there are k primes in $\mathcal{B}$. This is the exponent vector that corresponds to $G(a, b)$. Constructing the exponent vectors corresponding to $F(a, b)$ and $(a - b\sigma)$ will be explained in the next section. Take each vector modulo 2 and concatenate the vectors in order. Find a linear dependency amongst these "mega"-vectors and make a set $\mathcal{S}$ consisting of the corresponding relations (a, b).

3. Construct x and y such that $x^2 \equiv y^2 \pmod{n}$

   Let $x \in \mathbb{Z}$ be such that $x = \prod_{(a,b)\in\mathcal{S}} p_j^{1/2 \sum_{(a,b)\in\mathcal{S}} \rho_{(a,b),j}} \pmod{n}$. Let $\gamma^2 = \prod_{(a,b)\in\mathcal{S}}(a - b\sigma)$, and find γ. Take $y = \phi(\gamma)$ and note that x^2 and y^2 are new square integers that factors over $\mathcal{B}$.

4. GCD

   Compute $\gcd(n, x - y)$.

4.2 The Second "Mini"-Vector

Define a norm function so that if $\beta = s_0 + s_1\sigma + \cdots + s_{d-1}\sigma^{d-1} \in \mathbb{Q}[\sigma]$, then we have $N(\beta) = \prod_{j=1}^{d}(s_0 + s_1\sigma_j + \cdots + s_{d-1}\sigma_j^{d-1})$. Since the expression is symmetric in the roots $\sigma_1, \cdots, \sigma_d$, we see that $N(\beta) \in \mathbb{Q}$. Similarly, if $s_0, \cdots, s_{d-1} \in \mathbb{Z}$, then $N(\beta) \in \mathbb{Z}$.

As a result of the definition of our norm, we have that $N(\beta\beta') = N(\beta)N(\beta')$ for any $\beta \in \mathbb{Z}[\sigma]$. This means that if β is a square, say $\beta = \gamma^2$, then $N(\beta)$ is a square: $N(\beta) = N(\gamma^2) = N(\gamma)^2$. Equivalently, if $N(\beta)$ is not a square then β is not a square. If we turn our attention from β to $a - b\sigma$, we find that in order for the product of $a - b\sigma$ to be a square, we require the product of $N(a - b\sigma)$ to be a square:

$$\begin{aligned} N(a - b\sigma) &= (a - b\sigma_1)\cdots(a - b\sigma_d) \\ &= b^d(a/b - \sigma_1)\cdots(a/b - \sigma_d) \\ &= b^d f(a/b) \\ &= F(a, b), \end{aligned}$$

which is where we get our $F(a,b)$. It follows that if $\prod_{(a,b)} F(a,b)$ is not a square, then $\prod_{(a,b)}(a-b\sigma)$ is not a square. Thus, we require $\prod_{(a,b)} F(a,b)$ to be a square. Furthermore, we call an element $\beta \in \mathbb{Z}[\sigma]$ B-smooth if it's norm $N(\beta)$ is B-smooth.

Although we know that β being a square implies that $N(\beta)$ is also a square, it is not true that $N(\beta)$ being a square implies that β is a square in $\mathbb{Z}[\sigma]$. For example, let $f(z) = z^2+4$ and let f have root σ. Then $N(a+b\sigma) = a^2+b^2$. Similarly, if we take $b=0$, we have $N(a) = a^2$. However, if $a > 0$ is not a square in $\mathbb{Z}$, then we have that a is not a square in $\mathbb{Z}[\sigma]$.

Now that we understand why we need $\prod_{(a,b)\in\mathcal{S}} F(a,b)$ to be a square, we need to make the corresponding exponent vectors so that we can achieve this. We can sieve $G(a,b)$ using modular arithmetic and Hensel Lifting, but we have a slightly different sieve that we use for $F(a,b)$ because we may not have that $\mathbb{Z}[\sigma]$ is a Unique Factorization Domain.

The general idea here is that for each prime, p, in our factor base, we check that $p|a-br$ for some integer, r. If $p \nmid a-br$, then $p \nmid F(a,b)$ and if $p|a-br$, then $p|F(a,b)$. This only works with certain values of r, but that will be explained shortly. Then, for each prime, we consider several different values of r. That way, if we're unlucky and we have that $p \nmid F(a,b)$ but $p \nmid a-br$ for one particular r, we may have that $p|a-br$ for another r and we can sieve with that r. This is possible because a and b are not necessarily co-prime with each p. This gives us the best chance of accurately sieving $F(a,b)$.

We will now explain more about the r values. Let
$R(p) = \{r \in [0,p-1] \,|\, r \in \mathbb{Z}, f(r) \equiv 0 \pmod{p}\}$ where $p \in \mathcal{B}$. Since our integers a, b are co-prime, we have that

$$F(a,b) \equiv 0 \pmod{p} \text{ if and only if } a \equiv br \pmod{p} \text{ for some } r \in R(p).$$

We sieve various relations (a,b) by fixing b and viewing $F(a,b)$ as a polynomial in the variable a, and vice versa for a "double" sieve. While we sieve a particular $F(a,b)$ for prime factors, we can also sieve our residue classes $a \equiv br \pmod{p}$ for multiples of p. We can modify our exponent vectors to keep track of which residue classes are in fact multiples of p.

If $a \not\equiv br \pmod{p}$, then we can set our element $v_{p,r}(F(a,b)) = 0$. Otherwise, if $a \equiv br \pmod{p}$, then we define our exponent $v_{p,r}(F(a,b))$ in the usual way. Thus, for each pair (a,b) and for each pair (p,r), we have a separate coordinate, $v_{p,r}(F(a,b))$, in our exponent vector.

For example, let $n = 667$, $d = 2$, $m = 25$, and $f(z) = z^2+z+17$ and take $B = 19$. Then our factor base is $\mathcal{B} = \{-1,2,3,5,7,11,13,17,19\}$. We first need to make our sets,

$R(p) = \{r \in [0, p-1] \,|\, r \in \mathbb{Z}, f(r) \equiv 0 \pmod{p}\}$, for each prime in our factor base. We can see that $f(0) = 17 \equiv 1 \not\equiv 0 \pmod{2}$ and $f(1) = 19 \equiv 1 \not\equiv 0 \pmod{2}$, so we have $R(2) = \{\}$. Similarly, $R(3) = R(5) = R(7) = R(11) = R(13) = \{\}$. However, $f(0) = 17 \equiv 0 \pmod{17}$ and $f(16) = 289 \equiv 0 \pmod{17}$, but $f(r) \not\equiv 0 \pmod{17}$ for any other $r \in [0, 16]$. Therefore, we have that $R(17) = \{0, 16\}$. Similarly, we have $R(19) = \{1, 17\}$. Our mini-exponent vectors look like

$$(v_{17,0}(F(a,b)), v_{17,16}(F(a,b)), v_{19,1}(F(a,b)), v_{19,17}(F(a,b))).$$

We will make the mini-vectors for $F(-2,1)$, $F(-1,1)$, $F(1,1)$, $F(0,1)$, and $F(17,1)$. In the case of $F(-2,1)$, we have:

$$\begin{aligned}
(p,r) = (17,0): \quad -2 &\not\equiv 0 = 1 \cdot 0 \pmod{17} \\
(17,16): \quad -2 &\not\equiv 16 = 1 \cdot 16 \pmod{17} \\
(19,1): \quad -2 &\not\equiv 1 = 1 \cdot 1 \pmod{19} \\
(19,17): \quad -2 &\equiv 17 = 1 \cdot 17 \pmod{19}.
\end{aligned}$$

From this, we know that $19|F(-2,1)$. The only thing we need to keep in mind is that we still don't know what power of 19 divides $F(-2,1)$.

Similar to building our mini-vector for $G(a,b)$, we want to be able to keep track of prime powers. We have that $a \equiv br \pmod{p}$, so then we know that we also have $a \equiv b(r + pk) \pmod{p^2}$. We can plug this new a into $F(a,b) \equiv 0 \pmod{p^2}$ to solve for k, similar to the Hensel Lifting we did with the Quadratic Sieve. Then, our coordinate is $v_{p,r}(F(a,b))$ if we have that $a \equiv b(r + p^{t-1}k_{t-1}) \pmod{p^t}$, but $a \not\equiv b(r + p^t k_t) \pmod{p^{t+1}}$ for $t = v_{p,r}(F(a,b))$.

Let's try to lift our solution, $a \equiv b \cdot 17 \pmod{19}$, to a higher power of 19. Now that we are working modulo 19^2, our solution looks like $a \equiv b \cdot (17 + 19k) \pmod{361}$. We plug this into $0 \equiv F(a,b) \pmod{19}$ and find:

$$\begin{aligned}
0 &\equiv a^2 + ab + 17b^2 \pmod{361} \\
&\equiv (17b + 19kb)^2 + (17b + 19kb)b + 17b^2 \pmod{361} \\
&\equiv 289b^2 + 285b^2k + 17b^2 + 19b^2k + 17b^2 \pmod{361} \\
&\equiv 323 + 304k \pmod{361} \\
&\equiv 17 + 16k \pmod{361} \\
k &\equiv 202 \pmod{361}.
\end{aligned}$$

We put $k = 202$ back into our equation for a, and we find that $361|F(a,b)$ when $a \equiv b \cdot 245 \pmod{361}$. In the case of $F(-2,1)$, we find that $-2 \not\equiv 245 \pmod{361}$, so we do not have $19^2|F(-2,1)$. Therefore, our coordinate is $v_{19,17}(F(-2,-1)) = 1$ and we have our exponent vector for $F(-2,1)$, which is $(0,0,0,1)$. Note that if we did have $-2 \equiv 245 \pmod{361}$,

then our fourth coordinate would be 2, not 1.

Similarly, we make the exponent vectors for $F(-1,1)$, $F(1,1)$, $F(0,1)$, and $F(17,1)$, which are $(0,1,0,0)$, $(0,0,1,0)$, $(1,0,0,0)$, and $(1,0,0,1)$, respectively. We can see that the vectors corresponding to $F(-2,1)$, $F(0,1)$, and $F(17,1)$ are linearly dependent, so we know that the product of $F(-2,1)$, $F(0,1)$, and $F(17,1)$ should be a square. Indeed, $F(-2,1) = 17$, $F(0,1) = 19$, and $F(17,1) = 17 \cdot 19$, and when we multiply all of these together we find that the result is a square, $17^2 \cdot 19^2$.

To summarize this point, we have our p_j's labelled for primes $\leq B$. For each prime p_j, we have $r_{j,1}, \cdots, r_{j,w_j}$ values in $R(p_j)$. For each pair (p_j, r_{j,w_j}), we can run through our pairs $(a,b) \in \mathcal{S}'$, generally by fixing b and running through various a values. If we find that $a \not\equiv br_{j,w_j} \pmod{p_j}$ then we set our exponent $v_{p_j,r_{j,w_j}}(F(a,b)) = 0$. Otherwise, we find the maximum exponent of p_j which divides $F(a,b)$ and label it $v_{p_j,r_{j,w_j}}(F(a,b))$. Thus, the second mini-exponent vector for the Linear Algebra stage is
$\overrightarrow{v}_{F(a,b)} = (v_{p_1,r_{1,1}}(F(a,b)), \cdots, v_{p_1,r_{1,w_1}}(F(a,b)), \cdots, v_{p_k,r_{k,1}}(F(a,b))$.

Let $\mathcal{I} = \{\sigma \in \mathbb{Q}[\sigma] |\ \sigma \text{ is an algebraic integer}\}$ be an ideal. Then $\mathbb{Z}[\sigma]$ is a subset of $\mathcal{I}$. We will be using the following Theorem (although Crandall and Pomerance [3] present it as a Lemma):

Theorem 1. *Let $\mathcal{S} = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} | a - b\sigma$ is $B-$smooth$\}$ and let $\mathcal{I} = \{\sigma \in \mathbb{Q}[\sigma] | \sigma$ is an algebraic integer$\}$. If $\prod_{(a,b)\in\mathcal{S}}(a - b\sigma)$ is the square of an element in $\mathcal{I}$, then $\sum_{(a,b)\in\mathcal{S}} v(F(a,b)) \equiv \overrightarrow{0} \pmod{2}$.*

This theorem tells us that in order for $\prod_{(a,b)\in\mathcal{S}}(a - b\sigma)$ to be a square in $\mathbb{Z}[\sigma]$, we need the second mini-vectors corresponding to the pairs $(a,b) \in \mathcal{S}$ to be linearly dependent.

4.3 The Third "Mini"-Vector

Recall from our discussion of the Norm that it is necessary and not sufficient that $\prod_{(a,b)\in\mathcal{S}} F(a,b)$ be a square in $\mathbb{Z}$. Similarly, to ensure $\prod_{(a,b)\in\mathcal{S}}(a - b\sigma)$ is a square, it is not enough to find a linear dependency modulo 2 among our second mini-vectors. Observe: from our example, we found that $F(-2,1) \cdot F(0,1) \cdot F(17,1) = 17^2 \cdot 19^2$. However, when we look at the product in $\mathbb{Z}[\sigma]$, we find that it is not a square. In fact, the product in $\mathbb{Z}[\sigma]$ is $-\sigma^3 + 15\sigma^2 + 34\sigma$, which has degree 3 could not possibly be a square.

To ensure that $\prod_{(a,b)\in\mathcal{S}}(a - b\sigma)$ is a square in $\mathbb{Z}[\sigma]$, we use the following fact: if we are given an integer u and we want to determine whether or not u is a square, we can look

at u modulo a series of prime numbers $q_1, \cdots, q_\ell$. If $(\frac{u}{q_j}) = 1$, where $(\frac{u}{q_j})$ is the Legendre Symbol, for a sequence of primes q_j, then there is a very good probability that u is a square.

As before, we have $a - b\sigma \in \mathbb{Z}[\sigma]$. We want to find a set of pairs of (a, b), $\mathcal{S}$, with $\prod_{(a,b)\in\mathcal{S}}(a - b\sigma) = \gamma^2 \in \mathbb{Z}[\sigma]$. Consider the homomorphisms

$$\begin{aligned} \theta_1 &: \mathbb{Z}[\sigma] \to \mathbb{Z}_{p_1}, \\ \theta_2 &: \mathbb{Z}[\sigma] \to \mathbb{Z}_{p_2}, \\ &\cdots, \\ \theta_k &: \mathbb{Z}[\sigma] \to \mathbb{Z}_{p_k}, \end{aligned}$$

where $\theta_i(g(\sigma)) = g(s_i) \pmod{q_i}$ for integers s_i and primes q_i. We need that $q_i | f(s_i)$, where f is the minimal polynomial of σ, to be sure that these θ_i's are homomorphisms.

For each element $a_i - b_i\sigma$, we associate a vector $(\pm 1, \pm 1, \cdots, \pm 1)$ where the first term is the Legendre Symbol $\left(\frac{\theta_1(a_i - b_i\sigma)}{q_1}\right)$, the second term is the Legendre Symbol $\left(\frac{\theta_2(a_i - b_i\sigma)}{q_2}\right)$, etc. To ensure $\prod_{(a,b)\in\mathcal{S}}(a - b\sigma) = \gamma^2$, we require an even number of -1's in each component. This works because if $\theta_1(g_i(\sigma))$ and $\theta_1(g_j(\sigma))$ are both quadratic non-residues with respect to q_1, then $\theta_1(g_i(\sigma)) \cdot \theta_1(g_j(\sigma))$ is a quadratic residue since $\left(\frac{\theta_1(g_i(\sigma))}{q_1}\right) = -1$ and $\left(\frac{\theta_1(g_j(\sigma))}{q_1}\right) = -1$ imply that

$$\left(\frac{\theta_1(g_i(\sigma)) \cdot \theta_1(g_j(\sigma))}{q_1}\right) = \left(\frac{\theta_1(g_i(\sigma))}{q_1}\right) \cdot \left(\frac{\theta_1(g_j(\sigma))}{q_1}\right) = (-1) \cdot (-1) = 1.$$

As a result, we change all of our vector entries which are $+1$ to 0. Then, there is no confusion when we take all three of our mini-vectors modulo 2.

We return to our example where $n = 667$, $d = 2$, $m = 25$, $f(z) = z^2 + z + 17$, and $\mathcal{B} = \{-1, 2, 3, 5, 7, 11, 13, 17, 19\}$. We made the second mini-exponent vectors for the pairs $(-2, 1)$, $(-1, 1)$, $(0, 1)$, $(1, 1)$, and $(17, 1)$. We will carry on with these relations and illustrate how to construct the third mini-vectors.

Let the functions $g_1(\sigma)$, $g_2(\sigma)$, $g_3(\sigma)$, $g_4(\sigma)$, and $g_5(\sigma)$ correspond to the pairs $(-2, 1)$, $(-1, 1)$, $(0, 1)$, $(1, 1)$, and $(17, 1)$, respectively. In other words, let $g_1(\sigma) = -2 - \sigma$, $g_2(\sigma) = -1 - \sigma$, etc. We will take $s_1 = 2$, $s_2 = 3$, $s_3 = 4$, and $s_4 = 5$. We see that $f(s_1) = 23$, $f(s_2) = 29$, $f(s_3) = 37$, and $f(s_4) = 47$, and we have that $q_1 = 23$, $q_2 = 29$, $q_3 = 37$, and $q_4 = 47$, where q_i is prime and $q_i | f(s_i)$. Now, let the function θ_i be such that $\theta_i(g_j(\sigma)) = g_j(s_i) \pmod{q_i}$. We construct Table 4.1.

	$g_1(\sigma) = -2 - \sigma$	$g_2(\sigma) = -1 - \sigma$	$g_3(\sigma) = 0 - \sigma$	$g_4(\sigma) = 1 - \sigma$	$g_5(\sigma) = 17 - \sigma$
$\theta_1(g_i(\sigma)) \equiv g_i(2)$ (mod 23)	$-2-2=-4$ $\equiv 19$ (mod 23) QNR	$-1-2=-3$ $\equiv 20$ (mod 23) QNR	$0-2=-2$ $\equiv 21$ (mod 23) QNR	$1-2=-1$ $\equiv 22$ (mod 23) QNR	$17-2=15$ (mod 23) QNR
$\theta_2(g_i(\sigma)) \equiv g_i(3)$ (mod 29)	$-2-3=-5$ $\equiv 24 \equiv (\pm 13)^2$ (mod 29) QR	$-1-3=-4$ $\equiv 25 \equiv (\pm 5)^2$ (mod 29) QR	$0-3=-3$ $\equiv 26$ (mod 29) QNR	$1-3=-2$ $\equiv 27$ (mod 29) QNR	$17-3=14$ (mod 29) QNR
$\theta_3(g_i(\sigma)) \equiv g_i(4)$ (mod 37)	$-2-4=-6$ $\equiv 31$ (mod 37) QNR	$-1-4=-5$ $\equiv 32$ (mod 37) QNR	$0-4=-4$ $\equiv 33 \equiv (\pm 12)^2$ (mod 37) QR	$1-4=-3$ $\equiv 34 \equiv (\pm 16)^2$ (mod 37) QR	$17-4=13$ (mod 37) QNR
$\theta_4(g_i(\sigma)) \equiv g_i(5)$ (mod 47)	$-2-5=-7$ $\equiv 40$ (mod 47) QNR	$-1-5=-6$ $\equiv 41$ (mod 47) QNR	$0-5=-5$ $\equiv 42 \equiv (\pm 18)^2$ (mod 47) QR	$1-5=-4$ $\equiv 43$ (mod 47) QNR	$17-5=12$ $\equiv (\pm 23)^2$ (mod 47) QR

Table 4.1: Make Third Mini- Vectors: Part 1.

	Legendre Symbol Vector	"Mini"-Vector for $a - b\sigma$
$-2 - \sigma$	$(-1, 1, -1, -1)$	$(-1, 0, -1, -1)$
$-1 - \sigma$	$(-1, 1, -1, -1)$	$(-1, 0, -1, -1)$
$0 - 2\sigma$	$(-1, -1, 1, 1)$	$(-1, -1, 0, 0)$
$1 - \sigma$	$(-1, -1, 1, -1)$	$(-1, -1, 0, -1)$
$17 - \sigma$	$(-1, -1, -1, 1)$	$(-1, -1, -1, 0)$

Table 4.2: "Mini"-Vector Corresponding to $a - b\sigma$

Based on Table 4.1, we can make vectors $(\pm 1, \pm 1, \cdots, \pm 1)$ for each pair (a, b) where each corresponding Legendre Symbol. To make this clear, we have included in Table 4.1 whether or not the evaluation of $\theta_i(g_j(\sigma))$ corresponds to a quadratic residue or a quadratic non-residue with respect to q_i. We write QR for Quadratic Residue, in which case its Legendre Symbol is 1, or QNR for Quadratic Non-Residue, when its Legendre Symbol is -1. Each column of the table corresponds to the third mini-vector for its respective $a - b\sigma$, and we have the listed the final mini-exponent vector in Table 4.2.

Notice that the second column of Table 4.2 is the vectors with the Legendre Symbols. In the third column, we have adjusted these vectors so that all of the values of $+1$ have been changed to 0. This will enable us to find a linear dependency among the quadratic non-residues.

After making all sets of our mini-exponent vectors, we concatenate them together to form one exponent vector that looks like $\overrightarrow{v}(a - b\sigma) = \langle \overrightarrow{v}_{G(a,b)} || \overrightarrow{v}_{F(a,b)} || \overrightarrow{v}_{a-b\sigma} \rangle$. Then we take the vectors modulo 2 and find our linear dependency among the concatenated vectors. If no such linear dependency exists, we can increase our bound M and search for more relations. In total, we should have $V = \#\mathcal{B} + \sum_{p \leq B} \#R(p) + \ell$ smooth relations in order to successfully find a proper divisor of n.

After we have our linear dependency, we need to find x, y, and γ from our x^2, y^2, and γ^2. Finding x is easy since we know its prime factorization. This is done similar to the computation of y in the Quadratic Sieve. Once we have a set $\mathcal{S}$ which includes all of our linearly dependent, B-smooth relations (a, b), then we can add up the appropriate coordinates of the first mini-exponent vectors, divide each sum by two, and multiply the resulting prime powers together to determine x.

To find γ from γ^2, we can solve for $\gamma \pmod{p}$ for some prime p. Then we can use Hensel Lifting to lift our solution modulo p^2, p^3, etc. until our solution stabilizes. Once we have γ, we use our homomorphism to compute $y = \phi(\gamma) \pmod{n}$.

Finally, we compute $\gcd(x-y,n)$ as our factor of n and we hope to have successfully factored n.

4.4 Summary

First, choose a factor base $\mathcal{B}$ consisting of all prime numbers $\leq B$, using a different B than for the Quadratic Sieve. Next, choose a small integer d and let $m = \lfloor n^{1/d} \rfloor$. Write n as $n = m^d + c_{d-1}m^{d-1} + \cdots + c_0$ where $c_i \in [0, m-1]$. Let $f(z) = z^d + c_{d-1}z^{d-1} + \cdots + c_0$, using the same c_i's that we have just generated above and let σ be some root of f. Let $F(a,b) = b^d f(a/b)$ and $G(a,b) = a - bm$ for integers a, b.

Pick some reasonble bound M such that $-M \leq z \leq M$, and sieve $F(a,b)$ and $G(a,b)$ for B-smooth values. In general, we take $M \approx B$. If both $F(a,b)$ and $G(a,b)$ are B-smooth, let

$$\mathcal{S}' = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} |\ 0 < |a|, b \leq M,\ \gcd(a,b) = 1, \text{ and } F(a,b),\ G(a,b)\ B\text{-smooth}\}.$$

Keep track of the exponents when sieving $G(a,b)$ and form the first mini-exponent vectors in the same manner as was used in the Quadratic Sieve. Then, create the set $R(p)$ for each $p \in \mathcal{B}$. Fix $0 \leq |a| < M$, let b vary such that $(a,b) \in \mathcal{S}'$, and for each $p \in \mathcal{B}$, look for values of b such that $a \equiv br \pmod{p}$ for some $r \in R(p)$. If for a particular b value, no such r exists, then designate the appropriate coordinate in the exponent vector for $F(a,b)$ as 0. Otherwise, find the exponent as usual. Next, fix $0 \leq b < M$ and let a vary. Sieve until sufficiently many relations have been generated.

Choose a sequence of integers $s_1, \cdots, s_k$ and find primes $p_1, \cdots, p_k$ such that $p_i | f(s_i)$. For each $(a,b) \in \mathcal{S}'$, evaluate $a - b\sigma$ at $\sigma = s_i$ and take the result modulo p_i. If the Legendre Symbol $\left(\dfrac{(a - bs_i \mod p_i)}{p_i}\right) = 1$, then we set the i-th component of our last mini-vector to 0. However, if $\left(\dfrac{(a - bs_i \mod p_i)}{p_i}\right) = -1$, then we set the i-th component to -1.

We concatenate all three mini-exponent vectors and find a linear dependency modulo 2. We make a new set $\mathcal{S}$ of all the pairs (a,b) in our linear dependency. We us the original first mini-vector to create x and find γ via modular arithmetic and Hensel Lifting. Finally, we use our homomorphism ϕ to find $y = \phi(\gamma)$, and take $\gcd(x-y,n)$ as our factor of n.

Chapter 5

The Experiment

Crandall and Pomerance [3] tell us that the optimal bound for our factor base is $B = \exp(\frac{1}{2}(\ln n \ln\ln n)^{1/2})$. They further tell us that we require at least $\#\mathcal{B}+1$ smooth relations to ensure our success. They assume that the probability that a quadratic residue in $\mathbb{Z}_n$ is B-smooth is approximately u^{-u}, where $u = \ln n / \ln B$. This means that we expect to go through u^u values of z to find one $Q(z)$ which is B-smooth.

From this, we find that if we want to sieve a sequence of z values where $z \in [-M, M]$ for some integer M, we need

$$\begin{aligned} 2M+1 &= (u^u)\cdot(\#\mathcal{B}+1) \\ M &= (1/2)\cdot(u^u)\cdot(\#\mathcal{B}+1) - 1/2, \text{ where } u = \ln n/\ln B. \end{aligned}$$

This value of M is for the worst case scenario: we go through all u^u values of z in order to find each smooth relation, we require all $\#\mathcal{B}+1$ smooth relations to factor n successfully, and we do not take B to be smaller than the value given above.

Crandall and Pomerance [3] also tell us that a smaller value of B usually does work. Would a smaller value of M work in most cases, too? This is the question that we experimented with. We endeavoured to find the best possible M to quickly and successfully factor n.

In our experiment, we tested 12 different values of M: $1/10M$, $2/10M$, $\cdots$, $10/10M$, $11/10M$, $12/10M$. We used our own Maple implementation of the Quadratic Sieve with 75 different values of n, performing each run three times and averaging the time taken by the algorithm. We also recorded whether or not each run was successful and whether or not we had the number of smooth relations necessary to successfully factor n, i.e. whether or not the number of smooth relations exceeded $\#\mathcal{B}+1$. The results of the experiments are summarized in Figure 5.1.

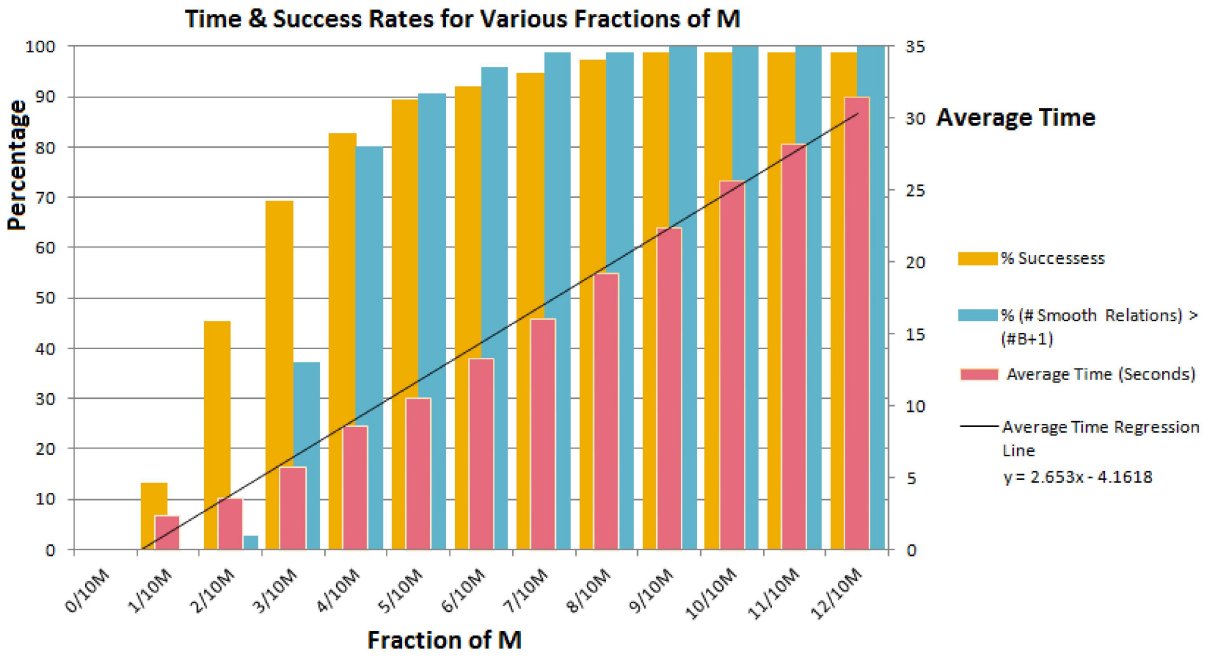

Figure 5.1: Experimental Results.

The incidences where the number of smooth values exceeds $(\#\mathcal{B}+1)$ indicate when the algorithm *should* have worked in factoring n. This is just to monitor our expectations for each fraction of M. We see that for some fractions of M, like $2/10M$, we have very few instances with (# Smooth Relations) $>(\#\mathcal{B}+1)$, but we have a much larger success rate. In this case, we were lucky and found a linear dependency among a smaller then expected number of vectors. On the other hand, for some fractions of M, say $7/10M$, we have more instances where we should be able to factor n than we have instances where we are actually able to factor n. In this case, the linear dependencies found resulted in trivial factorizations of n. Together, these two cases show us that although $(\#\mathcal{B}+1)$ is generous in many cases, it is fairly well chosen.

We can see from the figure that the Average Time, measured in seconds, taken to run the algorithm grows linearly with M and the number of successes and number of incidences where we *should* have enough smooth relations grows rapidly for small fractions of M and stabilizes for larger fractions of M. However, we have exactly the same success rates for $9/10M$ to $12/10M$. As M grows, we are getting less value for the extra time spent. This confirms that as z grows, it is less likely that $Q(z)$ is going to be B-smooth.

In the end, we find that one is able to customize the Quadratic Sieve depending on their requirements. If one has one number to factor and time is not a constraint, than $10/10M$ may be the best possible choice for M for his/her purpose. If one has several numbers to factor and not a lot of time to do it, than taking smaller fraction of M, say $7/10M$ or

$8/10M$, might be a better choice. For example, by choosing $8/10M$, the algorithm is sped up by a whopping 24.94% compared with $10/10M$, while the accuracy is reduced by less than 1.5% when compared with $10/10M$. Additionally, we conjecture that one could use an even smaller fraction of M if one used the Multiple Polynomial extension. One could also take a fraction smaller than $10/10M$ and, if the algorithm is unsuccessful, expand M and generate a few new relations, and find a new linear dependency. This is nice because one can still use all of the B-smooth numbers that the algorithm finds the first time around.

Chapter 6

Conclusion

Factoring large integers still remains a challenging problem. As recently as 2007, RSA Laboratories held a Factoring Challenge and asked the public to factor a collection of numbers which they believed to hold the greatest challenge for modern factoring capabilities. The project inspired major successes and in 2009 when RSA-768, a 768-bit or 232-digit number, was factored successfully after almost 3 years of effort [9]. The challenge was closed in 2007, but the RSA Laboratories has several un-factored numbers remaining on their website, and next in line is RSA-896, a 270-digit number. We did not have the time or resources to attempt to factor this, having only 4 months, a sturdy Toshiba, a 4-year-old IMac, and a broken Sony laptop. However, it remains a possibility for the long winter months ahead.

Further research includes implementing the Multiple Polynomial extension to find out what the success rates of various fractions of M are when the extension is involved and how much the extension is able to speed up the algorithm. The value is most likely be much smaller than $10/10M$, since the $Q(z)$ values are just getting larger and larger. At the moment this is just conjecture, though.

The Quadratic Sieve and Number Field Sieve algorithms are both conjectured to be sub-exponential time algorithms. Although we only looked at sub-exponential time factoring methods that involved sieving in some fashion in this paper, it would be interesting to explore other sub-exponential time algorithms. Among these is Lenstra's Elliptic Curve Factoring Method. This apparently works quite well if one of the prime factors of n is small, say 30-digits or less [14]. As a result, the primes used in RSA in practice are approximately the same size, around $\sqrt{n}$. However, they can't be too close to $\sqrt{n}$ because Pollard's original factoring method can be used if n is close to a prime power [14]. It would be interesting to see exactly how both of these algorithms work, though.

Factoring integers has never been more exciting than it is now, and we have never before

had so many methods to choose from when factoring a single integer. These methods have come a long way since 1903, and they are only likely to get faster. In standard RSA schemes, we are now dealing with integers where it is simply infeasible to attempt to factor by trial division, no matter how many Sundays one dedicates to it. RSA Laboratories' Factoring Challenge was a call to improve existing factoring methods and generate new ones. People rose to the challenge. RSA Laboratories still keeps an archive of the challenge on their website, including several numbers which have yet to be factored. Hopefully, this will continue to engage people and push forward the evolution of integer factoring.

References

[1] W. S. Anglin. *Mathematics, a Concise History and Philosophy.* Springer-Verlag, New York, 1994.

[2] Atkins. The magic words are squeamish ossifrage. In *Advances in Cryptology, Lecture Notes in Computer Science*, volume 209, pages 169–182, Asiacrypt, 1994. Springer-Verlag.

[3] Richard Crandall and Carl Pomerance. *Prime numbers.* Springer, New York, second edition, 2005. A computational perspective.

[4] J. A. Davis and D. B. Holdridge. Factorization using the quadratic sieve algorithm. In *Sandia Report Sand*, Report, pages 83–1346. Sandia National Laboratories, Albuquerque, New Mexico, 1983.

[5] Minking Eie and Shou-Te Chang. *A Course on Abstract Algebra.* World Scientific, Toh Tuck Link, Singapore, 2010.

[6] Steven D. Galbraith. *Mathematics of Public Key Cryptography.* Cambridge University Press, New York, 2012.

[7] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An introduction to mathematical cryptography.* Undergraduate Texts in Mathematics. Springer, New York, 2008.

[8] Edna E. Kramer. *The Nature and Growth of Modern Mathematics.* Princeton University Press, Princeton, NJ, 1981.

[9] RSA Laboratories. Online RSA-768 is factored!, August 2009.

[10] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, Boca Raton, 1997.

[11] School of Mathematics and University of St Andrews Statistics. Online Frank Nelson Cole, August 2005.

[12] C. Pomerance. Analysis and comparison of some integer factoring algorithms. In *Computational methods in number theory, Part I*, volume 154 of *Math. Centre Tracts*, pages 89–139. Math. Centrum, Amsterdam, 1982.

[13] Carl Pomerance. The quadratic sieve factoring algorithm. In T. Beth, N. Cot, and I. Ingemarrson, editors, *Advances in Cryptology*, volume 209 of *Lecture Notes in Computer Science*, pages 169–182, Eurocrypt '84, 1985. Springer-Verlag.

[14] Carl Pomerance. A tale of two sieves. *Notices Amer. Math. Soc.*, 43(12):1473–1485, 1996.

[15] Carl Pomerance, J. W. Smith, and Randy Tuler. A pipeline architecture for factoring large integers with the quadratic sieve algorithm. *SIAM J. Comput.*, 17:387–403, 1988.

[16] Robert D. Silverman. The multiple polynomial quadratic sieve. *Math. Comp.*, 48(177):329–339, 1987.