Cubic Polynomials in the Number Field Sieve

by

Ronnie Scott Williams, Jr., B.S.

A Thesis

In

Mathematics and Statistics

Submitted to the Graduate Faculty
of Texas Tech University in
Partial Fulfillment of
the Requirements for the Degree of

Master of Science

Approved

Dr. Chris Monico
Chair

Dr. Lars Christensen

Dr. Xiaochang Alex Wang

Fred Hartmeister
Dean of the Graduate School

May, 2010
ACKNOWLEDGMENTS

First, I would like to thank Dr. Chris Monico. Without his guidance, help and knowledge none of this would have been possible. I would also like to thank the other members of my committee, Dr. Lars Christensen and Dr. Alex Wang, for their encouragement and support throughout this process. In addition, I must express my deep appreciation to all of my colleagues and friends at Texas Tech University, especially Mr. Dale Pearson, who were always there to offer a helping hand.

On a personal note, I truly thank my family for their love and support throughout my entire life. Without it, I would not be where or who I am today. And finally, I thank my best friend and loving wife Erin, who was always with me, every step of the way. She is the reason this paper is what you see before you. This is for you as much as it is for me, my friends, my family, and my wife. Thank you.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>ii</td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>iv</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>v</td>
</tr>
<tr>
<td>1. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Public Key Cryptography</td>
<td>1</td>
</tr>
<tr>
<td>1.2 The Number Field Sieve</td>
<td>2</td>
</tr>
<tr>
<td>1.3 Thue’s Lemma</td>
<td>6</td>
</tr>
<tr>
<td>2. LINEAR ALGEBRA</td>
<td>9</td>
</tr>
<tr>
<td>3. THE LLL-ALGORITHM</td>
<td>13</td>
</tr>
<tr>
<td>4. POLYNOMIAL SELECTION</td>
<td>15</td>
</tr>
<tr>
<td>4.1 Equivalence Class and Lattice Correspondence</td>
<td>15</td>
</tr>
<tr>
<td>4.2 Construction of $O(N^{1/4})$ Quadratics</td>
<td>17</td>
</tr>
<tr>
<td>4.3 Construction of $O(N^{2/9})$ Cubics</td>
<td>18</td>
</tr>
<tr>
<td>5. EXAMPLES</td>
<td>21</td>
</tr>
<tr>
<td>5.1 $O(N^{1/4})$ Quadratics</td>
<td>21</td>
</tr>
<tr>
<td>5.2 $O(N^{2/9})$ Cubics</td>
<td>22</td>
</tr>
<tr>
<td>6. CONCLUSION</td>
<td>25</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>26</td>
</tr>
</tbody>
</table>
In order to use the Number Field Sieve to factor an integer, $N$, two coprime, irreducible polynomials with a common root modulo $N$ must be found. It is conjectured that there exist pairs of cubic polynomials with coefficients of size $O(N^{1/6}) = O(N^{3/18})$ for any choice of $N$, but this has yet to be proven. In this thesis, we provide a method for constructing two cubic polynomials with coefficients of size $O(N^{2/9}) = O(N^{4/18})$. This is achieved through a clever choice of common root and the use of the LLL-algorithm.
LIST OF FIGURES

2.1 Lattice with basis \{(0, 1)^\top, (1, 0)^\top\} .................................................. 10
2.2 Lattice with basis \{(1, 3)^\top, (3, 4)^\top\} .................................................. 10
2.3 Lattice with basis \{(2, 1)^\top, (-1, 2)^\top\} .................................................. 11
Throughout history, the need to keep information private has been widely recognized. From Caesar’s encrypted messages to his generals in the first century B.C.; to the “red telephone” – the Moscow-Washington hotline – put in place and used during the presidencies of John F. Kennedy and Lyndon B. Johnson to directly and securely communicate with the Soviet Union during the Cold War; and even today to your online bank account trying to keep all of your personal information private; cryptography has played a major part in keeping information confidential.

Along with the desire to secure information, there has always been an equal desire to steal the confidential information and break the encryption. We present a practical improvement to an already established method of breaking encryption, the Number Field Sieve.

First, we give a brief overview of public-key cryptography, a particular branch of cryptography which is widely used in everyday matters, then we give an explanation of the Number Field Sieve. Next, we move on to give some necessary information about Linear Algebra and the LLL-algorithm, which will be used throughout.

Our results are then presented. If \( N \) is a large number we wish to factor, we begin by constructing two coprime, irreducible \( O(N^{1/4}) \) quadratics with a common root modulo \( N \), and follow this by constructing two coprime, irreducible \( O(N^{2/9}) \) cubics with a common root modulo \( N \). We conclude by giving examples of this improvement.

### 1.1 Public Key Cryptography

In early cryptographic systems, such as the well-known Caesar Shift Cipher, it is necessary for both the sender and the receiver of a message to privately meet and agree upon a key to use for the encryption and decryption of messages. While a physical key exchange does provide a secure way to send and receive a message, it is very impractical to privately agree upon and exchange a key. Luckily, public key cryptography avoids this problem. Public key cryptography uses two keys, an encryption key and a decryption key. The to-be recipient of a message publishes the encryption key so that the sender can disguise the message, but keeps the decryption key private. While the decryption key is
essentially the inverse of the encryption key, there is no easily computed method of
determining a decryption key given an encryption key in this system.

In 1977, Ron Rivest, Adi Shamir and Leonard Adleman developed a type of public key
cryptography known as the RSA cryptosystem [12]. In this system, the to-be recipient,
Alice, picks two large prime numbers, \( p \) and \( q \), and computes their product, \( N = pq \). Alice
then computes \( \phi(N) = (p-1)(q-1) \), where \( \phi \) is the Euler phi-function. Next, Alice picks
an integer \( e \) such that \( (e, \phi(N)) = 1 \) and finds a \( d \) so that \( ed \equiv 1 \mod \phi(N) \). Having done
this, Alice publishes the pair \((N, e)\).

Now, the sender, Bob, converts his message into an integer representation, \( m \in \mathbb{Z}/N\mathbb{Z} \),
using an openly agreed upon padding scheme. Then Bob computes \( y = m^e \mod N \) using
Alice’s published pair \((N, e)\), and sends the encrypted message to Alice.

Alice can recover Bob’s original message by computing \( y^d \mod N \). This is possible
since Alice knows that \( y^d \equiv (m^e)^d \equiv m^{ed} \equiv m \mod N \). The last equivalence holds since
we required that \( ed \equiv 1 \mod \phi(N) \), which means \( ed = 1 + \phi(N)t \) for some \( t \in \mathbb{Z} \).
Therefore, \( m^{ed} \equiv m^{1+\phi(N)t} \equiv m(m^{\phi(N)t}) \equiv m(1^t) \equiv m \mod N \) by Euler’s Theorem. Thus,
Alice knows \( m \), the original message Bob wanted to send her.

Now, if an eavesdropper, Eve, was trying to intercept and read the message Bob sent to
Alice, she knows Alice’s published pair \((N, e)\) as well as Bob’s encrypted message, \( y = m^e \mod N \). If Eve knew \( \phi(N) \), then she could determine \( d \) by solving the equivalence
\( ed \equiv 1 \mod \phi(N) \), and then recover \( m \) just as Alice did. However, if \( \phi(N) \) were known
we could let \( \ell = \frac{N + 1 - \phi(N)}{2} \), then \( p' = \ell + \sqrt{\ell^2 - N} \) would be a proper divisor of \( N \).
Hence, determining \( \phi(N) \) would be computationally equivalent to factoring \( N \).

This means the best way for Eve to recover Bob’s message is to factor \( N \), which is
exceedingly difficult for large \( N \). However, there are still many ways to do this, one of
which is through using the Number Field Sieve.

1.2 The Number Field Sieve

Currently, the Number Field Sieve is the fastest known algorithm for factoring large
integers, those of more than 100 digits. It was first conceived by J.M. Pollard in [11],
however, this method was only applicable to numbers of the form \( x^3 + k \). Pollard’s original
method was subsequently refined by A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse and
himself in [7], making the sieve applicable to all integers. So, before moving on, we
present a very brief overview of the idea behind the Number Field Sieve.

Let \( R_1 \) and \( R_2 \) be integral domains with ring homomorphisms \( \psi_1 : R_1 \to \mathbb{Z}/N\mathbb{Z} \) and \( \psi_2 : R_2 \to \mathbb{Z}/N\mathbb{Z} \). Our goal is to find \((u, v) \in R_1 \times R_2\) such that \(\psi_1(u^2) = \psi_2(v^2)\) uniformly from among all such \((u, v)\) pairs. Once we have this, we know \(\psi_1(u^2) - \psi_2(v^2) \equiv 0 \pmod{N}\); hence \([\psi_1(u) - \psi_2(v)](\psi_1(u) + \psi_2(v)) \equiv 0 \pmod{N}\). If \(\psi_1(u) \neq \pm\psi_2(v) \pmod{N}\), then \(N\) can be factored with probability at least \(\frac{1}{2}\) by computing two greatest common divisors, \((\psi_1(u) - \psi_2(v), N)(\psi_1(u) + \psi_2(v), N) = N\).

In order to find such pairs, \((u, v)\), we want to produce sets of elements \(\{u_1, u_2, \ldots, u_t\} \subseteq R_1\) and \(\{v_1, v_2, \ldots, v_t\} \subseteq R_2\) for which \(\psi_1(u_j) = \psi_2(v_j)\) and \(u_j\) and \(v_j\) factor easily. Then by using these sets we would like to find another set \(S \subset \{1, 2, \ldots t\}\) for which both \(\prod_{j \in S} u_j = u^2 \in R_1\) and \(\prod_{j \in S} v_j = v^2 \in R_2\). It follows that \(\psi_1(u^2) = \psi_2(v^2)\), and we hope to have \(\psi_1(u) \neq \pm\psi_2(v)\), thus factoring \(N\), by computing greatest common divisors.

To construct the rings \(R_1\) and \(R_2\), and the homomorphisms \(\psi_1\) and \(\psi_2\) we choose two coprime, irreducible polynomials \(f_1, f_2 \in \mathbb{Z}[x]\) with a common root \(m \in \mathbb{Z}\) modulo \(N\). Then take \(R_i = \mathbb{Z}[x]/\langle f_i \rangle\) with \(\psi_i : \mathbb{Z}[x]/\langle f_i \rangle \to \mathbb{Z}/N\mathbb{Z}\) for \(i = 1, 2\) such that \(x + \langle f_i \rangle \mapsto m\). Equivalently, if we consider \(\theta_i\) to be a formal root of \(f_i\) then \(\mathbb{Z}[x]/\langle f_i \rangle \cong \mathbb{Z}[\theta_i]\), with \(\psi_i : \mathbb{Z}[\theta_i] \to \mathbb{Z}/N\mathbb{Z}\) and \(\theta_i \mapsto m\) for \(i = 1, 2\). If we let \(u_j = a_j - b_j\theta_1 \in \mathbb{Z}[\theta_1]\) and \(v_j = a_j - b_j\theta_2 \in \mathbb{Z}[\theta_2]\), where \(a_j\) and \(b_j\) are coprime integers, then, as desired, we have \(\psi_1(u_j) = a_j - b_jm = \psi_2(v_j)\) for \(j = 1, 2, \ldots, t\).

As stated above, we want to factor our \(u_i\)'s and \(v_i\)'s easily. However these are elements of \(R_1\) and \(R_2\), respectively, where we may not have unique factorization. To avoid this problem, instead of factoring the elements we instead seek to factor the ideals generated by them, \(\langle u_j \rangle\) and \(\langle v_j \rangle\), which will have unique factorization since number fields are Dedekind domains.

Before factoring the ideals we introduce a norm on elements of \(R_1\) and \(R_2\). We have \(f_i = c_{0,i} + c_{1,i}x + \cdots + c_{d_i,i}x^{d_i}\) with complex roots \(\alpha_{1,i}, \alpha_{2,i}, \ldots, \alpha_{d_i,i}\). If we divide \(f_i\) by \(c_{d_i,i}\) we can obtain a monic polynomial \(\frac{f_i}{c_{d_i,i}} = c_{0,i} + c_{1,i}x + \cdots + c_{d_i,i}x^{d_i}\). Now, for \(\gamma \in \mathbb{Q}[x]/\langle f_i \rangle = \mathbb{Q}(\theta_i)\) we define the norm \(N_{\mathbb{Q}(\theta_i)\mathbb{Q}}(\gamma) = \prod_{j=1}^{d_i} \sigma_j(\gamma)\) where \(\sigma_1, \sigma_2, \ldots, \sigma_{d_i}\) are distinct embeddings of \(\mathbb{Q}(\theta_i)\) into \(\mathbb{C}\). From this point, we will simply refer to this norm by \(N_i(\gamma)\). Notice that
\[ N_i(a_j - b_j \theta_1) = (a_j - b_j \alpha_{1,j}) \cdots (a_j - b_j \alpha_{d,j}) = b_j^{d_i} \left( \frac{a_j}{b_j} \right)^{i} \left( \frac{\alpha_{1,j}}{\alpha_{d,j}} \right) \]

Therefore, it follows that
\[ N_1(u_j) = N_1(a_j - b_j \theta_1) = \frac{b_j^{d_i} f_1 \left( \frac{a_j}{b_j} \right)}{c_{d_i, 1}} \]

\[ N_2(v_j) = N_2(a_j - b_j \theta_2) = \frac{b_j^{d_2} f_2 \left( \frac{a_j}{b_j} \right)}{c_{d_2, 1}}. \]

It can also be shown that factoring the ideals \( \langle u_j \rangle = \langle a_j - b_j \theta_1 \rangle \) and \( \langle v_j \rangle = \langle a_j - b_j \theta_2 \rangle \) reduces easily to factoring \( N_1(a_j - b_j \theta_1) \) and \( N_2(a_j - b_j \theta_2) \), respectively. Therefore, it suffices to find many \( (a_j, b_j) \) pairs for which we can factor \( N_1(a_j - b_j \theta_1) \). Thus, we find \( (a_j, b_j) \in [-A, A] \times [1, B] \subset R_1 \times R_2 \) such that \( N_1(a_j - b_j \theta_1) \) is \( \beta_1 \)-smooth, and \( N_2(a_j - b_j \theta_2) \) is \( \beta_2 \)-smooth, for some choice of \( \beta_1 \) and \( \beta_2 \). For simplicity we will take \( \beta_1 = \beta_2 = \beta \). Once we have found \( t > \pi(\beta_1) + \pi(\beta_2) = 2\pi(\beta) \) such \( (a_j, b_j) \) pairs, \( \mathbb{F}_2 \) linear algebra guarantees that there exists some \( S \subset \{1, 2, \ldots, t\} \) such that \( \prod_{j \in S} N_1(a_j - b_j \theta_1) \) and \( \prod_{j \in S} N_2(a_j - b_j \theta_2) \) are square, which will correspond to our desired \( u^2 \in R_1 \) and \( v^2 \in R_2 \), respectively. There are actually a few more details required to force this to happen, however we will forgo providing them.

The reason why \( \mathbb{F}_2 \) linear algebra guarantees the existence of such an \( S \) can be seen as follows. Let \( m = \pi(\beta) < t \) and write \( N_1(a_j - b_j \theta_1) = p_1^{\alpha_{1,j}} p_2^{\alpha_{2,j}} \cdots p_m^{\alpha_{m,j}} \) and \( N_2(a_j - b_j \theta_2) = p_1^{\beta_{1,j}} p_2^{\beta_{2,j}} \cdots p_m^{\beta_{m,j}} \), where \( p_1, p_2, \ldots, p_m \) are all of the primes up to \( m \). We want to find some number of \( N_i(a_j - b_j \theta_i) \)'s whose product is square in \( \mathbb{Z} \), for \( i = 1, 2 \), so it suffices to show some product of the \( N_i(a_j - b_j \theta_i) \)'s will have all even \( \alpha \)'s and \( \beta \)'s.

Multiplication of the \( N_i(a_j - b_j \theta_i) \)'s corresponds to addition of the vectors \( (\alpha_{1,j}, \alpha_{2,j}, \ldots, \alpha_{m,j}, \beta_{1,j}, \beta_{2,j}, \ldots, \beta_{m,j})^\top \), and since we only care that the \( \alpha \)'s and \( \beta \)'s are even, we consider these vectors to be in \( \mathbb{F}_2 \). We have \( t \) total \( N_i(a_j - b_j \theta_i) \)'s, for \( i = 1, 2 \), so we have \( t \) vectors of dimension \( 2m = 2\pi(\beta) < t \). Therefore, there is a linear dependence on these \( t \) vectors such that there exist some \( \gamma_j \) \( j = 1 \in \mathbb{F}_2 \), not all zero, such that
\[ \sum_{j=1}^{t} \gamma_j(\alpha_{1,j}, \alpha_{2,j}, \ldots, \alpha_{m,j}, \beta_{1,j}, \beta_{2,j}, \ldots, \beta_{m,j})^\top = 0. \]

Hence, let \( S = \{ j : \gamma_j \neq 0 \} \), then \( \prod_{j \in S} N_1(a_j - b_j \theta_1) \) and \( \prod_{j \in S} N_2(a_j - b_j \theta_2) \) will have all even \( \alpha \)'s and \( \beta \)'s, and therefore be squares. From this we can essentially recover our desired \( u^2 \in R_1 \) and \( v^2 \in R_2 \), so we can factor \( N \) by computing greatest common divisors as mentioned above.
At this point, we still have some freedom in the choice of variables $\beta_1, \beta_2, A, B$ and the degree of our polynomials, $d$. So, we now want to briefly discuss the effects of different possible choices of these variables. The amount of work, or the runtime, of the Number Field Sieve can be roughly broken down into three steps: a sieving step; a linear algebra step; and a square-root step. A careful analysis shows that the asymptotic runtime is optimal when all three steps have roughly the same runtime.

Obviously, we would like to minimize the runtime as much as possible. However the runtime can only be minimized subject to a particular constraint which we will now derive. First, find the maximums $M_1$ of $|N_1(a_j - b_j \theta_1)|$ and $M_2$ of $|N_2(a_j - b_j \theta_2)|$ for $(a_j, b_j) \in [-A, A] \times [1, B] = R$. Now, using a theorem of Canfield, Erdős and Pomerance found in [2] we can estimate the probability $\tilde{p}_1$ that $t_1 \in [1, M_1]$ is $\beta_1$-smooth and the probability $\tilde{p}_2$ that $t_2 \in [1, M_2]$ is $\beta_2$-smooth. Then the expected number of acceptable $(a_j, b_j)$ pairs in $R$ is about $2AB \tilde{p}_1 \tilde{p}_2$. We know that we need $\pi(\beta_1) + \pi(\beta_2)$ such $(a_j, b_j)$ pairs in $R$, so we must have $2AB \tilde{p}_1 \tilde{p}_2 \geq \pi(\beta_1) + \pi(\beta_2)$. Therefore, we want to minimize (1.1) subject to the constraint

$$2AB \tilde{p}_1 \tilde{p}_2 \geq \pi(\beta_1) + \pi(\beta_2),$$

$$\approx \frac{\beta_1}{\log \beta_1} + \frac{\beta_2}{\log \beta_2}.$$ 

Careful observation of the derivation of the above constraint reveals, for optimization purposes, that our undefined variables $\beta_1, \beta_2, A, B$ and $d$ are all dependent upon each other. For instance, if $A, B$ and $d$ were fixed we could easily determine the values $M_1$ and $M_2$. Then using the theorem of Canfield, Erdős and Pomerance we could write our probabilities as a function of $\beta_i$ and minimize the runtime. Or if $\beta_1, \beta_2$ and $d$ were known, we could again use the theorem of Canfield, Erdős and Pomerance to write our probabilities as a function of $M_i$ and minimize the runtime. Then knowing the optimal $M_i$ we could find the optimal range for $a_j$ and $b_j$. This is because we know $M_i \geq N_i(a_j - b_j \theta_i) = \frac{b^d f_i(a_j / b_j)}{c_0}$, and $d$ gives us a bound on the coefficients of $f_i$. In a similar manner, if we know $A, B, \beta_1$ and $\beta_2$ we could find the optimal choice for degree $d$. Since the constraint depends on the choice of $\beta_1, \beta_2, A, B$ and $d$ and the runtime of the Number Field Sieve depends on minimizing with respect to this constraint, it is also dependent upon our choice of $\beta_1, \beta_2, A, B$ and $d$.
1.3 Thue’s Lemma

Before moving on to discuss the machinery needed for our improvement, as well as the construction of our polynomials, we make a brief aside. We present a generalization of a well-known lemma of Thue first seen in [13] which will be modified into two theorems which will show the existence of one polynomial with small coefficients.

**Lemma 1.3.1 (Thue).** Let $N \in \mathbb{Z}$ and $a \in \mathbb{Z}^+$ with $a$ and $N$ coprime. Then the congruence $ax \equiv y \pmod{N}$ admits a solution $x_0, y_0$, where $0 < |x_0| < \sqrt{N}$ and $0 < |y_0| < \sqrt{N}$.

Now generalizing Thue’s lemma we show there exists a polynomial congruent to zero modulo $N$ with small coefficients.

**Theorem 1.3.1.** Let $N \in \mathbb{Z}^+$ and $r_1, r_2, \ldots, r_n \in \mathbb{Z}^+$ with each $r_i$ coprime to $N$, for $i = 1, \ldots, n$. Then the congruence $x_0 + x_1 r_1 + x_2 r_2 + \cdots + x_n r_n \equiv 0 \pmod{N}$ admits a nontrivial solution $x_0, x_1, \ldots, x_n$ with $0 \leq |x_i| \leq N^{1/(n+1)}$ for $i = 1, 2, \ldots, n$.

**Proof.** Let $B = \left\lfloor N^{1/(n+1)} \right\rfloor + 1$, where $\lfloor \cdot \rfloor$ represents the greatest-integer function, and consider the set of integers $S = \{x_0 + x_1 r_1 + x_2 r_2 + \cdots + x_n r_n : 0 \leq x_0, x_1, \ldots, x_n \leq B - 1 \}$. Since there are $B^{n+1} > N$ possible $(n+1)$-tuples $(x_0, x_1, \ldots, x_n)$, the Pigeonhole Principle guarantees that there exist at least two distinct $(n+1)$-tuples whose corresponding sums are congruent modulo $N$, say $a_0 + a_1 r_1 + \cdots + a_n r_n \equiv b_0 + b_1 r_1 + \cdots + b_n r_n \pmod{N}$. Then let $x_i = a_i - b_i$ for $i = 0, \ldots, n$ and we have

$$x_0 + x_1 r_1 + \cdots + x_n r_n \equiv (a_0 - b_0) + (a_1 - b_1)r_1 + \cdots + (a_n - b_n)r_n \equiv 0 \pmod{N},$$

with $0 \leq |x_0|, |x_1|, \ldots, |x_n| \leq B - 1 \leq N^{1/(n+1)}$. And since $(a_0, a_1, \ldots, a_n) \neq (b_0, b_1, \ldots, b_n)$ at least one $x_j$ is nonzero. \hfill $\Box$

The previous theorem assumed that nothing was known about the sizes of the $r_i$’s. If indeed we do have information on the size of each $r_i$ we can obtain a tighter bound on our coefficients. That is, provided the $r_i$’s are relatively small.

**Theorem 1.3.2.** Let $N \in \mathbb{Z}^+, r_1, r_2, \ldots, r_n \in \mathbb{Z}^+$ with each $r_i$ coprime to $N$ for $i = 1, \ldots, n$, and $R = \max\{r_1, r_2, \ldots, r_n\}$. Then the congruence $x_0 + x_1 r_1 + x_2 r_2 + \cdots + x_n r_n \equiv 0 \pmod{N}$ admits a nontrivial solution $x_0, x_1, \ldots, x_n$ with

$$0 \leq |x_0|, |x_1|, \ldots, |x_n| \leq (n + 1)^{1/n} \min\left\{R, \left(\frac{1}{n+1}\right)^{1/n} N^{n/(n+1)}\right\}^{1/n}.$$
Proof. First, if \( \min \{ R, \left( \frac{1}{n+1} \right) N^{n/(n+1)} \} = \left( \frac{1}{n+1} \right) N^{n/(n+1)} \) then our desired bounds become

\[
0 \leq |x_0|, |x_1|, \ldots, |x_n| \leq (n + 1)^{1/n} \min \left\{ R, \left( \frac{1}{n+1} \right) N^{n/(n+1)} \right\}^{1/n} = (n + 1)^{1/n} \left( \frac{1}{n+1} \right) N^{n/(n+1)} \frac{1}{n} \begin{align*}
\end{align*}
\]

reducing the conclusion to that of Theorem 4.1.1, so we are done.

Therefore, suppose \( \min \{ R, \left( \frac{1}{n+1} \right) N^{n/(n+1)} \} = R. \) Let \( B = \left[ (n + 1)^{1/n} R^{1/n} \right] + 1 \) and consider the set of integers \( S = \{ x_0 + x_1 r_1 + x_2 r_2 + \cdots + x_n r_n : 0 \leq x_0, x_1, \ldots, x_n \leq B - 1 \}. \) Then for each \( y \in S \) we have \( 0 \leq y \leq (n + 1)(B - 1)R < (n + 1)BR. \) Now, there are \( B^{n+1} \) such \( (n + 1) \)-tuples \((x_0, x_1, \ldots, x_n)\) and we have that

\[
B^n > ((n + 1)^{1/n} R^{1/n})^n = (n + 1)R,
\]

so,

\[
B^{n+1} > (n + 1)BR.
\]

Thus, each \( x \in S \) is less than or equal to \((n + 1)BR\), but there are more than \((n + 1)BR\) possible \((n + 1)\)-tuples, hence, by the Pigeonhole Principle, there exist distinct \((n + 1)\)-tuples \((a_0, a_1, \ldots, a_n)\) and \((b_0, b_1, \ldots, b_n)\) such that

\[
a_0 + a_1 r_1 + \cdots + a_n r_n = b_0 + b_1 r_1 + \cdots + b_n r_n,
\]

and therefore must be congruent modulo \( N \). Let \( x_i = a_i - b_i \) for \( i = 0, \ldots, n \) and we have

\[
x_0 + x_1 r_1 + \cdots + x_n r_n \equiv (a_0 - b_0) + (a_1 - b_1)r_1 + \cdots + (a_n - b_n)r_n \equiv 0 \pmod{N},
\]

with \( 0 \leq |x_0|, |x_1|, \ldots, |x_n| \leq B - 1 \leq (n + 1)^{1/n} R^{1/n}. \) \( \Box \)

Hence, if we can find \( r_1, r_2 \equiv r_1^2 \pmod{N} \) and \( r_3 \equiv r_1^3 \pmod{N} \) such that \( \max\{r_1, r_2, r_3\} = O(N^{2/3}) \), Theorem 1.3.2 guarantees the existence of one cubic polynomial with \( O(N^{2/9}) \) coefficients. Now, we desire a second linearly independent \( O(N^{2/9}) \) cubic, however, sufficient conditions for its existence are unknown. We also conjecture that it suffices to have \( |r_1 - r_2|, |r_1 - r_3| = O(N^{1/2}) \) for Theorem 1.3.2 to guarantee the existence of
one cubic polynomial with $O(N^{1/6})$ coefficients, however it is unclear how to prove this or that the method presented below constructs two such polynomials.
CHAPTER 2
LINEAR ALGEBRA

Much of our work relies on the structures and operations presented in any Linear Algebra text. However, we do need to introduce a few additional concepts.

Definition 2.0.1. Let $n$ be a positive integer. A subset, $\mathcal{L}$, of the $n$-dimensional real vector space $\mathbb{R}^n$ is called a lattice if there exist linearly independent elements $b_1, b_2, \ldots, b_m$ of $\mathbb{R}^n$ such that

$$\mathcal{L} = \sum_{i=1}^{m} \mathbb{Z} b_i = \left\{ \sum_{i=1}^{m} r_i b_i, r_i \in \mathbb{Z} \right\}.$$

We say $b_1, b_2, \ldots, b_m$ form a basis for $\mathcal{L}$, or they span $\mathcal{L}$.

To simplify the notation for a lattice and its corresponding basis vectors we will use the following convention: a lattice $\mathcal{L}$ with basis $b_1, b_2, \ldots, b_m$, will be denoted

$$\mathcal{L} = \sum_{i=1}^{m} \mathbb{Z} b_i = \text{Col}_\mathbb{Z}(L),$$

where $L = (b_1 \ b_2 \ \cdots \ b_m)$ is the matrix with columns $b_1, b_2, \ldots, b_m$ and $\text{Col}_\mathbb{Z}(L)$ denotes the $\mathbb{Z}$-span of the columns of $L$.

For instance, if we consider the standard basis vectors in $\mathbb{R}^2$, $(1, 0)^\top$ and $(0, 1)^\top$, as a basis for a lattice

$$\mathcal{L} = \text{Col}_\mathbb{Z} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

we would simply obtain a $1 \times 1$ grid of vertices in $\mathbb{R}^2$, as shown in Figure 2.1.
Figure 2.1. Lattice with basis \{(0, 1)^T, (1, 0)^T\}

Alternatively, consider the basis vectors \((1, 3)^T\) and \((3, 4)^T\). The lattice generated by this basis appears in Figure 2.2.

Figure 2.2. Lattice with basis \{\((1, 3)^T, (3, 4)^T\)\}

Notice that the basis vectors \((1, 3)^T\) and \((3, 4)^T\) are quite long. In fact, the same lattice can be generated by the shorter vectors \((2, 1)^T\) and \((-1, 2)^T\) as seen in Figure 2.3.
Theorem 2.0.1. Let \( L \in \text{Mat}_{m \times n}(\mathbb{R}) \), then the lattice \( \mathcal{L} = \text{Col}_\mathbb{Z} L = \text{Col}_\mathbb{Z} L' \) if and only if \( L' = LU \) for some \( U \in \text{GL}(m, \mathbb{Z}) \).

Proof. First, suppose \( \text{Col}_\mathbb{Z} L = \text{Col}_\mathbb{Z} L' \), then there exists a \( U \in \text{Mat}_{m \times m}(\mathbb{Z}) \) such that \( L' = LU \). This can be seen if we consider \( L = (l_1 \ l_2 \ \cdots \ l_m) \), then \( l_i = L'x_i \). Let \( U = (x_1 \ x_2 \ \cdots \ x_m) \), then \( L' = LU \) as desired.

Similarly, there exists a \( U' \in \text{Mat}_{m \times m}(\mathbb{Z}) \) such that \( L = L'U' \). Therefore, we have \( L' = LU = (L'U')U = L'(U'U) \) and equivalently, \( 0 = L' - L'(U'U) = L'(I - U'U) \). Since \( L' \) is a basis for the lattice \( \mathcal{L} \), \( L' \) has full rank, so it is invertible; hence, we must have \( I - U'U = 0 \), or \( U'U = I \). Thus, \( U, U' \in \text{GL}(m, \mathbb{Z}) \) and so, \( L' = LU \) with \( U \in \text{GL}(m, \mathbb{Z}) \) as desired.

On the other hand, suppose \( L' = LU \) for some \( U \in \text{GL}(m, \mathbb{Z}) \). Let \( a \in \text{Col}_\mathbb{Z} L' \), then \( a = L'x \) for some \( x \in \mathbb{Z}^m \), and it follows \( a = L'x = LUX \). Since \( U \in \text{GL}(m, \mathbb{Z}) \), we have \( UX = y \in \mathbb{Z}^m \). Hence, \( a = LUX = Ly \), so \( a \in \text{Col}_\mathbb{Z} L \) and \( \text{Col}_\mathbb{Z} L' \subseteq \text{Col}_\mathbb{Z} L \).

Now, let \( b \in \text{Col}_\mathbb{Z} L \), then \( b = Lw \) for some \( w \in \mathbb{Z}^m \). Since \( U \in \text{GL}(m, \mathbb{Z}) \), \( U^{-1} \in \text{GL}(m, \mathbb{Z}) \) exists, hence \( L = L'U^{-1} \). Thus, \( b = Lw = L'U^{-1}w \), and \( U^{-1}w = z \in \mathbb{Z}^m \) so \( b = Lw = L'U^{-1}w = L'z \). Therefore, \( b \in \text{Col}_\mathbb{Z} L' \), implying \( \text{Col}_\mathbb{Z} L \subseteq \text{Col}_\mathbb{Z} L' \). \( \square \)

Definition 2.0.2. If \( \mathcal{L} = \text{Col}_\mathbb{Z}(L) \) is a lattice then the discriminant of \( \mathcal{L} \) denoted \( d(\mathcal{L}) \) is defined by

\[
d(\mathcal{L}) = \sqrt{\text{det}(L^\top L)}.\]
Clearly, if $L$ is square then $d(L) = \sqrt{\det(L^\top L)} = \sqrt{\det(L^\top) \det(L)} = \sqrt{\det(L)^2} = \det(L)$. Now, if there exist $L, L' \in \text{Mat}_{m \times n}(\mathbb{R})$ such that $m \neq n$ and $\text{Col}_Z L = L = \text{Col}_Z L'$ then $L' = LU$ for some $U \in \text{GL}(m, \mathbb{Z})$ as shown in Theorem 2.0.1. Hence, $\det((L')^\top L') = \det((U^\top L^\top)LU) = \det(U^\top) \det(L^\top L) \det(U) = \det(L^\top L) [\det(U)]^2$. Since $U \in \text{GL}(m, \mathbb{Z})$, we know $\det(U) = \pm 1$, thus $\det((L')^\top L) = \det(L^\top L)$. Therefore, we have that $d(L)$ is well defined.
In our effort to improve the practical efficiency of the Number Field Sieve we would like to find two coprime, irreducible polynomials with “small” coefficients, sharing a common root modulo $N$, the number we wish to factor. Where “small” is relative to the size of $N$. If we interpret the coefficients of an $n^{th}$-degree polynomial as an $n$-dimensional vector, the task of finding “small” coefficients is equivalent to finding a “short” vector. Ideally, we would like our vector to be as short as possible, however this task, aptly named “The Shortest Vector Problem”, has been well studied and is known to be an NP-hard problem [5].

In 1982, an algorithm was developed by Arjen Lenstra, Hendrik Lenstra and László Lovász which provides a method for efficiently finding vectors “very close” to the shortest vector [6]. This algorithm, which is known as the LLL-Algorithm, runs in polynomial time [6]. In fact, if given as input $d$, $n$-dimensional basis vectors, $b_1, b_2, \ldots, b_d$ for a lattice $\mathcal{L} \in \mathbb{R}^n$ with $d \leq n$, and $B$ an upper bound on the norms of the $b_i$’s, the algorithm runs in time $O(d^5 n \log^3 B)$ [10].

We will now describe a few results which will be needed in Chapter 4 – Polynomial Selection. The included theorems have been taken from [6], with adaptations found in [3].

**The Gram-Schmidt Process.** Let $b_1, b_2, \ldots, b_n \in \mathbb{R}^n$ be a basis of the vector space $V$. Define inductively the vectors $b_i^*$ for $1 \leq i \leq n$, and the real numbers $\mu_{i,j}$ for $1 \leq j < i \leq n$ as follows:

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*,$$

$$\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle},$$

where $\langle \cdot, \cdot \rangle$ denotes the ordinary inner product on $\mathbb{R}^n$. Then, $b_1^*, b_2^*, \ldots, b_n^*$ is an orthonormal basis of $V$.

We will call a basis $b_1, b_2, \ldots, b_n$ for a lattice $\mathcal{L}$ **reduced** if

$$|\mu_{i,j}| \leq \frac{1}{2} \quad \text{for} \quad 1 \leq j < i \leq n,$$
and

\[ |b_i^* + \mu_{i-1} b_{i-1}^*|^2 \geq \frac{3}{4} |b_{i-1}^*|^2 \quad \text{for} \quad 1 < i \leq n, \]

where \(| \cdot |\) denotes the ordinary Euclidean length.

**Theorem 3.0.1.** Let \( b_1, b_2, \ldots, b_n \) be a reduced basis for a lattice \( \mathcal{L} \) in \( \mathbb{R}^n \) then

\[
d(\mathcal{L}) \leq \prod_{i=1}^{n} |b_i| \leq 2^{n(n-1)/4} d(\mathcal{L}).
\]

**Corollary 3.0.1.** Let \( b_1, b_2, \ldots, b_m \) be a reduced basis for a lattice \( \mathcal{L} \) in \( \mathbb{R}^n \) with \( m \leq n \) then

\[
d(\mathcal{L}) \leq \prod_{i=1}^{m} |b_i| \leq 2^{n(n-1)/4} d(\mathcal{L}).
\]

**Sketch of Proof.** Define recursively basis vectors \( b_i \) for \( i = m + 1, \ldots, n \) such that \( b_i \) is a unit vector in the orthogonal complement of the subspace generated by \( b_1 \cdots b_{i-1} \). The desired result follows by applying Theorem 3.0.1. \( \square \)

We mentioned above that the LLL-algorithm finds vectors “very close” to the shortest vector. The notion of “very close” is explicitly given in the following theorem.

**Theorem 3.0.2.** Let \( \mathcal{L} \subset \mathbb{R}^n \) be a lattice with reduced basis \( b_1, b_2, \ldots, b_n \). Let \( x_1, x_2, \ldots, x_t \in \mathcal{L} \) be linearly independent. Then

\[
|b_j| \leq 2^{(n-1)/2} \max(|x_1|, \ldots, |x_t|), \text{ for } 1 \leq j \leq t.
\]
CHAPTER 4
POLYNOMIAL SELECTION

One method of constructing polynomials for the Number Field Sieve is to define
\( f_1(x) = x - m \) and \( f_2(x) = c_0 + c_1x + \cdots + c_dx^d \) with \( m \in \mathbb{Z} \) where \( c_dm^d + \cdots + c_1m + c_0 \) is
the base-\( m \) representation of \( N \). Note, \( m \) will be the common root of \( f_1 \) and \( f_2 \). However, if
we choose \( f_1 \) and \( f_2 \) in this manner there is an obvious imbalance in \( ||f_1|| \) and \( ||f_2|| \) as
observed in [8] and [4]. Also, in [1] it was shown, not only is there an imbalance in norm
size, but in fact choosing reasonably higher degree polynomials improves the practical
efficiency of the Number Filed Sieve. Consequently, we provide a method for constructing
two coprime, irreducible \( O(N^{1/4}) \) quadratics \( f_1 \) and \( f_2 \) with a common root modulo \( N \), and
two coprime, irreducible \( O(N^{2/9}) \) cubics \( g_1 \) and \( g_2 \) with a common root modulo \( N \).

Note that in practice it does not matter if \( ||f_1|| \) and \( ||f_2|| \) are both \( O(N^{1/4}) \).
Computationally, what matters is that \( ||f_1|| \cdot ||f_2|| = O(N^{2/4}) = O(N^{1/2}) \). This also occurs for
\( O(N^{2/9}) \) cubics, it is not necessary for both \( ||g_1||, ||g_2|| = O(N^{2/9}) \), but that their product be
\( O(N^{4/9}) \). Hence, without loss of generality, we will consider both of our cubics to be
roughly the same size, but we keep in mind that this need not be the case.

4.1 Equivalence Class and Lattice Correspondence
To apply the LLL-algorithm to the problem at hand, we first relate solutions of the
equation \( a_0 + a_1r + \cdots + a_br^b \equiv 0 \pmod{N} \) to the column space of a matrix. This will
allow us to relate our polynomials to points on a lattice and invoke the LLL-algorithm.
The necessary relation is given in the following theorem.

**Theorem 4.1.1.** Let \( N,k \in \mathbb{Z}^+ \) and \( r \in \mathbb{R} \) with \( r \geq 1 \), and \( k \geq 0 \). If
\( z(k,r,N) = \{(a_0,a_1,\ldots,a_k)^\top \in \mathbb{Z}^{k+1} : a_0 + a_1r + a_2r^2 + \cdots + a_br^b \equiv 0 \pmod{N}\}, \) and
\[
A_{k,r,N} = \begin{pmatrix}
-r & -r^2 & \cdots & -r^k & N \\
1 & 0 & \cdots & 0 & 0 \\
0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & 0
\end{pmatrix}.
\]

Then \( \text{Col}_\mathbb{Z} A_{k,r,N} = z(k,r,N) \).
Proof. Let $a \in \text{Col}_\mathbb{Z} A_{k,r,N}$, then

$$
\begin{pmatrix}
    a_0 \\
    a_1 \\
    \vdots \\
    a_k
\end{pmatrix} = \begin{pmatrix}
    -r & -r^2 & \cdots & -r^k & N \\
    1 & 0 & \cdots & 0 & 0 \\
    0 & 1 & \cdots & 0 & 0 \\
    \vdots & \vdots & \ddots & \vdots & \vdots \\
    0 & 0 & \cdots & 1 & 0
\end{pmatrix} \begin{pmatrix}
    x_1 \\
    x_2 \\
    \vdots \\
    x_{k+1}
\end{pmatrix},
$$

for some $x_1, x_2, \ldots, x_{k+1} \in \mathbb{Z}$.

Hence,

$$
\begin{align*}
    a_0 &= -x_1 r - x_2 r^2 - \cdots - x_k r^k + x_{k+1} N, \\
    a_1 &= x_1, \\
    a_2 &= x_2, \\
    \vdots &= \vdots \\
    a_k &= x_k.
\end{align*}
$$

Therefore, $a_0 = -a_1 r - a_2 r^2 - \cdots - a_k r^k + x_{k+1} N$, or equivalently,

$a_0 + a_1 r + a_2 r^2 + \cdots + a_k r^k = x_{k+1} N$; implying that

$a_0 + a_1 r + a_2 r^2 + \cdots + a_k r^k \equiv 0 \pmod{N}$. Thus, $\text{Col}_\mathbb{Z} A_{k,r,N} \subseteq \mathbb{Z}(k, r, N)$.

Now, suppose $(a_0, a_1, \ldots, a_k)^\top \in \mathbb{Z}(k, r, N)$. Then

$a_0 + a_1 r + a_2 r^2 + \cdots + a_k r^k \equiv 0 \pmod{N}$; thus $a_0 + a_1 r + a_2 r^2 + \cdots + a_k r^k = x_{k+1} N$ for some $x_{k+1} \in \mathbb{Z}$, so $a_0 = -a_1 r - a_2 r^2 - \cdots - a_k r^k + x_{k+1} N$. Let $a' = (a_1, a_2, \ldots, a_k, x_{k+1})^\top$. Then

$$
\begin{pmatrix}
    a_0 \\
    a_1 \\
    \vdots \\
    a_k
\end{pmatrix} = \begin{pmatrix}
    -r & -r^2 & \cdots & -r^k & N \\
    1 & 0 & \cdots & 0 & 0 \\
    0 & 1 & \cdots & 0 & 0 \\
    \vdots & \vdots & \ddots & \vdots & \vdots \\
    0 & 0 & \cdots & 1 & 0
\end{pmatrix} \begin{pmatrix}
    a_1 \\
    a_2 \\
    \vdots \\
    a_k \\
    x_{k+1}
\end{pmatrix} = A_{k,r,N} a' \text{ with } a' \in \mathbb{Z}^{k+1},
$$

so $(a_0, a_1, \ldots, a_k)^\top \in \text{Col}_\mathbb{Z} A_{k,r,N}$. Hence, $\mathbb{Z}(k, r, N) \subseteq \text{Col}_\mathbb{Z} A_{k,r,N}$. \hfill \blacksquare

Now let us focus our attention to specifically consider the polynomials spanned by the same basis vectors and exclude $(N, 0, \cdots)^\top$. Notice, we lose any polynomial that have been translated by a factor of $N$, since we are no longer considering the vector $(N, 0, \cdots)^\top$ as part of our basis. However, this is of no great concern, since any of the polynomials we lose can easily be recovered simply by adding multiples of $N$ onto our polynomials in the
span of our new basis. These polynomials will obviously still have a solution to the equation \( f(x) \equiv 0 \pmod{N} \).

We now may proceed by using this equivalence class and lattice correspondence.

4.2 Construction of \( O(N^{1/4}) \) Quadratics

In 2006, Peter Montgomery gave one method for producing two \( O(N^{1/4}) \) quadratics with a common root modulo \( N \) by using geometric progressions and vector cross products [9]. Montgomery’s method was also described in much further detail in [4]. We now provide a different method of constructing such quadratics using the LLL-algorithm.

Given \( N \in \mathbb{Z}^+ \), define \( r_1 \) and \( r_2 \) as follows,

\[
\begin{align*}
  r_1 &= \left\lfloor \frac{N^{1/2}}{2} \right\rfloor + k \quad \text{with } |k| \text{ “small”,} \\
  r_2 &\equiv r_1^2 \pmod{N},
\end{align*}
\]

with the \( r_i \)'s taken to satisfy \(-\frac{N}{2} < r_i < \frac{N}{2}\). Throughout, let \( \lfloor \cdot \rfloor \) denote the greatest-integer function. Then we have \( r_1 = N^{1/2} - \epsilon + k = O(N^{1/2}) \) with \( 0 \leq \epsilon < 1 \), so

\[
\begin{align*}
  r_1^2 &= N - 2\epsilon N^{1/2} + \epsilon^2 + 2kN^{1/2} + k^2 - 2ek. \\
  r_2 &\equiv r_1^2 \equiv N^{1/2}(2k - 2\epsilon) + \epsilon^2 - 2ek + k^2 \pmod{N},
\end{align*}
\]

so \( r_2 = O(N^{1/2}) \).

**Theorem 4.2.1.** Let \( N \in \mathbb{Z}^+ \) and \( \mathcal{L} = \text{Col}_\mathbb{Z}(L) \) where

\[
L = \begin{pmatrix} r_1 & r_2 \\ -1 & 0 \\ 0 & -1 \end{pmatrix},
\]

and \( |r_1|, |r_2| \leq \alpha N^{1/2} \). If \( \mathbf{b}_1 \) and \( \mathbf{b}_2 \) form an LLL-reduced basis for a lattice \( \mathcal{L} \) then \( \|\mathbf{b}_1\| \cdot \|\mathbf{b}_2\| \leq 2^{5/2} \alpha N^{1/2} \).

**Proof.** First, we have

\[
L^T L = \begin{pmatrix} r_1^2 + 1 & r_1 r_2 \\ r_1 r_2 & r_2^2 + 1 \end{pmatrix},
\]

so

\[
\det(L^T L) = (r_1^2 + 1)(r_2^2 + 1) - r_1^2 r_2^2 = r_1^2 + r_2^2 + 1.
\]
Hence, \( d(L) = \sqrt{\det(L^*L)} = \sqrt{r_1^2 + r_2^2 + 1} \). Since \(|r_1|, |r_2| \leq \alpha N^{1/2} \) we have

\[
d(L) = \sqrt{r_1^2 + r_2^2 + 1} \leq \sqrt{(\alpha N^{1/2})^2 + (\alpha N^{1/2})^2 + 1} = (2\alpha^2 N + 1)^{1/2} \leq (4\alpha^2 N)^{1/2} = 2\alpha N^{1/2}.
\]

It follows by Corollary 3.0.1,

\[
d(L) \leq \|b_1\| \cdot \|b_2\| \leq 2^{3/2}d(L) \leq 2^{3/2}(2\alpha N^{1/2}) = 2^{5/2}\alpha N^{1/2}.
\]

Thus, the quadratics formed using the entries of \( b_1 \) and \( b_2 \) for coefficients will have the common root \( r \) modulo \( N \), and the product of coefficient norms of these quadratics will be \( O(N^{1/2}) \).

4.3 Construction of \( O(N^{2/9}) \) Cubics

We now proceed to construct two \( O(N^{2/9}) \) cubics similarly to the construction of the \( O(N^{1/4}) \) quadratics.

Given \( N \in \mathbb{Z}^+ \), define \( r_1, r_2 \) and \( r_3 \) as follows,

\[
r_1 = \left[N^{1/3}\right] + k \quad \text{with} \quad |k| \text{ “small”},
\]

\[
r_2 \equiv r_1^2 \pmod{N},
\]

\[
r_3 \equiv r_1^3 \pmod{N},
\]

18
with the $r_i$'s taken to satisfy $\frac{-N}{2} < r_i < \frac{N}{2}$. Then we have

$$
\begin{align*}
    r_1 &= N^{1/3} - \epsilon + k = O(N^{2/3}) \quad \text{with } 0 \leq \epsilon < 1, \\
    r_1^2 &= N^{2/3} - 2\epsilon N^{1/3} + 2kN^{1/3} + \epsilon^2 - 2\epsilon k + k^2 = O(N^{2/3}), \\
    r_1^3 &= N - 3\epsilon N^{2/3} + 3kN^{2/3} + 3\epsilon^2 N^{1/3} - 6\epsilon kN^{1/3} + 3k^2 N^{1/3} - \epsilon^3 + 3\epsilon^2 k - 3\epsilon k^2 + k^3 \\
    &= N + N^{2/3}(3k - 3\epsilon) + N^{1/3}(3\epsilon^2 - 6\epsilon k + 3k^2) - \epsilon^3 + 3\epsilon^2 k - 3\epsilon k^2 + k^3.
\end{align*}
$$

Hence, it is clear that modulo $N$, $r_2$ and $r_3$ are $O(N^{2/3})$ as well. Then we have the following theorem.

**Theorem 4.3.1.** Let $N \in \mathbb{Z}^+$ and $\mathcal{L} = \text{Col}_z(L)$ where

$$
L = \begin{pmatrix}
    r_1 & r_2 & r_3 \\
    -1 & 0 & 0 \\
    0 & -1 & 0 \\
    0 & 0 & -1
\end{pmatrix}.
$$

and $|r_1|, |r_2|, |r_3| \leq \alpha N^{2/3}$. If $b_1, b_2$ and $b_3$ form an LLL-reduced basis for a lattice $\mathcal{L}$ then $\|b_i\| \cdot \|b_j\| \leq 2^{11/3} \alpha^{2/3} N^{4/9}$, for some $i, j \in \{1, 2, 3\}$ with $i \neq j$.

**Proof.** First, notice that

$$
L^T L = \begin{pmatrix}
    r_1^2 + 1 & r_1 r_2 & r_1 r_3 \\
    r_1 r_2 & r_2^2 + 1 & r_2 r_3 \\
    r_1 r_3 & r_2 r_3 & r_3^2 + 1
\end{pmatrix},
$$

so

$$
\det(L^T L) = (r_1^2 + 1)((r_2^2 + 1)(r_3^2 + 1) - (r_2 r_3)(r_2 r_3)) \\
- (r_1 r_2)((r_1 r_2)(r_2^2 + 1) - (r_2 r_3)(r_1 r_3)) \\
+ (r_1 r_3)((r_1 r_2)(r_2 r_3) - (r_2^2 + 1)(r_1 r_3)) \\
= (r_1^2 + 1)(r_2^2 + r_3^2 + 1) - (r_1 r_2)(r_1 r_2) - (r_1 r_3)(r_1 r_3) \\
= r_1^2 + r_2^2 + r_3^2 + 1.
$$
Therefore, $d(L) = \sqrt{\det(L^T L)} = \sqrt{r_1^2 + r_2^2 + r_3^2 + 1}$. Since $|r_1|, |r_2|, |r_3| \leq \alpha N^{2/3}$ it follows

$$d(L) = \sqrt{r_1^2 + r_2^2 + r_3^2 + 1} \leq \sqrt{(\alpha N^{2/3})^2 + (\alpha N^{2/3})^2 + (\alpha N^{2/3})^2 + 1}$$

$$= (3\alpha^2 N^{4/3} + 1)^{1/2} \leq (4\alpha^2 N^{4/3})^{1/2} = 2\alpha N^{2/3}.$$

Using the bounds from Corollary 3.0.1 we have

$$d(L) \leq ||b_1|| \cdot ||b_2|| \cdot ||b_3|| \leq 2^3 d(L).$$

Without loss of generality, we may assume $||b_3|| \geq d(L)^{1/3}$. Thus, we have

$$\frac{||b_1|| \cdot ||b_2||}{||b_3||} \leq \frac{2^3 d(L)}{d(L)^{1/3}} = 2^3 d(L)^{2/3} \leq 2^3 (2\alpha N^{2/3})^{2/3}$$

$$= 2^{2/3} \alpha^{2/3} N^{4/9}$$

$$= 2^{11/3} \alpha^{2/3} N^{4/9}.$$

Hence, with our chosen $r_1, r_2$ and $r_3$, Theorem 4.2.2 gives us $||b_1|| \cdot ||b_2|| = O(N^{4/9})$ and as mentioned above we may assume, without loss of generality, $||b_1||, ||b_2|| = O(N^{2/9}).$

Since the $b_i$’s are simply a change of basis from the original basis vectors of $L$, Theorem 4.2.1 tells us that $b_{11} + b_{12} r_1 + b_{13} r_1^2 + b_{14} r_1^3 \equiv 0 \pmod{N}$ and

$b_{21} + b_{22} r_1 + b_{23} r_1^2 + b_{24} r_1^3 \equiv 0 \pmod{N}$ where $b_i = (b_{i1}, b_{i2}, b_{i3}, b_{i4})$ for $i = 1, 2$. Therefore, we have shown there exist two cubic polynomials, with a common root modulo $N$, whose norms of coefficients have a product of $O(N^{4/9})$. 

□
CHAPTER 5
EXAMPLES

Let
\[ N = 45671760398941087043587521606556281920349273069698283977390\]
\[ 74346628988327155475222843793393 ,\]
we have that \( \log_{10} N \approx 90.66 \), and so \( N \) has 91 digits.

5.1 \( O(N^{1/4}) \) Quadratics

Define \( r_1 = \left\lfloor N^{1/2} \right\rfloor \) and \( r_2 \equiv r_1^2 \) (mod \( N \)), then
\[ r_1 = 2137095234165784363995092720634079799836426483, \]
\[ r_2 = -75430630543476127971378133018032127380044104, \]
with \( \log_{10} r_1 \approx 45.33 \) and \( \log_{10} r_2 \approx 43.88 \). Since \( N^{1/2} \) will have approximately 45 digits, \( r_1 \) and \( r_2 \) are roughly the same size as \( N^{1/2} \).

Now, define a lattice \( \mathcal{L} = \text{Col}_2(L) \) where
\[ L = \begin{pmatrix} r_1 & r_2 \\ -1 & 0 \\ 0 & -1 \end{pmatrix} . \]

Performing the LLL Algorithm on \( L \) we obtain a LLL-reduced basis \( b_1 \) and \( b_2 \), with \( B = (b_1 \ b_2) \), for \( \mathcal{L} \):
\[ B = \begin{pmatrix} 12484337953248623322139 & -54330406087511693205427 \\ -1153466329877377424353 & -1022267779097210978607 \\ -32679925629560330284215 & -28962817664512286576602 \end{pmatrix} . \]
Thus we have

\[ f_1 := 12484337953248623322139 - 115346632987777424353r_1 - 32679925629560330284215r_1^2 \equiv 0 \pmod{N}, \]

and

\[ f_2 := -54330406087511693205427 - 1022267779097210978607r_1 - 2896281764512286576602r_1^2 \equiv 0 \pmod{N}. \]

Calculating the norms of the coefficient vectors of \( f_1 \) and \( f_2 \) we obtain

\[ ||f_1|| \approx 35002381602666395733248 \text{ and } ||f_2|| \approx 61576642195835044877593. \]

So, \( ||f_1|| \cdot ||f_2|| \approx 2155329127949467867477348796786844573640312064 \text{ and } \log_{10}(||f_1|| \cdot ||f_2||) \approx 45.33 \text{ with } \log_{10}N^{1/2} \approx 45.33. \)

5.2 \( O(N^{2/3}) \) Cubics

Define \( r_1 = \left[ N^{1/3} \right] + 1, r_2 \equiv r_1^2 \pmod{N}, \text{ and } r_3 \equiv r_1^3 \pmod{N}, \) so we have

\[ r_1 = 1659138281147271980794587079218, \]
\[ r_2 = 27527398359683241231316814777642879140250720497401922074\]
\[ \quad 91524, \]
\[ r_3 = 62257985549129555436382746887045948041709874346586508077\]
\[ \quad 54839, \]

with \( \log_{10}r_1 \approx 30.22, \log_{10}r_2 \approx 60.44 \) and \( \log_{10}r_3 \approx 60.79. \) Since \( N^{2/3} \) has approximately 60 digits \( r_1, r_2 \) and \( r_3 \) are all roughly the same size as \( N^{2/3}. \)

Now we define a lattice, \( \mathcal{L} = \text{Col}_2(L), \) where

\[
L = \begin{pmatrix}
  r_1 & r_2 & r_3 \\
-1 & 0 & 0 \\
0 & -1 & 0 \\
0 & 0 & -1
\end{pmatrix}.
\]
The LLL Algorithm performed on $L$ to obtain an LLL-reduced basis $b_1, b_2$ and $b_3$, with $B = (b_1 b_2 b_3)$ for $L$:

$$B = \begin{pmatrix}
-98228473793261830482 & 88601408057407884491 & 53500889367358105108 \\
9743458171161776159 & 161279695637696264892 & -154799413463330414830 \\
20270774434332188756 & 141413847455697130658 & 221261060999008882603 \\
-8962732699933084116 & -6256200906654277101 & -97830684913496159260
\end{pmatrix}.$$

Thus we have

$$f_1 := -98228473793261830482 + 9743458171161776159r_1 + 20270774434332188756r_1^2 - 8962732699933084116r_1^3 \equiv 0 \pmod{N},$$

and

$$f_2 := 88601408057407884491 + 161279695637696264892r_1 + 141413847455697130658r_1^2 - 6256200906654277101r_1^3 \equiv 0 \pmod{N}.$$

Calculating the norms of the coefficient vectors of $f_1$ and $f_2$, we obtain $||f_1|| = 101168191218904030906$ and $||f_2|| = 240351309101460311537$. So we see,$||f_1|| \cdot ||f_2|| = 24315907198890445572338346693427836362522$ and $\log_{10}(||f_1|| \cdot ||f_2||) \approx 40.39$ with $\log_{10}N^{4/9} \approx 40.29$.

Had we used a common method of polynomial selection, for instance, $g_1(x) = x - r$ and $g_2(x) = c_d x^d + \cdots + c_1 x + c_0$, where $c_d r^d + \cdots + c_1 r + c_0$ is the base-$r$ representation of $N$, we could have obtained the following pairs of polynomials. For a linear and a cubic polynomial pick $r = 46228727369091444241658 \approx N^{1/4}$, then

$$g_1(x) = x - 46228727369091444241658,$$

$$g_2(x) = 46228727369091444241655r^3 + 16865200394060600400013r^2 + 35657985555376054828676r + 221447468030237345693.$$
For a linear and a quintic polynomial pick \( r = 1354969596273877205 \approx N^{1/5} \), then

\[
\begin{align*}
    h_1(x) &= x - 1354969596273877205, \\
    h_2(x) &= 1354969596273877200r^4 + 1036564656970223895r^3 \\
    &\quad + 1310231758085038208r^2 + 1353325192992913241r \\
    &\quad + 947436200777683913. 
\end{align*}
\]

Thus \( \|g_1\| \approx 46228727369091444241658 \) and \( \|g_2\| \approx 60770644157735489411999 \),
giving \( \|g_1\| \cdot \|g_2\| \approx 2809349540812023697913160178264464736880854342 \),
and hence \( \log_{10}(\|g_1\| \cdot \|g_2\|) \approx 45.45 \). Also, we have \( \|h_1\| \approx 1354969596273877205 \) and
\( \|h_2\| \approx 2712239035803142378 \), so
\( \|h_1\| \cdot \|h_2\| \approx 3675001431340433809866798852703693490 \), and hence
\( \log_{10}(\|h_1\| \cdot \|h_2\|) \approx 36.57 \).

Notice as the degree of the polynomials increase, even with the common method, there is a reduction in norm size. However, recall from Section 1.2 that the coefficients of our polynomials are not the only factor in determining the runtime of the Number Field Sieve. So, as the degree of our polynomials increase, the coefficients do decrease, however in this case, the runtime of the sieve is largely influenced by the degree. Hence, our polynomials provide both small degree and coefficients, and will therefore require less runtime than the common method with high degree polynomials.

Thus, our method has produced two coprime, irreducible cubic polynomials with product of coefficient vector norms are roughly the same size as \( N^{4/9} \).

Using either of the above pair of polynomials in the Number Field Sieve we would find \( N = pq \) where

\[
\begin{align*}
    p &= 3746040568309680732803673837072688430073910417, \\
    q &= 1219200902021984102438498732411383778193048929, 
\end{align*}
\]

thereby achieving our goal of factoring the large integer \( N \).
Thus, we have provided methods for the construction of two $O(N^{1/2})$ quadratics and two $O(N^{2/9})$ cubics. If it were possible to find $r_1, r_2, r_3 = O(N^{1/2})$, our method would produce two $O(N^{1/6})$ cubics. However, in practice, finding such $r_i$'s is a rarity. What generally does seem to occur is that there exist $r_1, r_2, r_3$ such that $|r_1 - r_2| < \alpha N^{1/2}$ and $|r_1 - r_3| < \beta N^{1/2}$, with small $\alpha, \beta \in \mathbb{R}^+$, for which two $O(N^{1/6})$ cubics can be formed. It is, however, left unproven that this LLL-based method with such $r_i$'s produces these $O(N^{1/6})$ cubics.
BIBLIOGRAPHY


