A Beginner's Guide To The General Number Field Sieve

Michael Case
Oregon State University, ECE 575
case@engr.orst.edu

Abstract

RSA is a very popular public key cryptosystem. This algorithm is known to be secure, but this fact relies on the difficulty of factoring large numbers. Because of the popularity of the algorithm, much research has gone into this problem of factoring a large number.

The size of the number that we are able to factor increases exponentially year by year. This fact is partly due to advancements in computing hardware, but it is largely due to advancements in factoring algorithms. The General Number Field Sieve is an example of just such an advanced factoring algorithm. This is currently the best known method for factoring large numbers.

This paper is a presentation of the General Number Field Sieve. It begins with a discussion of the algorithm in general and covers the theory that is responsible for its success. Because often the best way to learn an algorithm is by applying it, an extensive numerical example is included as well.

I. Introduction

The General Number Field Sieve is an algorithm for factoring very large numbers. Factoring is very important in the field of cryptography, specifically in the RSA cryptosystem.

The Rivest, Shamir, Adleman (RSA) cryptosystem is a scheme for encrypting and decrypting messages, and its security relies on the fact that factoring large composite numbers is a very hard, computationally intensive task. The RSA algorithm works in the following way:

- Choose two large primes p and q. Set $n = pq$.
- Choose a random e satisfying $1 \leq e < n$.
- Set $d = e^{-1} \pmod{(p-1)(q-1)}$.
- A message m is encrypted to $c \equiv m^e \pmod{n}$. Note that only e and n were needed to compute c. e and n are known as the public key and are public information.

- An encrypted message e is decrypted by evaluating $e^d \pmod{n} = m$. Because d can decrypt messages, it should be kept secret. d is known as the secret key.

This system can be broken by factoring n into p and q. If n is factored then $(p-1)(q-1)$ can be found and from this d can be computed. Therefore, any adversary that factors n can find the private key d and with it decrypt any encrypted message.

Because the security of RSA is so dependent on an adversary's inability to factor a large composite number, much research has been done to find ways to quickly factor such numbers.

The Number Field Sieve (NFS) is the fruit of that research. This is an algorithm for factoring composite numbers that is currently the best known method for factoring numbers over 100 digits. The NFS has two common variations: the Special Number Field Sieve (SNFS) and the General Number Field Sieve (GNFS). The SNFS is an algorithm that can quickly factor large numbers but works only for numbers of a special form. The GNFS works for all composite numbers, but this flexibility is at the cost of the GNFS being slightly slower than the SNFS. However, because of its increased flexibility, the GNFS is the method of choice in many factoring challenges. For this reason, it is the GNFS that will be examined in this paper.

II. The GNFS Algorithm

A. The Difference of Squares Factorization Method

Suppose that one wants to factor a composite number n, and for two numbers $s, r \in \mathbb{Z}$, $s^2 \equiv r^2 \pmod{n}$. Then $s^2 - r^2 \equiv 0 \pmod{n}$. Suppose n has the prime factorization $n = pq$. Then

$$\begin{aligned} & pq \mid \left(s^2 - r^2\right) \\ \implies & pq \mid (s-r)(s+r) \\ \implies & p \mid (s-r)(s+r) \text{ and } q \mid (s-r)(s+r) \end{aligned}$$

A standard result from number theory states that if $c \mid ab$ and $\gcd(b, c) = 1$ then $c \mid a$. This implies that the following conditions must hold:

$$\begin{cases} p \mid (s+r) \text{ or } p \mid (s-r) \\ q \mid (s+r) \text{ or } q \mid (s-r) \end{cases}$$

The above implies that it is not possible that $p \nmid (s+r)$ and $p \nmid (s-r)$. Similarly, it is not possible that $q \nmid (s+r)$ and $q \nmid (s-r)$. Table I summarizes the possibilities for p and q dividing $s+r$ and $s-r$.

As an example of how to read Table I, suppose $p \mid (s+r)$, $p \mid (s-r)$, $q \nmid (s+r)$, and $q \mid (s-r)$. $\gcd(pq, s+r) \in \{1, p, q, pq\}$, the divisors of $n = pq$. Since $p \mid (s+r)$, $p \mid \gcd(pq, s+r)$. Now,

TABLE I

POSSIBILITIES FOR p AND q DIVIDING $s+r$ AND $s-r$

Possible Divisibility Scenarios				**GCD Results**		
$p \mid (s+r)$	$p \mid (s-r)$	$q \mid (s+r)$	$q \mid (s-r)$	$\gcd(pq, s+r)$	$\gcd(pq, s-r)$	Successful Factorization
No	Yes	No	Yes	0	pq	
No	Yes	Yes	No	q	p	$\star$
No	Yes	Yes	Yes	q	pq	$\star$
Yes	No	No	Yes	p	q	$\star$
Yes	No	Yes	No	pq	0	
Yes	No	Yes	Yes	pq	q	$\star$
Yes	Yes	No	Yes	p	pq	$\star$
Yes	Yes	Yes	No	pq	p	$\star$
Yes	Yes	Yes	Yes	pq	pq	

$pq \nmid (s+r)$ because $q \nmid (s+r)$ and hence the only value that $\gcd(pq, s+r)$ can assume is p. Similarly, $\gcd(pq, s-r) = pq$ because both $p \mid (s-r)$ and $q \mid (s-r)$. Because one of the gcd's was able to isolate either p or q, this scenario led to a successful factorization of $n = pq$.

If it is assumed that all of the combinations in Table I are equally likely then $s^2 \equiv r^2 \pmod{n}$ implies that either $\gcd(pq, s+r)$ or $\gcd(pq, s-r)$ gives a nontrivial factor of $n = pq$ with probability $2/3$.

Although it is not guaranteed that having $s^2 \equiv r^2 \pmod{n}$ will give a nontrivial factor of n, due to this high probability, one would not expect to have to find many pairs s, r satisfying $s^2 \equiv r^2 \pmod{n}$ in order to factor n.

B. Free Parameters in the GNFS

The GNFS algorithm includes two free parameters that must be chosen to meet certain criteria. These free variables will be used throughout the derivation of the GNFS along with a composite integer n that is to be factored. The first such parameter is a polynomial $f : \mathbb{R} \to \mathbb{R}$ with integer coefficients, and the second parameter is a natural number $m \in \mathbb{N}$ that satisfies $f(m) \equiv 0 \pmod{n}$.

In practice, finding f and m such that the above hold is a simple matter so long as m is chosen first. Consider the base-m expansion of n.

$$n = a_d m^d + a_{d-1} m^{d-1} + \ldots + a_0$$

By defining the function f as

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0$$

$f(m) = n$. Therefore $f(m) \equiv 0 \pmod{n}$, and so f and m meet the above criteria. Let f, m, and the composite n be given throughout this document.

C. The Ring $\mathbb{Z}[\theta]$

The GNFS works because of the properties of a ring called $\mathbb{Z}[\theta]$. This ring will now be explained.

Let $\theta \in \mathbb{C}$ be a (possibly complex) root of the polynomial f from Section II-B. Let d be the degree of the polynomial f. The space $\mathbb{Z}[\theta]$ is defined as follows.

$$\mathbb{Z}[\theta] = \left\{ x : x = a_{d-1}\theta^{d-1} + a_{d-2}\theta^{d-2} + \ldots + a_0 \text{ for } \{a_j\} \subset \mathbb{Z} \right\}$$

Theorem 2.1: With multiplication defined as the normal polynomial multiplication, $\mathbb{Z}[\theta]$ forms a ring.

The definition of this ring causes some strange behavior when elements are multiplied. To see this, let $A, B \in \mathbb{Z}[\theta]$. Let $a(x)$ and $b(x)$ be two polynomials such that $a(\theta) = A$ and $b(\theta) = B$.

By the division algorithm, $a(x)b(x) = e(x)f(x) + c(x)$ where $e(x)$ and $c(x)$ are two polynomials with integer coefficients and the degree of $c(x)$ is less than the degree of f. Define $C = c(\theta)$.

$$\begin{aligned} AB &= a(x)b(x)\Big|_{x=\theta} \\ &= e(x)f(x)\Big|_{x=\theta} + c(x)\Big|_{x=\theta} \\ &= e(\theta)f(\theta) + C \\ &= e(\theta) \cdot 0 + C \\ &= C \end{aligned}$$

Note that by construction, the degree of C is less than the degree d of f. Then obviously, $C \in \mathbb{Z}[\theta]$. [1]

This suggests that the multiplication of two polynomials evaluated at θ should be carried out as follows

$$a(x)\Big|_{x=\theta} \cdot b(x)\Big|_{x=\theta} = [a(x)b(x) \pmod{f(x)}]_{x=\theta}$$

[1]Even if the degree of C had not been less than d, C could have been reduced modulo f to something with degree less than d. C has an equivalent element with degree less than d, so strictly speaking, $C \in \mathbb{Z}[\theta]$ in this case as well.

It is very important to take note of this multiplication method because it will be used extensively in examples to follow.

D. The Heart of the GNFS Algorithm

The fundamental reason that the GNFS algorithm will factor composite numbers will be explained in this section.

Suppose one can find a $\beta^2 \in \mathbb{Z}[\theta]$ that is a perfect square and a $y^2 \in \mathbb{Z}$ that is a perfect square. Then one can produce a difference of squares congruence that can be used to factor n as detailed in Section II-A. This works because of the following theorem.

Theorem 2.2: Given a polynomial $f(x)$ with integer coefficients, a root $\theta \in \mathbb{C}$, and an $m \in \mathbb{Z}/n\mathbb{Z}$ such that $f(m) \equiv 0 \pmod{n}$, there exists a unique mapping $\phi : \mathbb{Z}[\theta] \to \mathbb{Z}/n\mathbb{Z}$ satisfying

1) $\phi(ab) = \phi(a)\,\phi(b) \quad \forall a, b \in \mathbb{Z}[\theta]$
2) $\phi(a+b) = \phi(a) + \phi(b) \quad \forall a, b \in \mathbb{Z}[\theta]$
3) $\phi(1) \equiv 1 \pmod{n}$
4) $\phi(\theta) \equiv m \pmod{n}$

(The above conditions also imply that $\phi(za) = z\phi(a) \quad \forall a \in \mathbb{Z}[\theta], z \in \mathbb{Z}$.)

One can apply this theorem to obtain a difference of squares congruence in the following way: suppose there exists a finite set U of pairs of integers (a, b) such that

$$\prod_{(a,b)\in U} (a + b\theta) = \beta^2 \text{ and } \prod_{(a,b)\in U} (a + bm) = y^2$$

for $\beta \in \mathbb{Z}[\theta]$ and $y \in \mathbb{Z}$. Let $x = \phi(\beta)$. Then working congruent modulo n,

$$\begin{aligned} x^2 &= \phi(\beta)\,\phi(\beta) \\ &= \phi\left(\beta^2\right) \\ &= \phi\left(\prod_{(a,b)\in U}(a+b\theta)\right) \\ &= \prod_{(a,b)\in U}(\phi(a+b\theta)) \\ &= \prod_{(a,b)\in U}(a+bm) \\ &= y^2 \end{aligned}$$

Thus a relation $x^2 \equiv y^2 \pmod{n}$ has been created and by Section II-A, there is a probability of $2/3$ that this will lead to a factorization of n.

E. Finding a perfect square in $\mathbb{Z}[\theta]$ and in $\mathbb{Z}$

The following sections will discuss in length procedures for finding perfect squares in $\mathbb{Z}[\theta]$ and in $\mathbb{Z}$. The method for finding both squares is based on a particular strategy. In order to motivate the discussion, a numerical example using the same strategy is given below.

Suppose one wishes to find a perfect square in $\mathbb{Z}$. Further suppose that for some reason, this task is not as simple as taking an arbitrary integer and squaring it. Also, suppose that there are numbers known for which all of their prime factors are less than or equal to 19. Let this set of numbers be

$$\{455, 39270, 770, 429, 1616615, 3990, 106590, 187, 19019\} \tag{II.1}$$

These numbers have the property that all their prime factors are contained in the set

$$\{2, 3, 5, 7, 11, 13, 17, 19\} \tag{II.2}$$

and all exponents occurring in the prime factorizations are equal to 1. The factorization of each number is illustrated in Table II.

Each number in the array has a unique prime factorization involving only the primes in (II.2). Therefore, each number in Table II can be represented with a vector composed of all the exponents occurring in the prime factorization. Note that this means that there will be one entry in the vector for each prime in

TABLE II

FACTORS FOR THE NUMERICAL EXAMPLE OF SECTION II-E

Number	**Factorization**							
	2	3	5	7	11	13	17	19
455			⋆	⋆		⋆		
39270	⋆	⋆	⋆	⋆	⋆		⋆	
770	⋆		⋆	⋆	⋆			
429		⋆			⋆	⋆		
1616615			⋆	⋆	⋆	⋆	⋆	⋆
3990	⋆	⋆	⋆	⋆				⋆
106590	⋆	⋆	⋆		⋆		⋆	⋆
187					⋆		⋆	
19019				⋆	⋆	⋆		⋆

(II.2). For example

$$\begin{aligned} 455 &= 2^0 3^0 5^1 7^1 11^0 13^1 17^0 19^0 \\ 455 &\leftrightarrow (0,0,1,1,0,1,0,0) \end{aligned}$$

Under this notation, multiplying two numbers together will yield an integer with an exponent vector equivalent to adding the exponent vectors of the two numbers.

$$\begin{aligned} 770 \cdot 455 &\leftrightarrow (1,0,1,1,1,0,0,0) + (0,0,1,1,0,1,0,0) \\ &\leftrightarrow (1,0,2,2,1,1,0,0) \end{aligned}$$

If a product of a subset of the numbers in (II.1) results in an exponent vector with all even entries, then the product is a perfect square.

This is equivalent to finding a vector $[a_1, a_2, \ldots, a_9]^T$ such that

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ & & & \vdots & & & & \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}^T \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_9 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \pmod 2 \qquad \text{(II.3)}$$

where the matrix on the left is a result of the relationship

$$\begin{bmatrix} 455 \\ 39270 \\ \vdots \\ 19019 \end{bmatrix} \leftrightarrow \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ & & & & \vdots & & & \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Because (II.1) is a system of 8 equations and 9 unknowns, a (nonunique) solution does exist. One solution to this equation is $[a_1, a_2, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9]^T = [1, 1, 0, 0, 1, 1, 0, 0, 0]^T$. This implies that $455 \cdot 39270 \cdot 1616615 \cdot 3990$ is a perfect square. Indeed, a simple calculation shows that $455 \cdot 39270 \cdot 1616615 \cdot 3990 = (339489150)^2$.

This method for finding perfect squares is of great importance in the GNFS, and ideas used in the above example will be used in later sections.

1) Definition of Smoothness on $\mathbb{Z}[\theta]$ and $\mathbb{Z}$:

Definition 2.1: A rational factor base is a finite collection of prime numbers.

In this paper, only rational factor bases of small, consecutive primes are considered. Therefore, for the purposes of this paper, a rational factor base can be thought of as a set

$$\{p : p \text{ is prime and } p \leq M\} \quad \text{for some } M \in \mathbb{N}$$

Definition 2.2: An integer $l \in \mathbb{Z}$ is said to be smooth over a rational factor base $\mathcal{R}$ if $\mathcal{R}$ contains all of the prime divisors of l.

Note that in the numerical example of Section II-E, all of the numbers $\{455, 39270, \ldots\}$ (equation II.1) were smooth over the rational factor base $\{2, 3, 5, 7, 11, 13, 17, 19\}$.

It is now necessary to define an algebraic factor base, a concept very similar to a rational factor base. However, some things must be assumed in order to properly define an algebraic factor base.

Definition 2.3: An algebraic factor base is a finite set $\{a + b\theta\} \subset \mathbb{Z}[\theta]$ where for $a, b \in \mathbb{Z}$, each $a + b\theta$ satisfies $\forall\,(a, b)\,, \nexists\ c, d \in \mathbb{Z}[\theta]$ such that $c \cdot d = a + b\theta$. (This condition causes $a + b\theta$ to be what is commonly called a "prime ideal.")

Definition 2.4: An element $l \in \mathbb{Z}[\theta]$ is said to be smooth over an algebraic factor base $\mathcal{A}$ if $\exists\, W \subset \mathcal{A}$ such that $\prod_{(c,d)\in W} (c + d\theta) = l$.

The definition of an algebraic factor base involves elements $a + b\theta \in \mathbb{Z}[\theta]$. $\mathbb{Z}[\theta]$ is a difficult space to represent on a computer, and hence development of an algorithm based on $\mathbb{Z}[\theta]$ would be difficult. Fortunately, this concept of an algebraic factor base has an analog that gives a way to more easily represent elements $a + b\theta \in \mathbb{Z}[\theta]$.

Theorem 2.3: Let $f(x)$ be a polynomial with integer coefficients and let $\theta \in \mathbb{C}$ be a root of $f(x)$. Then the set of pairs $\{(r, p)\}$ where p is a prime integer and $r \in \mathbb{Z}/n\mathbb{Z}$ with $f(r) \equiv 0 \pmod{p}$ is in bijective correspondence with the set of $a+b\theta \in \mathbb{Z}[\theta]$ that satisfy the criteria for being in an algebraic factor base.

This theorem can be used to represent the algebraic factor base $\{a + b\theta\}$ as a finite set of pairs of integers $\{(r, p)\}$. While not every element of $\mathbb{Z}[\theta]$ can be represented as a pair (r, p), what can be represented is sufficient to meet the needs of the GNFS.

2) Finding Smooth Numbers: Sieving Techniques: In order to find a square in $\mathbb{Z}[\theta]$ and in $\mathbb{Z}$ as required by Section II-A, it first necessary to find pairs of numbers (a, b) such that $a + b\theta$ is smooth in some algebraic factor base and $a + bm$ is smooth in some rational factor base.

Let $\mathcal{R}$ be an arbitrary rational factor base represented by the set of primes $\{q_i\}$ and let $\mathcal{A}$ be an arbitrary algebraic factor base in $\mathbb{Z}[\theta]$ represented by the set of pairs $\{(r_i, p_i)\}$ as described by Theorem 2.3.

Theorem 2.4: For $c + d\theta$ in an algebraic factor base and that has the representation (r, p), $c + d\theta$ divides $a + b\theta \in \mathbb{Z}[\theta]$ if and only if $a \equiv -br \pmod{p}$.

Theorem 2.5: A finite set U of pairs $(r, p) \in \mathbb{Z}[\theta]$ represents a complete factorization of $a + b\theta$ if and only if $\prod_{(r_i,p_i)\in U} p_i = (-b)^d f(-a/b)$ where d is the degree of f.

Theorem 2.6: A prime number q will divide $a + bm$ if and only if $a \equiv -bm \pmod{q}$.

Using the above three theorems, smooth elements of $\mathbb{Z}[\theta]$ and $\mathbb{Z}$ can be found in the following way:

(a) Fix $b \in \mathbb{Z}$, and let N be an arbitrary positive integer.

(b) Let a vary from $-N$ to N. Create two arrays: one for the various values of $a+b\theta$ that will result and another for the various values of $a+bm$ that will result. This concept is illustrated in Figure 1.

Fig. 1. Sieve Arrays

$$\left|\begin{array}{c} -N+b\theta \\ (-N+1)+\theta \\ \vdots \\ (N-1)+b\theta \\ N+b\theta \end{array}\right| \quad \left|\begin{array}{c} -N+bm \\ (-N+1)+m \\ \vdots \\ (N-1)+bm \\ N+bm \end{array}\right|$$

(c) For each q_i in $\mathcal{R}$, q_i will divide $a+bm$ if and only if $a \equiv -bm \pmod{q_i}$. Find values of a for which $a=-bm+kq_i$ for some $k \in \mathbb{Z}$, and for each value of a make note of this factor of $a+bm$ in the sieve array. Repeat this process for every $q_i \in \mathcal{R}$. When finished, make note of all the $a+bm$ in the sieve array that are completely factored by this method. These $a+bm$ are smooth in $\mathcal{R}$.

(d) Proceed in an identical manner for the $a+b\theta$ sieve array. An $(r_i, p_i) \in \mathcal{A}$ divides $a+b\theta$ if and only if $a \equiv -br_i \pmod{p_i}$. Find values of a satisfying $a=-br_i+kp_i$ for some $k \in \mathbb{Z}$. For each a found, make note of this (r_i, p_i) factor of $a+b\theta$ in the sieve array. When finished, for all $a+b\theta$ in the sieve array there will be a list of (r_i, p_i) factors. If $\prod p_i = (-b)^d f(-a/b)$ then this list of factors is a complete factorization and hence $a+b\theta$ is smooth over the given algebraic factor base $\mathcal{A}$.

(e) Compare the two arrays entry by entry. At any position, if both the $a+b\theta$ and the $a+bm$ are smooth then this (a, b) is what was sought after. Save it for later use.

One can repeat this procedure by altering b to find as many (a, b) satisfying the required criteria as may be needed.

3) Verifying That Elements of $\mathbb{Z}[\theta]$ and $\mathbb{Z}$ Are Squares: From Section II-E.2, one can find smooth $a+bm$ and smooth $a+b\theta$. A method similar to the numerical example of Section II-E to find squares in $\mathbb{Z}\theta$ and $\mathbb{Z}$ will be used. However, before this is done it is necessary to develop methods for testing for squareness in $\mathbb{Z}$ and $\mathbb{Z}[\theta]$.

It is relatively easy to determine whether or not an arbitrary $s \in \mathbb{Z}$ is a perfect square. In fact, the methods used in the GNFS will give access to the prime factorization of s for the s that is to be tested for squareness. In this case, s is a perfect square if and only if every exponent occurring in the prime

factorization is even. That is, for every exponent e in the prime factorization, if $e \equiv 0 \pmod 2$ then s is a perfect square in $\mathbb{Z}$. Testing $l \in \mathbb{Z}[\theta]$ for perfect squareness is more complicated.

Theorem 2.7: Let $l \in \mathbb{Z}[\theta]$ have the factorization $l = (a_1 + b_1\theta)^{e_1} (a_2 + b_2\theta)^{e_2} \ldots$ where for every j, $a_j + b_j\theta$ satisfies the criteria to be in an algebraic factor base. If l is a perfect square in $\mathbb{Z}[\theta]$ then $\forall i, e_i \equiv 0 \pmod 2$.

This is one such condition that a perfect square $l \in \mathbb{Z}[\theta]$ will satisfy. However, it is not the only condition.

Definition 2.5: The Legendre symbol $\left(\frac{a}{p}\right)$ for $a \in \mathbb{Z}$ and p a prime integer is defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \pmod p \text{ has a solution} \\ -1 & \text{if } x^2 \equiv a \pmod p \text{ has no solution} \\ 0 & \text{if } p \mid a \end{cases}$$

Theorem 2.8: Let U be a set of (a, b) pairs such that $\prod_{(a,b)\in U} (a + b\theta)$ is a perfect square in $\mathbb{Z}[\theta]$. Then for any (s, q) with q prime and s given as Theorem 2.3 with $(s, q) \nmid a + b\theta$ for any $(a, b) \in U$,

$$\prod_{(a,b)\in U} \left(\frac{a + bs}{q}\right) = 1$$

Note that in the above theorem, $(s, q) \nmid a + b\theta$ implies that $a \not\equiv -bs \pmod q$. Thus $q \nmid a + bs$ and so $\left(\frac{a+bs}{q}\right) \neq 0$. This is an important observation to make as it will be used in later sections.

The above two theorems give necessary but not sufficient conditions for an element of $\mathbb{Z}[\theta]$ to be a perfect square. That is, if the goal is to show that something is a perfect square, then the above theorems are the converse of what is needed.

In practice, one determines if an element $l \in \mathbb{Z}[\theta]$ is square in the following way:

(a) Verify that for a factorization

$$l = (a_1 + b_1\theta)^{e_1} (a_2 + b_2\theta)^{e_2} \ldots$$

$e_j \equiv 0 \pmod 2$ for every j.

(b) Let $\mathcal{Q}$ be a set of pairs of numbers (s, q) with q prime and s given as in Theorem 2.3. Choose $\mathcal{Q}$ such that $(s, q) \nmid a + b\theta$ for every $a + b\theta$ occurring in the factorization of l. Verify that for every $(s, q) \in \mathcal{Q}$,

$$\prod_{(a,b)\in U} \left(\frac{a+bs}{q}\right) = 1$$

for U defined as in Theorem 2.8. The set $\mathcal{Q}$ is called the quadratic character base and each $(s, q) \in \mathcal{Q}$ is called a quadratic character.

(c) If the above two conditions are satisfied, then l is probably a perfect square in $\mathbb{Z}[\theta]$. Note that to increase this probability, one should increase the number of elements in $\mathcal{Q}$.

In summary, there are now developed methods for testing for perfect squares in $\mathbb{Z}[\theta]$ and $\mathbb{Z}$.

4) Putting It All Together: From Smooth Numbers to Square Numbers: Up to this point methods are developed to find a set of numbers $U = \{(a, b)\}$ such that $a + bm$ is smooth in a rational factor base $\mathcal{R}$ and $a + b\theta$ is smooth in an algebraic factor base $\mathcal{A}$. This section will describe how to use this information to find a square in $\mathbb{Z}$ and in $\mathbb{Z}[\theta]$. Throughout, ideas similar to the numerical example of Section II-E are used.

Let the rational factor base $\mathcal{R}$ have k elements, and let the algebraic factor base $\mathcal{A}$ have l elements. Choose an arbitrary quadratic character base $\mathcal{Q}$ with u elements. $\mathcal{R}$ and $\mathcal{A}$ will be used to find a square in $\mathbb{Z}$ and $\mathbb{Z}[\theta]$, and $\mathcal{Q}$ will be used to verify that the result is a square.

Each $(a, b) \in U$ can be represented as a row vector with $1 + k + l + u$ entries. The first entry should be equal to 0 if $a + bm$ is positive and 1 if $a + bm$ is negative. The next k entries are given to the exponent vector modulo 2, as described in Section II-E. The following l entries are used for indicating whether a particular element of $\mathcal{A}$ divides $a + b\theta$. The exponent on this element of $\mathcal{A}$ that appears in the factorization modulo 2 is what should appear in each of these l entries. The final u entries are used in conjunction with the quadratic character base $\mathcal{Q}$. Each entry is set to 0 if for the appropriate (s, q), $\left(\frac{a+bs}{q}\right) = 1$. Otherwise, set the entry to 1.

In summary, let the rational factor base $\mathcal{R}$ be $\{t_1, t_2, \ldots, t_k\}$, let the algebraic factor base $\mathcal{A}$ be $\{(r_1, p_1), (r_2, p_2), \ldots (r_l, p_l)\}$, and let the quadratic character base $\mathcal{Q}$ be $\{(s_1, q_1), (s_2, q_2), \ldots (s_u, q_u)\}$. For a given (a, b), $a + bm$ has a factorization $t_1^{e_1} t_2^{e_2} \cdots t_k^{e_k}$. $a + b\theta$ has the factorization that can be represented as $(r_1, p_1)^{f_1} (r_2, p_2)^{f_2} \cdots (r_l, p_l)^{f_l}$.

Then the pair (a, b) should be represented by a row vector of the following form:

$$\left[\begin{cases} 0, a+bm \geq 0 \\ 1, \text{else} \end{cases} \right] \quad \begin{matrix} e_1 \pmod 2 & e_2 \pmod 2 & \cdots & e_k \pmod 2 \\ f_1 \pmod 2 & f_2 \pmod 2 & \cdots & f_l \pmod 2 \end{matrix} \quad \begin{cases} 0, \left(\frac{a+bs_1}{q_1}\right) = 1 \\ 1, \text{else} \end{cases} \begin{cases} 0, \left(\frac{a+bs_2}{q_2}\right) = 1 \\ 1, \text{else} \end{cases} \cdots \begin{cases} 0, \left(\frac{a+bs_u}{q_u}\right) = 1 \\ 1, \text{else} \end{cases} \Bigg] \tag{II.4}$$

Now suppose a $V \subset U$ is found such that $\prod_{(a,b)\in V}(a+bm)$ is a perfect square in $\mathbb{Z}$ and $\prod_{(a,b)\in V}(a+b\theta)$ is a perfect square in $\mathbb{Z}[\theta]$. Then the following must all hold:

(a) $\prod_{(a_j,b_j)\in V}(a_j+b_jm)$ must be positive. Let $c_j = \begin{cases} 0, a_j+b_jm \geq 0 \\ 1, \text{else} \end{cases}$. Note that this is just the first entry in the vector for (a_j, b_j). Then $\prod_{(a_j,b_j)\in V}(a_j+b_jm)$ is positive if and only if $\sum c_j = 0 \pmod 2$. This insures that the number of negative numbers in the product is even. Because -1 raised to an even power is 1, the product will be positive.

(b) Every exponent occurring in the prime factorization of $\prod_{(a_j,b_j)\in V}(a_j+b_jm)$ must be even. Because $\forall\ j, a_j+b_jm$ is smooth on $\mathcal{R}$, the product will also be smooth on $\mathcal{R}$. Furthermore, if e_j is the corresponding exponent appearing on any $t \in \mathcal{R}$ in the prime factorization of a_j+b_jm, then the exponent appearing in the prime factorization of the product is $\sum_{(a_j,b_j)\in V} e_j$. Thus, for $\prod_{(a_j,b_j)\in V}(a_j+b_jm)$ to be square, $\forall t \in \mathcal{R}$,

$$\sum_{(a_j,b_j)\in V} e_j \equiv 0 \pmod 2 \Leftrightarrow \sum_{(a_j,b_j)\in V} (e_j \pmod 2) \equiv 0 \pmod 2$$

Each $e_j \pmod 2$ in the sum on the left is an entry in the vector representation of (a, b).

(c) Every exponent occurring in the prime ideal factorization of $\prod_{(a_j,b_j)\in V}(a_j+b_j\theta)$ must be even. Similar to the above, $\forall\ j, a_j+b_j\theta$ is smooth in $\mathcal{A}$ implies that $\prod_{(a_j,b_j)\in V}(a_j+b_j\theta)$ smooth in $\mathcal{A}$. Let $a_j+b_j\theta$ have the representation $(r_1,p_1)^{e_{j_1}}(r_2,p_2)^{e_{j_2}}\ldots(r_l,p_l)^{e_{j_l}}$. Then $\prod_{(a_j,b_j)\in V}(a_j+b_j\theta)$ has the representation

$$(r_1,p_1)^{\sum e_{j_1}}(r_2,p_2)^{\sum e_{j_2}}\ldots(r_l,p_l)^{\sum e_{j_l}}$$

Each exponent in this expansion is required to be even. Thus $\forall\ i, \sum e_{j_i} \equiv 0 \pmod 2$. This implies that $\forall\ i, \sum (e_{j_i} \pmod 2) \equiv 0 \pmod 2$. Note that each $e_{j_i} \pmod 2$ is just an entry in the vector representation of (a_j, b_j).

(d) For every $(s, q) \in \mathcal{Q}, \prod_{(a_j,b_j)\in V}\left(\frac{a_j+b_js}{q}\right)$ must be 1. Because $\forall\ j, \left(\frac{a_j+b_js}{q}\right) \in \{1, -1\}$, in order for $\prod_{(a_j,b_j)\in V}\left(\frac{a_j+b_js}{q}\right) = 1$, the number of j for which $\left(\frac{a_j+b_js}{q}\right) = -1$ must be even. For a given

(s, q), the vector representation of (a_j, b_j) has an entry corresponding to

$$\left\{ \begin{array}{l} 0, \left(\frac{a_j+b_j s}{q}\right) = 1 \\ 1, \text{else} \end{array} \right\}$$

If the sum of these entries is even then the number of j's for which $\left(\frac{a_j+b_j s}{q}\right) = -1$ will be even. Hence

$$\prod_{(a_j,b_j)\in V} \left(\frac{a_j + b_j s}{q}\right) = 1 \Leftrightarrow \sum_{(a_j,b_j)\in V} \left\{ \begin{array}{l} 0, \left(\frac{a_j+b_j s}{q}\right) = 1 \\ 1, \text{else} \end{array} \right\} \equiv 0 \pmod 2$$

Because all 4 of the above conditions must hold simultaneously, $\prod_{(a_j,b_j)\in V}(a_j + b_j m)$ is a perfect square in $\mathbb{Z}$ and $\prod_{(a_j,b_j)\in V}(a_j + b_j \theta)$ is a perfect square in $\mathbb{Z}[\theta]$ if and only the sum of the vector representation of each $(a_j, b_j) \in V$ is equivalent to the zero vector modulo 2.

Let the set U of smooth (a, b) have y elements. Let X be a y x $(1 + k + l + u)$ matrix with each row being equivalent to the vector representation of an $(a, b) \in U$.

Finding a $V \subset U$ in order to get perfect squares is equivalent to finding a column vector A such that

$$X^T \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_y \end{bmatrix} \equiv 0 \pmod 2 \tag{II.5}$$

If $y > 1 + k + l + u$, this congruence is guaranteed to have a nontrivial solution A.

Because of this congruence modulo 2, every A_j is in the set $\{0, 1\}$ (the residue set of 2). Let the subset $V \subset U$ be defined by $\forall(a_j, b_j) \in U, (a_j, b_j) \in V$ if $A_j = 1$. Then $\prod_{(a_j,b_j)\in V}(a_j + b_j m)$ is a perfect square in $\mathbb{Z}$ and $\prod_{(a_j,b_j)\in V}(a_j + b_j \theta)$ is a perfect square in $\mathbb{Z}[\theta]$.

F. A Summary Of The Above Methods

The GNFS algorithm to factor a composite number n can be summarized as follows:

(a) Choose an $m \in \mathbb{Z}$ and find a corresponding f satisfying $f(m) \equiv 0 \pmod n$ by the base-m expansion method.

(b) Define a rational factor base $\mathcal{R}$ such that $\mathcal{R}$ has finitely many elements and $\forall x \in \mathcal{R}$, x is prime. Let k be the number of elements in $\mathcal{R}$.

(c) Define an algebraic factor base $\mathcal{A}$ such that $\mathcal{A}$ has finitely many elements and $\forall(r, p) \in \mathcal{A}$, p is prime and r satisfies $f(r) \equiv 0 \pmod p$. Let l be the number of elements in $\mathcal{A}$.

(d) Define a quadratic character base $\mathcal{Q}$ with finitely many elements so that $\forall(s,q) \in \mathcal{Q}$, q is prime and $f(s) \equiv 0 \pmod{q}$. Ensure that $\forall(s,q) \in \mathcal{Q}$, $(s,q) \notin \mathcal{A}$. Let u be the number of elements in $\mathcal{Q}$.

(e) For a fixed $b \in \mathbb{Z}$, build sieve arrays as in Section II-E.2. Note the elements of the sieve arrays that are smooth and also for these elements record which $q_i \in \mathcal{R}$ and which $(r_i, p_i) \in \mathcal{A}$ are divisors. Repeat this process for various b as necessary until more than $1+k+l+u$ pairs (a,b) have been found such that $a+bm$ is smooth in $\mathbb{Z}$ and $a+b\theta$ is smooth in $\mathbb{Z}[\theta]$. Let y be the number of smooth (a,b) found.

(f) Populate a y x $(1+k+l+m)$ matrix X as described in Section II-E.4.

(g) Solve the equation

$$X^T \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_y \end{bmatrix} \equiv 0 \pmod{2}$$

for $\{A_1, \ldots, A_y\}$. Let the subset $V \subset U$ be defined by $\forall(a_j, b_j) \in U, (a_j, b_j) \in V$ if $A_j = 1$. Then $\prod_{(a_j,b_j)\in V}(a_j + b_j m)$ is a perfect square in $\mathbb{Z}$ and $\prod_{(a_j,b_j)\in V}(a_j + b_j\theta)$ is a perfect square in $\mathbb{Z}[\theta]$.

(h) With the mapping ϕ from Section II-D,

$$\phi\left(\prod_{(a_j,b_j)\in V}(a+b\theta)\right) \equiv \prod_{(a_j,b_j)\in V}(a_j + b_j m) \pmod{n}$$

Use this to attempt to factor n using the difference of square factorization method of Section II-A. If no factorization is found, go to (b) and repeat this process.

III. An Example

In this section the GNFS is used to factor an example number. To help solidify the above concepts, this example will be presented at length.

Suppose one desires to factor the number $n = 45113$. A preliminary step is to verify that the number is composite. Assume some primality test has been done and 45113 is known to be composite. The GNFS can then be used to factor 45113.

The first step in the GNFS is to pick an integer m and a polynomial f as discussed in Section II-B. Let $m = 31$. f must be chosen to satisfy $f(m) \equiv 0 \pmod{n}$, but by considering the base-m expansion of n this task is easily done.

$$45113 = 31^3 + 15 \cdot 31^2 + 29 \cdot 31 + 8$$

Define $f(x) = x^3 + 15x^2 + 29x + 8$. Then $f(m) = f(31) = 45113 = n$, and therefore $f(m) \equiv 0 \pmod{n}$.

The next task to be done in setting up the GNFS is to pick the rational and algebraic factor bases. For the rational factor base $\mathcal{R}$, simply consider all primes below 30.

$$\mathcal{R} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$$

Any algebraic factor base $\mathcal{A}$ can be represented by pairs (r, p) where p is a prime and r satisfies $f(r) \equiv 0 \pmod{p}$ (Theorem 2.3). Arbitrarily, let p be any prime less than 90 and find a set r_i such that $\forall i, f(r_i) \equiv 0 \pmod{p}$. For each r_i, add an entry (r_i, p) to $\mathcal{A}$. Repeating this for all p in the set of primes less than 90 yields

$$\begin{aligned}\mathcal{A} \;=\; \{\; &(0,2),(6,7),(13,17),(11,23),(26,29),(18,31),(19,41),(13,43),(1,53),(46,61),\\ &(2,67),(6,67),(44,67),(50,73),(23,79),(47,79),(73,79),(28,89),(62,89),(73,89)\;\}\end{aligned}$$

Note that the $\mathcal{R}$ chosen has $k = 10$ elements and the $\mathcal{A}$ chosen has $l = 20$ elements. The cardinality of these sets will be important later.

In addition to a rational factor base and an algebraic factor base, a quadratic character base must also be found. Choose primes q not occurring in the algebraic factor base and for each q, find all s satisfying $f(s) \equiv 0 \pmod{q}$. For each s, add the pair (s, q) to the quadratic character base. In this example, the primes $97, 101, 103, 107$ did not appear in $\mathcal{A}$. Using these primes, the quadratic character base $\mathcal{Q}$ is then computed to be

$$\mathcal{Q} = \{(28, 97), (87, 101), (47, 103), (4, 107), (8, 107), (80, 107)\}$$

Note that $\mathcal{Q}$ has $u = 6$ entries. By Section II-E.4, more than $1 + k + l + u = 37$ pairs (a, b) with $a + bm$ smooth in $\mathcal{R}$ and $a + b\theta$ smooth in $\mathcal{A}$ must be found.

The GNFS is now set up. The first step in executing it is to construct sieve arrays to find smooth $a + b\theta$ and smooth $a + bm$. Let b run from 1 to 41 and let a run from -400 to 400. Loop over the list of possible b, and for each b, construct two arrays with $(2 \cdot 400 + 1)$ entries. Use these arrays as described in Section II-E.4 to find the values of a for which $a + bm$ and $a + b\theta$ are smooth. If both of these are smooth for the same a, save this (a, b) pair. Repeat this with each b ranging from 1 to 41. This results in 38 pairs (a, b) satisfying $a + bm$ smooth over $\mathcal{R}$ and $a + b\theta$ smooth over $\mathcal{A}$. See Table III for a complete listing.

It is relatively easy to check that any of these pairs is smooth. for example, consider the pair $(119, 11)$. $a + bm = 119 + 31 * 11$ factors as $2^2 \cdot 5 \cdot 23$. Because all of these numbers are in $\mathcal{R}$, $a + bm$ is

TABLE III

SMOOTH PAIRS (a, b) FOUND BY SIEVING

(-73,1)	(-13,1)	(-6,1)	(-2,1)	(-1,1)	(1,1)	(2,1)	(3,1)
(13,1)	(15,1)	(23,1)	(61,1)	(1,2)	(3,2)	(33,2)	(2,3)
(5,3)	(19,4)	(14,5)	(37,5)	(313,5)	(11,7)	(15,7)	(-7,9)
(119,11)	(-247,12)	(175,13)	(5,17)	(-1,19)	(35,19)	(17,25)	(49,26)
(375,29)	(9,32)	(1,33)	(78,37)	(5,41)	(9,41)		

smooth over $\mathcal{R}$ for this particular $(119, 11)$. It can be shown that the following pairs $(r, p) \in \mathcal{A}$ divide $a + b\theta = 119 + 11\theta$: $\{(19, 41), (44, 67), (62, 89)\}$. By Theorem 2.5, this is complete factorization of $a + b\theta$ if and only if $41 \cdot 67 \cdot 89 = (-11)^3 f(-119/11)$. The reader can verify that both sides of this equation are equal in absolute value. (Theorem 2.5 can be weakened to equality in absolute value with no consequences.)

The next step in the GNFS is to set up the matrix equation of (II.5). This requires that the matrix X be found, a relatively straightforward procedure that can be done using the definition of each row of X as in (II.4). For example, the row of X corresponding to the pair $(119, 11)$ is

$$[\underbrace{0}_{\text{sign of } a+bm}, \overbrace{0,0,1,0,0,0,0,0,1,0}^{\text{exponents on the factors of } a+bm}, \underbrace{0,0,0,0,0,0,1,0,0,0,0,0,1,0,0,0,0,0,1,0}_{\text{exponents on the factors of } a+b\theta}, \overbrace{1,1,0,0,0,0}^{\text{for use with } \mathcal{Q}}]$$

Using X, the equation

$$X^T \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_y \end{bmatrix} \equiv 0 \pmod 2$$

can be solved for $[A_1, A, 2, \ldots, A_y]^T$. Note that because X has more rows than columns this solution will not be unique. One such solution is

$$[A_1, \ldots, A_y]^T = [0,0,0,1,0,1,0,0,1,1,1,0,0,1,1,0,1,1,1,0,0,0,1,0,1,0,1,0,1,0,0,1,0,0,0,0,0,0]^T$$

This implies that for the following pairs (a, b)

$$\begin{aligned} V \;=\; & \{\,(-2,1),(1,1),(13,1),(15,1),(23,1),(3,2),(33,2),(5,3), \\ & (19,4),(14,5),(15,7),(119,11),(175,13),(-1,19),(49,26)\,\} \end{aligned}$$

$\prod_{(a,b)\in V}(a+bm)$ is a perfect square in $\mathbb{Z}$ and $\prod_{(a,b)\in V}(a+bm\theta)$ is a perfect square in $\mathbb{Z}[\theta]$. Evaluating this yields

$$\begin{aligned}\prod_{(a,b)\in V}(a+bm) &= 459997127517951955826063769600000\\ \prod_{(a,b)\in V}(a+b\theta) &= 58251363820606365\cdot\theta^2+149816899035790332\cdot\theta+75158930297695972\end{aligned}$$

Square roots in $\mathbb{Z}$ and $\mathbb{Z}[\theta]$ now need to be computed. The reader can verify that

$$\begin{aligned}2553045317222400^2 &= \prod_{(a,b)\in V}(a+bm)\\ \left(108141021\cdot\theta^2+235698019\cdot\theta+62585630\right)^2 &= \prod_{(a,b)\in V}(a+b\theta)\end{aligned}$$

Using the mapping ϕ from Theorem 2.2,

$$\phi\left(108141021\cdot\theta^2+235698019\cdot\theta+62585630\right)=111292745400$$

Therefore, using an argument presented in Section II-D, one can conclude that

$$111292745400^2\equiv 2553045317222400^2 \pmod{n}$$

Attempting to factor n with this relation yields

$$\begin{aligned}\gcd(45113, 111292745400+2553045317222400) &= 197\\ \gcd(45113, 111292745400-2553045317222400) &= 229\end{aligned}$$

Therefore, $n=45113=197\cdot 229$. The GNFS has successfully factored n.

IV. Conclusion

The GNFS is a very sophisticated algorithm for factoring composite numbers. While the algorithm is complex, it does successfully factor a number relatively quickly. Due to the setup steps necessary, the GNFS is significantly slower than other popular factoring methods for small composite numbers. However, for large composite numbers the time spent in setting up the GNFS is negligible and the algorithm is dramatically faster than any other factoring algorithm.

This point was proved on January 18, 2002 when a team of researchers from the University of Bonn successfully factored a 155 digit (512 bit) composite integer in 3.7 months using the GNFS. Had this 512 bit number been a public key in the RSA cryptosystem, the security of the system would have been

compromised and an adversary would have gained access to the private key. The development of the GNFS has brought into question the security of the RSA cryptosystem. Because of the widespread use of RSA, the existence of the GNFS should cause any computer security expert to worry.

REFERENCES

[1] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*. Prentice Hall, 2002.

[2] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction To The Theory Of Numbers*, 5th ed. Wiley, 1991.

[3] J. Rotman, *A First Course In Abstract Algebra*. Prentice Hall, 1996.

[4] D. M. Bressoud, *Factorization and Primality Testing*. Springer, 1989.

[5] M. E. Briggs, "An introduction to the general number field sieve," Master's thesis, Virginia Polytechnic Institute, 1998.

[6] R. M. Huizing, "An implementation of the number field sieve, Tech. Rep. NM-R9511, 1995. [Online]. Available: citeseer.nj.nec.com/huizing95implementation.html

[7] R. Elkenbracht-Huizing, "An implementation of the number field sieve," 1996. [Online]. Available: citeseer.nj.nec.com/elkenbracht-huizing96implementation.html

[8] K. Nakamula, "A survey on the number field sieve." [Online]. Available: citeseer.nj.nec.com/312752.html

[9] F. Bahr, J. Franke, and T. Kleinjung, "New prime factorisation record obtained using the general number field sieve." [Online]. Available: www.ercim.org/publication/Ercim_News/enw49/franke.html