2009

Factoring Large Numbers with Continued Fractions

Matthew S. Frey
University of Redlands

University of Redlands

Factoring Large Numbers with Continued Fractions

A thesis submitted in partial fulfillment
of the requirements for honors in mathematics

Bachelor of Science
in
Mathematics
by

Matthew S. Frey

April 2009

Honors Committee:
Professor Tamara Veenstra
Professor Steve Morics
Professor Jim Bentley
Professor Paul McQuesten

I would like to dedicate this paper to my mathematics professors at University of Redlands. It is through your selfless dedication to not only the dynamic field of mathematics, but to me as a student who has gained knowledge, confidence and a lifelong love of learning from each one of you. Through your mentorship, I have developed the ability to analyze and evaluate data and most of all, to be able to write and speak about my knowledge and conclusions. I thank each of you for your time, valuable resources and for the inspiration that gave me the courage to complete this project.

Contents

Chapter 1

Goal of my Project

The goal of my project was to gain a better understanding of the CFRAC algorithm and to be able to share my knowledge of factorization of large numbers as it relates to the national security of our country. In order to complete my goal I conducted research of the field of mathematics with a specific exploration of the CFRAC algorithm. With RSA being publicly described in 1977, major breakthroughs were established in message encryption. My goal was to find out if it was possible to crack the RSA code through utilization of CFRAC. In order to do this, I needed to explore the special properties of finite and infinite continued fractions. I also needed to further my knowledge of the program Maple which enabled me to work through the CFRAC algorithm much more quickly.

Chapter 2

Introduction

The media has introduced cryptography through popular movies such as Windtalkers, A Beautiful Mind and National Treasure. Even though these movies provide us with a layman's understanding of the conceptualization and definition of public key encryption, it is through more specific analysis that we can gain a clearer understanding of the continued fraction factorization method (CFRAC). The CFRAC algorithm is an integer factorization method that has the ability to factor integers that are fifty digits or less. Factorization and public key cryptography have developed into one of the major mathematical achievements in the twentieth century. One noted encryption method was developed by Ron Rivest, Adi Shamir and Leonard Adleman whose initials of their last names (RSA) were used to name the algorithm. The RSA algorithm is used for public-key cryptography which utilizes two keys, one for encryption and the other for decryption. The RSA algorithm retains its popularity due to its simplicity and security. It is implemented through the following steps:

1. Choose two distinct prime numbers p and q which are to be kept secret.
2. Let $N = pq$. N is public information and will be used as the modulus.
3. Compute $\phi(N) = (p-1)(q-1)$. $\phi(N)$ will be kept secret.
4. Choose an integer e such that $1 < e < \phi(N)$ and $gcd(e, \phi(N)) = 1$. e is then released to the public.
5. Find d by solving $ed = 1 \pmod{\phi(N)}$. In other words, find the inverse of $e \pmod{\phi(N)}$. d is to be kept secret.

Public: e and N Private: $p, q, \phi(N)$ and d

As we apply the RSA algorithm it is important to remember that public key cryptography must utilize keys that are long enough and random enough

so that the possibility of guessing the keys is nearly impossible. Additionally the encryption process must be sophisticated enough to ensure that the original message cannot be recovered without utilization of the key.

An example of this algorithm is displayed through two people, Amy and Bill. Amy chooses relatively large primes p and q, computes N which is typically 300 or so digits long, computes $\phi(N)$, and chooses an integer e such that $1 < e < \phi(N)$. She then sends Bill her public key $(e, \phi(N))$ while not worrying if anyone intercepts $(e; \phi(N))$. At this point Bill encrypts his message[1] M by $M^e \pmod N$ which we will call L. Bill then sends his encrypted message L to Amy who can use d to decrypt the message. Amy would do this by raising L to d. That is, Amy would compute $L^d \pmod N$ which is congruent to M.

The decryption algorithm works because $L^d \equiv (M^e)^d \equiv M^{ed} \pmod N$. We know that $ed = 1 \pmod{\phi(N)}$ because e and d are inverses of each other. That is, we know that $ed = 1 + k\phi(N)$ where k is an integer. So, $M^{ed} = M^{1+k\phi(N)} = M(M^k)^{\phi(N)} \equiv M \pmod N$ by Euler's theorem.

The strength of RSA's security is dependent on the fact that the only way to decrypt a message is to find d. To do so, one would either have to guess values which could take years, or factor N. By factoring N we acquire p and q. We can then use p and q to find $\phi(N)$. Since e is public information and we know $\phi(N)$ we can acquire d. The first step in this process is having the ability to factor large numbers which we can do by using CFRAC. Once the CFRAC technique is mastered, we can utilize factorization of large numbers which will allow us to decrypt coded messages. We must begin this process by looking at finite continued fractions as they relate to CFRAC.

[1]We are assuming Bill's message consists of numbers only. If Bill's message consisted of letters, he would be required to first change his letters to numbers.

Chapter 3

Finite Continued Fractions

The goal of this chapter is to begin our understanding of what a continued fraction is. To start, we will look at a definition.

Definition 3.0.1. *A finite continued fraction is of the form:*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

where $a_0, a_1, \ldots, a_n \epsilon R$ *and all except for possibly* a_0 *are positive. The values* $a_0, a_1, \ldots, a_n$ *are the partial denominators of the fraction.[2]*

An example of a finite continued fraction is

$$\frac{51}{19} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{6}}}$$

Theorem 3.0.1. *Any finite rational number can be written as a finite continued fraction.*

Proof. Let $\frac{a}{b}$, where $b > 0$, be an arbitrary rational number. Then, by Euclid's algorithm we have:

$$\begin{aligned}
a &= ba_0 + r_1 && 0 < r_1 < b \\
b &= r_1 a_1 + r_2 && 0 < r_2 < r_1 \\
r_1 &= r_2 a_2 + r_3 && 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} a_{n-1} + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n a_n + 0
\end{aligned}$$

The key point here is that since each remainder r_k is positive then $a_1, a_2, \ldots, a_n$ must be positive. We can then manipulate the above equations to look like:

$$\begin{aligned}
\frac{a}{b} &= a_0 + \frac{r_1}{b} = a_0 + \frac{1}{\frac{b}{r_1}} && (3.0.1)\\
\frac{b}{r_1} &= a_1 + \frac{r_2}{r_1} = a_1 + \frac{1}{\frac{r_1}{r_2}} && (3.0.2)\\
\frac{r_1}{r_2} &= a_2 + \frac{r_3}{r_2} = a_2 + \frac{1}{\frac{r_2}{r_3}} \\
&\vdots \\
\frac{r_{n-1}}{r_n} &= a_n
\end{aligned}$$

When looking at the above you may have noticed that we can substitute equation 3.0.2 into 3.0.1. This is seen here:

$$\frac{a}{b} = a_0 + \frac{r_1}{b} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_1}{r_2}}} \tag{3.0.3}$$

We can keep this process going by substituting in for $\frac{r_1}{r_2}$ and so on until we arrive at the following:

$$\frac{a}{b} = a_0 + \frac{r_1}{b} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots \frac{1}{a_{n-1} + \frac{1}{a_n}}}}}} \tag{3.0.4}$$

Thus, every rational number, $\frac{a}{b}$, can be written as a finite continued fraction. □

The construction of a finite continued fraction is simply an application of Euclid's algorithm seen above. We will illustrate the steps in this process with the example $\frac{223}{51}$. The first step is to find a_0. This is found by dividing 223 by 51 and taking the floor of the result, which is 4. Now, we have $4 + \frac{19}{51} = 4 + \frac{1}{\frac{51}{19}}$. In the next step we need to find the continued fraction expansion for $\frac{51}{19}$. We continue using the Euclidean algorithm and find that $a_1 = 2$ because $51 = 2 * 19 + 13$. Next, we have $19 = 1 * 13 + 6$. Therefore, $a_2 = 1$. We will continue in this manner until the remainder is equal to 0. $13 = 2 * 6 + 1$ so $a_3 = 2$. $6 = 6 * 1 + 0$ which means two things $a_4 = 6$ and we are finished with the algorithm due to the remainder equaling 0. Since we have found all a_i in the continued fraction expansion of $\frac{223}{51}$ we can write

the following:

$$\frac{223}{51} = 4 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{6}}}} \tag{3.0.5}$$

The above was a very nice example in that it only took five partial denominators to write out the continued fraction expansion. This will not always be the case which is why one might write the continued fraction in the following manner.

$$\frac{223}{51} = [4; 2, 1, 2, 6] \tag{3.0.6}$$

This form of notation is obviously much easier to read and write and will as a result, be used quite a bit throughout this paper.

At this point it might seem that we could start looking at the continued fraction factoring algorithm, but we need a bit more information on continued fractions before we can do so. Therefore, we will take a look at the definition for a convergent.

Definition 3.0.2. *The continued fraction made from* $[a_0; a_1, a_2, \ldots, a_n]$ *by cutting off the expansion after the* k^{th} *partial denominator* a_k *is called the* k^{th} *convergent of the given continued fraction and denoted by* C_k*; in symbols,*

$$C_k = [a_0; a_1, a_2, \ldots, a_k] \quad 1 \leq k \leq n$$

We let the zeroth convergent C_0 *be equal to the number* a_0*.[2]*

If we go ahead and look at equation 3.0.5 from above, we have

$$\frac{223}{51} = 4 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{6}}}}$$

and the 2^{nd} convergent in this case is $[4; 2, 1] = 4 + \frac{1}{2 + \frac{1}{1}} = \frac{13}{3}$. Basically, we can think about the convergent of a continued fraction as adding up the partial denominators to a certain point. Remember that the k^{th} convergent will contain the first $k + 1$ partial denominators since the continued fraction starts with a_0. A convergent can be useful because we can look at how fast a certain fraction is zooming in on its actual value. Burton defines the equation for finding a certain convergent in the following manner,

Definition 3.0.3. *The k^{th} partial denominator can be defined in terms of p_k and q_k.*

$$\begin{aligned} p_0 &= a_0 & q_0 &= 1 \\ p_1 &= a_1 a_0 + 1 & q_1 &= a_1 \end{aligned}$$

and in general

$$\begin{aligned} p_k &= a_k p_{k-1} + p_{k-2} \\ q_k &= a_k q_{k-1} + q_{k-2} \end{aligned}$$

for $k = 2, 3, \ldots, n$.[2]

If we go ahead and compute the first few convergence of $[a_0; a_1, \ldots, a_n]$ we get

$$C_0 = a_0 = \frac{a_0}{1} = \frac{p_0}{q_0} \tag{3.0.7}$$

$$C_1 = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1} = \frac{p_1}{q_1} \tag{3.0.8}$$

$$C_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{a_2(a_1 a_0 + 1) + a_0}{a_2 a_1 + 1} = \frac{p_2}{q_2} \tag{3.0.9}$$

Theorem 3.0.2. *$C_k = \frac{p_k}{q_k}$ for $0 \leq k \leq n$.*

Proof. We have already seen that $C_k = \frac{p_k}{q_k}$ for $k = 0, 1$ and 2 in equations 3.0.7, 3.0.8, and 3.0.9. Now, let us assume that the above is true for $k = m$ where $2 < m < n$. That is, we are assuming that

$$C_m = \frac{p_m}{q_m} = \frac{a_m p_{m-1} + p_{m-2}}{a_m q_{m-1} + q_{m-2}} \tag{3.0.10}$$

and would like to prove that $C_{m+1} = \frac{p_{m+1}}{q_{m+1}}$. We know that C_{m+1} is equal to

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots \frac{1}{a_m + \frac{1}{a_{m+1}}}}} \tag{3.0.11}$$

which if written in the shorter notation is equal to $[a_0; a_1, \ldots, a_m, a_{m+1}]$. The key thing to notice is that C_{m+1} is also equal to $[a_0; a_1, \ldots, a_m + \frac{1}{a_{m+1}}]$. We can write C_{m+1} in this way because we are just turning two terms into one. We have not changed the equation at all. All we have done is changed the

number of terms from $m+2$ to $m+1$. At this point we will go ahead and rewrite a few things we know.

$$C_m = [a_0; a_1, \ldots, a_m] = \frac{a_m p_{m-1} + p_{m-2}}{a_m q_{m-1} + q_{m-2}}$$

and

$$C_{m+1} = [a_0; a_1, \ldots, a_m + \frac{1}{a_{m+1}}]$$

Now, it is important to understand that $p_{m-1}, p_{m-2}, q_{m-1}$ and q_{m-2} are independent of the last term in the continued fraction. If you do not see why look back at how p_k and q_k are defined in Definition 3.0.3. Since C_m and C_{m+1} are exactly the same up until the final term, then the equation $\frac{a_m p_{m-1}+p_{m-2}}{a_m q_{m-1}+q_{m-2}}$ will be exactly the same except for the term a_m[1]. The last term in the continued fraction for C_{m+1} is $(a_m + \frac{1}{a_{m+1}})$. Therefore

$$\begin{aligned}
C_{m+1} &= \frac{(a_m + \frac{1}{a_{m+1}})p_{m-1} + p_{m-2}}{(a_m + \frac{1}{a_{m+1}})q_{m-1} + q_{m-2}} \\
&= \frac{a_m p_{m-1} + \frac{p_{m-1}}{a_{m+1}} + p_{m-2}}{a_m q_{m-1} + \frac{q_{m-1}}{a_{m+1}} + q_{m-2}} \\
&= \frac{a_m p_{m-1} + p_{m-2} + \frac{p_{m-1}}{a_{m+1}}}{a_m q_{m-1} + q_{m-2} + \frac{q_{m-1}}{a_{m+1}}} \\
&= \frac{p_m + \frac{p_{m-1}}{a_{m+1}}}{q_m + \frac{q_{m-1}}{a_{m+1}}} \\
&= \frac{a_{m+1} p_m + p_{m-1}}{a_{m+1} q_m + q_{m-1}}
\end{aligned}$$

Thus, by induction

$$C_k = \frac{p_k}{q_k} \qquad \forall\ k \text{ s.t. } 0 \leq k \leq n \tag{3.0.12}$$

□

[1] a_m is the final term in the continued fraction.

Now that we have explored some of the basics of finite continued fractions it is time to go ahead and take a look at infinite continued fractions. The reason we need to be extremely interested in infinite continued fractions is because we will be dealing with irrational numbers in the CFRAC[2] algorithm. This means that we will not be using finite continued fractions directly since they represent rational numbers, but we will make use of them in understanding infinite continued fractions.

[2]The proof of this will be seen in the infinite continued fractions chapter.

Chapter 4

Infinite Continued Fractions

Infinite continued fractions are very similar to finite continued fractions in that they are written and can be represented almost the same. We will this through the following definitions from Burton.

Definition 4.0.4. *An infinite simple continued fraction is an expression of the form*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}}$$

where $a_0, a_1, a_2, \dots$ is an infinite sequence of integers, all positive except for possibly a_0.[2]

Definition 4.0.5. *An infinite simple continued fraction can be written as*

$$[a_0; a_1, a_2, \dots] \qquad k \geq 2 \quad [2]$$

As can be seen, infinite continued fractions contain a difference from finite continued fractions, and that is they go on forever. With a little bit more effort it is also possible to show that the k^{th} convergent of an infinite continued fraction is found in the same manner as in finite continued fractions. This is because we are only looking at the infinite continued fraction up to the k^{th} convergent, that is, we are now looking at a finite number of values. Therefore we can apply the same equations found for the k^{th} convergent of a finite continued fraction, so we have:

$$\frac{p_k}{q_k} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}} \tag{4.0.1}$$

We will now look at a few theorems which will help us prove a very important concept later.

Theorem 4.0.3. *For p_k, q_k defined as follows*

$$p_k = a_k p_{k-1} + p_{k-2}$$
$$q_k = a_k q_{k-1} + q_{k-2}$$

we have the following

$$(p_k)(q_{k-1}) - (p_{k-1})(q_k) = (-1)^{k-1} \qquad for k \geq 1 \tag{4.0.2}$$

Proof. For $k = 1$

$$\begin{aligned}(p_1)(q_0) - (p_0)(q_1) &= (a_1 a_0 + 1)(1) - (a_1 a_0) \\ &= 1 \\ &= (-1)^0\end{aligned}$$

Now assume that $p_j q_{j-1} - p_{j-1} q_j = (-1)^{j-1}$ holds. Then

$$p_{j+1} q_j - p_j q_{j+1} = (a_{j+1} p_j + p_{j-1}) q_j - p_j (a_{j+1} q_j + q_{j-1})$$

by substituting in for p_{j+1} and q_{j+1} from equation 4.0.1. Thus,

$$\begin{aligned}&= (a_{j+1} p_j q_j + p_{j-1} q_j) - (a_{j+1} p_j q_j + p_j q_{j-1}) \\ &= (a_{j+1} p_j q_j - a_{j+1} p_j q_j) + (p_{j-1} q_j - p_j q_{j-1}) \\ &= (p_{j-1} q_j) - (p_j q_{j-1}) \\ &= -(-1)^{j-1} \qquad \text{by our inductive hypothesis} \\ &= (-1)^j\end{aligned}$$

□

Theorem 4.0.4. *p_j and q_j do not have any factors in common. That is, $\frac{a_j p_{j-1} + p_{j-2}}{a_j q_{j-1} + q_{j-2}}$ is in reduced form.*

Proof. Assume that p_j and q_j do have factors in common, that is, $gcd(p_j, q_j) = k$, where $k > 1$. If this were true, then $(p_{j-1} q_j) - (p_j q_{j-1})$ is divisible by k. This of course cannot be true because we have already proved that $(p_{j-1} q_j) - (p_j q_{j-1}) = (-1)^j$. Since $(-1)^j$ is only divisible by 1 or -1 and not $k > 1$ then $gcd(p_j, q_j)$ must equal 1. Thus, by contradiction, p_j and q_j do not have any factors in common. □

Notice that in equation 4.0.1 if we let $k = j$ and divide both sides by $q_j q_{j-1}$ we have

$$\frac{p_{j-1}}{q_{j-1}} - \frac{p_j}{q_j} = \frac{(-1)^j}{q_j q_{j-1}}$$

which is equal to

$$\frac{p_j}{q_j} - \frac{p_{j-1}}{q_{j-1}} = \frac{(-1)^{j-1}}{q_j q_{j-1}} \tag{4.0.3}$$

It is apparent that the convergent of a particular continued fraction will alternate between being an over-approximation and an under approximation and will converge to some value. The alternating portion is due to $(-1)^{j-1}$. As far as converging to some value, we need to recall that the convergents are an approximation to the actual value of whatever we are approximating, say x. Since each convergent is an approximation of x and each convergent alternates between being an over-approximation and an under approximation then x will lie between successive convergents. As far as converging to some value, we know that $q_j q_{j-1}$ will increase as j increases due to $q_j = a_j q_{j-1} + q_{j-2}$ where a_j, $q_j > 0 \; \forall \; j > 0$. So, $\frac{(-1)^{j-1}}{q_j q_{j-1}}$ will converge to 0 as $q_j q_{j-1}$ becomes large enough meaning that the difference between two successive convergents is essentially 0. If the difference between successive convergents is essentially 0 then we know the results of these specific convergents will be equal to x.

At this point we are only missing one theorem to be able to prove the most important concept in this paper. That theorem was briefly mentioned at the end of chapter 3.

Theorem 4.0.5. *Infinite continued fractions represent irrational numbers.*

Proof. Suppose that

$$x = [a_o; a_1, a_2, \dots]$$

and

$$C_n = \frac{p_n}{q_n}$$

We have already seen that the value of x lies between two successive convergents, C_n and C_{n+1}, and that the absolute value of the difference between two successive convergents is equal to $\frac{1}{q_n q_{n-1}}$ so we have

$$0 < |x - C_n| < |C_{n+1} - C_n| = \frac{1}{q_n q_{n+1}}$$

The reason we know $|x - C_n| < |C_{n+1} - C_n|$ is because x lies between C_{n+1} and C_n, therefore the distance between x and C_n will be less than the distance between C_{n+1} and C_n.

If we assume that x is a rational number, then it can be written as $\frac{a}{b}$, meaning that we have

$$0 < |\frac{a}{b} - \frac{p_n}{q_n}| < \frac{1}{q_n q_{n+1}}$$

Now we will multiply by the common denominator between $\frac{a}{b}$ and $\frac{p_n}{q_n}$, bq_n.

$$0 < |aq_n - bp_n| < \frac{b}{q_{n+1}}$$

At this point we have our contradiction because if you recall q_{n+1} increases without an upper bound so if n is chosen to be large enough then

$$b < q_{n+1}$$

which implies that

$$\frac{b}{q_{n+1}} < 1 \tag{4.0.4}$$

meaning that, given our bounds, we have

$$0 < |aq_n - bp_n| < 1 \tag{4.0.5}$$

But this cannot be true because this says there exists a positive integer greater than 0 and less than 1. Thus, x must be an irrational number. □

Theorem 4.0.6. *If we are trying to approximate a real number, x, where $x > 1$ and the convergents are of the form $\frac{p_j}{q_j}$ then $|p_j^2 - x^2 q_j^2| < 2x$.*

Proof. We have already seen that the convergents alternate above and below the actual value in equation 4.0.3, meaning that our number x will be between $\frac{p_j}{q_j}$ and $\frac{p_{j+1}}{q_{j+1}}$. We also know that the absolute value of the difference between these two convergents is $\frac{1}{q_j q_{j+1}}$ for any value of j. So,

$$\begin{aligned} |p_j^2 - x^2 q_j^2| &= q_j^2 |\frac{p_j^2}{q_j^2} - x^2| \\ &= q_j^2 |x^2 - \frac{p_j^2}{q_j^2} \\ &= q_j^2 |x - \frac{p_j}{q_j}||x + \frac{p_j}{q_j}| \end{aligned}$$

The next step requires us to remember that the absolute value of the difference between two successive convergents is $\frac{1}{q_j q_{j+1}}$. The number we are trying

to approximate, x, is somewhere between these convergents. Therefore, the absolute value of the difference between x and one of these convergents is going to be less than $\frac{1}{q_j q_{j+1}}$. Furthermore, $\frac{p_j}{q_j}$ is going to be less than $x + \frac{1}{q_j q_{j+1}}$. The reason is because $\frac{p_j}{q_j} = x \pm |x - \frac{p_j}{q_j}$ since $|x - \frac{p_j}{q_j}$ is the difference between x and $\frac{p_j}{q_j}$. The $\pm$ sign is included because we are unsure as to whether or not $\frac{p_j}{q_j}$ is an under or over approximation. In this case we will assume that we are dealing with an over approximation. We can now substitute $\frac{1}{q_j q_{j+1}}$ in for $|x - \frac{p_j}{q_j}|$ which results in the following,

$$|p_j^2 - x^2 q_j^2| < q_j^2 \frac{1}{q_j q_{j+1}} \left(x + \left(x + \frac{1}{q_j q_{j+1}} \right) \right)$$

At this point we can see that if $\frac{p_j}{q_j}$ was instead an under-approximation, then the result would be $q_j^2 \frac{1}{q_j q_{j+1}} \left(x + \left(x - \frac{1}{q_j q_{j+1}} \right) \right)$ which is still less than $q_j^2 \frac{1}{q_j q_{j+1}} \left(x + \left(x + \frac{1}{q_j q_{j+1}} \right) \right)$. We can now combine our x terms together to obtain,

$$q_j^2 \frac{1}{q_j q_{j+1}} \left(x + \left(x + \frac{1}{q_j q_{j+1}} \right) \right) = q_j^2 \frac{1}{q_j q_{j+1}} \left(2x + \frac{1}{q_j q_{j+1}} \right)$$

Next we will subtract $2x$ from both sides of the equation and factor out $2x$ from the right side of the equation,

$$|p_j^2 - x^2 q_j^2| - 2x < 2x \left(-1 + \frac{q_j}{q_{j+1}} + \frac{1}{2x q_{j+1}^2} \right)$$

Since $x > 1$ we can remove $2x$ from the denominator of the last term resulting in

$$\begin{aligned} 2x \left(-1 + \frac{q_j}{q_{j+1}} + \frac{1}{2x q_{j+1}^2} \right) &< 2x \left(-1 + \frac{q_j}{q_{j+1}} + \frac{1}{q_{j+1}} \right) \\ &= 2x \left(-1 + \frac{q_j + 1}{q_{j+1}} \right) \end{aligned}$$

In this next step we will be making the assertion that $q_j + 1 \leq q_{j+1}$. This is true because $q_{j+1} = a_{j+1} q_j + q_{j-1}$ where q_{j-1} is a positive integer. So, we have

$$\begin{aligned} 2x\left(-1+\frac{q_j+1}{q_{j+1}}\right) &\leq 2x\left(-1+\frac{q_{j+1}}{q_{j+1}}\right) \\ &= 2x\,(0) \\ &= 0 \end{aligned}$$

If we add $2x$ to both sides we have,

$$|p_j^2 - x^2 q_j^2| < 2x \tag{4.0.6}$$

□

In the CFRAC algorithm we will be looking at factoring a number n by finding the continued fraction expansion of $\sqrt{n}$. Therefore, we will continue by showing that theorem 4.0.6 holds true when $x = \sqrt{n}$.

Theorem 4.0.7. *Suppose n is a positive integer which is not a perfect square with convergent $\frac{p_j}{q_j}$. Then $p_j^2 > 2\sqrt{n} \pmod{n}$.*

Proof. First, we apply theorem 4.0.6 and replace x by $\sqrt{n}$.

$$|p_j^2 - nq_j^2| < 2\sqrt{n}$$

by removing the absolute value sign we have

$$-2\sqrt{n} < p_j^2 - nq_j^2 < 2\sqrt{n}$$

Since we are reducing $\pmod{n}$ we have

$$-2\sqrt{n} < p_j^2 < 2\sqrt{n} \pmod{n} \tag{4.0.7}$$

□

This theorem is one of the reasons why the CFRAC algorithm works. We will see why later, but for now we will begin looking at some factoring algorithms.

Chapter 5

Factoring Algorithms

Before we start looking at the CFRAC algorithm, it is definitely worth mentioning a couple of algorithms that was a major contribution to its creation. The first algorithm is credited to Pierre de Fermat.

5.1 Fermat's Algorithm

The basic idea of Fermat's Algorithm is to factor n by trying to find an x and y such that

$$n = x^2 - y^2 = (x - y)(x + y) \tag{5.1.1}$$

To do this, we let x be the ceiling of $\sqrt{n}$. Then, compute $x^2 - n$. If the result is a perfect square then we are done. If not, then we increment x by 1 until $x^2 - n$ is a perfect square. The reason we start at the ceiling of $\sqrt{n}$ is because if we did not then $x^2 - n$ would be a negative number. An example illustrating Fermat's Algorithm is provided. In this example, $n = 319$, so we will start by letting $x = 18$ since 18 is the next integer greater than $\sqrt{319}$. If 18 does not provide a solution then we increase 18 by 1 and continue doing so until we obtain a perfect square. Thus,

$$18^2 - 319 = 5 \tag{5.1.2}$$
$$19^2 - 319 = 41 \tag{5.1.3}$$
$$20^2 - 319 = 81 \tag{5.1.4}$$

At this point we are done because 81 is a perfect square, the square root being equal to 9. Now we will substitute these values into $(x - y)(x + y)$ to find the factors of 319. We have $x = 20$ and $y = 9$ so $(20 - 9)(20 + 9) = (11)(29) = 319$. This algorithm works particularly well when the factors

of n are close to $\sqrt{n}$. This is a problem because of how the word "close" might mean within ± 100 of $\sqrt{n}$. If we were dealing with a 50 digit number this algorithm would then not be very helpful. So, a mathematician named Maurice Kraitchik decided to improve Fermat's Algorithm.

5.2 Kraitchik's Improvement

Maurice Kraitchik felt that a lot of time could be saved if instead of looking for an x and y that solves $x^2 - y^2 = n$, we look for a "random" x and y that solves $x^2 \equiv y^2 \pmod{n}$.[1] So, we have

$$x^2 - y^2 \equiv 0 \pmod{n} \tag{5.2.5}$$

This implies that n will divide $x^2 - y^2$ which is equal to $(x-y)(x+y)$ meaning that n and $x^2 - y^2$ share a common factor. To find an x and y that satisfy equation 5.2.5, we will try and solve the equation $x^2 \pmod{n} \equiv y^2$. That is, we will be plugging in values for x, reducing $\pmod{n}$, and hope that the result is a perfect square. As in Fermat's Algorithm, we will be letting x start at the ceiling of $\sqrt{n}$. So, we will now take a look at an example.

If we are trying to factor the number 2911 we start at the ceiling of $\sqrt{2911}$ which is 54. If $54^2 \pmod{2911}$ does not result in a perfect square then we proceed by increasing x by 1 until we arrive at a perfect square.

x	$x^2 \pmod{2911}$	Perfect Square?
54	5	No
55	114	No
56	225	Yes

Since $56^2 \pmod{2911}$ is a perfect square we are finished. We have $x = 56$ and $y = 15$ thus 2911 divides $(56 - 15)(56 + 15)$. We then compute the $gcd(56-15, 2911) = 41$. Now that we have seen an improvement on Fermat's factorization technique, we will proceed by looking at an improvement on Kraitchik's technique. This improvement is of course the continued fraction factoring algorithm, or CFRAC.

5.3 CFRAC Algorithm

The CFRAC algorithm was developed in 1975 by Michael Morrison and John Brillhart. CFRAC was the first known algorithm to successfully factor the seventh Fermat number which is $2^{2^7}+1$. The algorithm uses infinite continued fractions along with some other techniques to factor integers up to fifty digits

long. We start by finding the continued fraction expansion of $\sqrt{n}$ where n is the number we are trying to factor.

$$\sqrt{n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

Notice that we could have expanded $\sqrt{n}$ using shorthand notation instead, that is

$$\sqrt{n} = [a_0; a_1, a_2, a_3, \ldots]$$

If you recall from definition 3.0.1, the a_i terms are called partial denominators. We will also need to remember that definition 3.0.3 defines p_k as the numerator of the k-th convergent and that p_k is dependent upon a_k, p_{k-1} and p_{k-2}. These p_k terms represent possible values for x. Therefore, we can square these terms, p_k^2 while reducing $\pmod{n}$ to represent possible values for x^2.

So, once we have computed the continued fraction expansion of $\sqrt{n}$ we will be able to create a table of a_k, p_k and $p_k^2 \pmod{n}$ terms. Next, we will turn our attention to the p_k^2 terms and for each k we will determine the prime factorization of p_k^2. Once each p_k^2 term is factored we want to look for common prime factors. That is not to say that the prime factors have to be exactly the same, but that we want to find integers that appear more than once throughout our list of prime factors. If an integer appears only once throughout the list of prime factors, but it is raised to an even power then this number will be included. Once we have identified the numbers that appear more than once, or are raised to an even power, then we will create a set which includes these integers. We will call this set B. Before we go further in the algorithm, an example of how to find B is shown. For this example, assume the four b_k^2 terms and their prime factorizations are as follows:

$$\begin{aligned} b_1^2 &= 10 = 2 \cdot 5 \\ b_2^2 &= 6 = 2 \cdot 3 \\ b_3^2 &= 20 = 2^2 \cdot 5 \\ b_4^2 &= 35 = 5 \cdot 7 \end{aligned}$$

By observation it can be seen that 2 and 5 appear more than once in the above prime factorizations. Since 3 and 7 only appear once and are not raised to an even power they will not be included in B. Therefore, in this example,

$$B = \{2, 5\} \tag{5.3.6}$$

The set B tells us what prime factorizations we will be paying attention to. If a prime factorization contains at least one number that does not appear in B then that p_k^2 term will be ignored. In the above example p_2^2 and p_4^2 will be ignored since these prime factors contain 3 and 7 respectively which are not in the set B.

Now that we have an understanding of what the set B consists of, we can continue on in the algorithm. The next step is to convert each prime factorization that we are not ignoring into a vector form which we will call v_k. If we look back to our example and ignore $k = 2$ and $k = 4$, the vector form is as follows:

$$\begin{aligned} p_1^2 &= 10 = 2^1 \cdot 5^1 = (1,1) \\ p_3^2 &= 20 = 2^2 \cdot 5^1 = (2,1) \end{aligned}$$

Again, by observation we can see that the vector form is recording the exponents of each prime in the corresponding prime factorization. When writing out the set B, we write the integers in ascending order. These vectors will be needed in the next part of the algorithm.

The next part requires the addition of two or more vectors, v_k, to equal the zero vector modulus two. That is, we want to add two or more vectors so that each term in the resulting vector is an even number. If this can be achieved then we will move on to the next step. If not, then more a_k, p_k, and p_k^2 terms will need to be calculated. One thing to note is that if we do calculate more a_k, p_k and p_k^2 terms then we will want to reevaluate B because with the addition of more prime factorizations comes the possibility of increasing the size of B. So, say $v_h + v_m \pmod 2 = 0$ vector for some $h, m \geq 0$, then we will proceed by multiplying p_h and p_m which again represents x. Next we will multiply the prime factorizations corresponding to h and m. Since $v_h + v_m \pmod 2$ results in the zero vector, we know that the product of the prime factorizations of h and m will only contain even exponents. The multiplication of the prime factorizations represent possible values for y^2. The next step is to factor out a square term, which we will be able to do since we only have even exponents. Thus, we can write y^2 as an integer squared meaning that y is represented as the integer.

If $x \neq \pm y \pmod n$ then $gcd(x + y, n)$ is a nontrivial factor of n and if $x = \pm y \pmod n$ then a new set of vectors will need to be used. The above is quite a bit to take in, so we will now take a look at an example. In this example we will be trying to factoring $n = 8131$. Remember that we would normally be trying to factor a fifty or so digit integer with this algorithm so a four digit integer is relatively small.

We begin by finding the continued fraction expansion of $\sqrt{8131}$ up to five terms.

$$\sqrt{8131} \approx 90 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{1}{3}}}} \tag{5.3.7}$$

Next, we will create a table with five iterations of k.

k	0	1	2	3	4
a_k	90	5	1	4	3
$p_k \pmod{8131}$	90	451	541	2615	255
$p_k^2 \pmod{8131}$	-31	126	-35	54	-23

Now we want to look at the last row in the table and find the prime factorization for each value of k.

k	$p_k^2 \pmod{8131}$	Prime Factorization
0	-31	$(-1)(31)$
1	126	$(2)(3)^2(7)$
2	-35	$(-1)(5)(7)$
3	54	$(2)(3)^3$
4	-23	$(-1)(23)$

At first glance we see that -1, 2, 3 and 7 appear more than once. Therefore we will set $B = -1, 2, 3, 7$. This means we will be ignoring $k = 0$, 2, and 4 because there exist primes in these prime factorizations that do not appear in B. So, we will go ahead and look at the vector form for $k = 1$ and 3. The vector forms for $k = 1$ and 3 are

$$(0, 1, 2, 1) \text{ and } (0, 1, 3, 0) \text{ respectively} \tag{5.3.8}$$

If we add the two vectors in equation 5.3.8 and reduce the resulting vector modulus two the resulting vector is

$$(0, 1, 2, 1) + (0, 1, 3, 0) \equiv (0, 0, 1, 1) \pmod{2}$$

Since this is not the zero vector, we must go through more iterations of k. That is, we will continue by finding more partial denominators of $\sqrt{8131}$ and then create a larger table. In this case we will find two more partial denominators, meaning our table will contain two more iterations of k.

$$\sqrt{8131} \approx 90 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{3 + \cfrac{1}{7 + \frac{1}{1}}}}}} \tag{5.3.9}$$

Therefore, our table now consists of

k	0	1	2	3	4	5	6
a_k	90	5	1	4	3	7	1
$p_k \pmod{8131}$	90	451	541	2615	255	4400	4655
$p_k^2 \pmod{8131}$	-31	126	-35	54	-23	89	-90

and the corresponding prime factorization are as follows

k	$p_k^2 \pmod{8131}$	Prime Factorization
0	-31	$(-1)(31)$
1	126	$(2)(3)^2(7)$
2	-35	$(-1)(5)(7)$
3	54	$(2)(3)^3$
4	-23	$(-1)(23)$
5	89	89
6	-90	$(-1)(2)(3)^2(5)$

At this point we want to reevaluate our set B. It is apparent that $B = \{-1, 2, 3, 5, 7\}$ because of the addition of the prime 5 in $k = 6$ prime factorization. Thus, we will be ignoring $k = 0, 4, 5$, again because these prime factorizations contain primes that are not in the set B. The vector form for $k = 1, 2, 3, 6$ is as follows

$$(0, 1, 2, 0, 1), (1, 0, 0, 1, 1), (0, 1, 3, 0, 0) \text{ and } (1, 1, 2, 1, 0) \qquad (5.3.10)$$

Our goal now is to see if we can add any number of these vectors, while only using each vector once, together to obtain the zero vector. It may be helpful to reduce the vectors modulus 2 now. If we do so we obtain

$$(0, 1, 0, 0, 1), (1, 0, 0, 1, 1), (0, 1, 1, 0, 0) \text{ and } (1, 1, 0, 1, 0) \pmod 2$$

Notice that the addition of v_1, v_2, and v_6 reduced modulus 2 provides

$$(0, 1, 0, 0, 1) + (1, 0, 0, 1, 1) + (1, 1, 0, 1, 0) = (0, 0, 0, 0, 0) \pmod 2$$

Now that we have found a combination of vectors that added together equal the zero vector when reduced modulus 2 we can calculate x and y s.t. $x^2 \equiv y^2 \pmod n$. Remember, x is equal to the product of the $p_k \pmod n$ that correspond to the vectors used in obtaining the zero vector. Since we used the vectors corresponding to $k = 1, 2$, and 6 we will be multiplying p_1, p_2, and p_6. The result is:

$$x \equiv (451)(541)(4655) \equiv 7501 \pmod{8131}$$

Next we want to compute y^2. We do this by multiplying the prime factorizations corresponding to $k = 1, 2$, and 6.

$$\begin{aligned} y^2 &= [(2)(3)^2(7)] \cdot [(-1)(5)(7)] \cdot [(-1)(2)(3)^2(5)] \\ &= [(-1)^2(2)^2(3)^4(5)^2(7)^2] \\ &= [(2)^2(3)^4(5)^2(7)^2] \\ &= [(2)(3)^2(5)(7)]^2 \end{aligned}$$

This then implies that $y = [(2)(3)^2(5)(7)] = 630$. We now want to check to see if $x \equiv y \pmod{8131}$. If this condition is true, then we need to either add different vectors together to acquire the zero vector or run through more iterations of k. If the condition is false, then we are finished and have successfully factored 8131. In this case,

$$7501 \equiv \pm 630 \pmod{8131} \tag{5.3.11}$$

as seen here

$$7501 - 8131 \equiv -630 \pmod{8131} \tag{5.3.12}$$

So, we must decide whether or not to look for more combinations of vectors or to run through more iterations of k. It is evident that we must run through more iterations of k because we cannot create another combination of vectors to obtain the zero vector. The proof of this is based on logic. We are looking at the vectors

$$(0, 1, 2, 0, 1), (1, 0, 0, 1, 1), (0, 1, 3, 0, 0), (1, 1, 2, 1, 0) \tag{5.3.13}$$

Notice that if we reduce these vectors modulus two then we have

$$(0, 1, 0, 0, 1), (1, 0, 0, 1, 1), (0, 1, 1, 0, 0), (1, 1, 0, 1, 0) \tag{5.3.14}$$

Because there exists a 1 in the third position of the third vector while non of the other vectors contain a 1 in the third position it is clear that the third vector will not be used. We already know that the first, second, and fourth vectors achieve our goal, but we want to show that there are no others. Thus we need to explain why the addition of the first and second, first and fourth, and second and fourth vectors do not equal the zero vector. We can actually do better than this and explain why two vectors when reduced modulus two must be the exact same vector in order to obtain the zero vector. The reasoning is simply because all of the possible outcomes when adding the

same position of two vectors together are

$$\begin{aligned} 0+0 \pmod 2 &= 0 \\ 1+1 \pmod 2 &= 0 \\ 1+0 \pmod 2 &= 1 \\ 0+1 \pmod 2 &= 1 \end{aligned}$$

So, the only time a zero is the result is when you are adding $0+0$ or $1+1$ which implies the two vectors are exactly the same after reducing them modulus 2. Therefore, since none of the above vectors are exactly the same reduced modulus 2, there will not be any other combinations of vectors which lead to the desired result.

The next two partial denominators of $\sqrt{8131}$ are shown below.

$$\sqrt{8131} \approx 90 + \cfrac{1}{5+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{3+\cfrac{1}{7+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{8}}}}}}}}} \tag{5.3.15}$$

Based on the expansion above, we have the next two iterations of k as seen here,

k	0	1	2	3	4	5	6	7	8
a_k	90	5	1	4	3	7	1	1	8
$p_k \pmod{8131}$	90	451	541	2615	255	4400	4655	924	3916
$p_k^2 \pmod{8131}$	-31	126	-35	54	-23	89	-90	21	-10

As we calculate more values of k we are increasing our chances of obtaining a combination of vectors that result in the zero vector. At the same time, we are also making the process more difficult in the sense that the set B could become much larger, therefore causing the vectors to become longer. Regardless, we must find the prime factorizations for $k = 7$ and 8 and check to see if our set B has changed.

k	$p_k^2 \pmod{8131}$	Prime Factorization
0	-31	$(-1)(31)$
1	126	$(2)(3)^2(7)$
2	-35	$(-1)(5)(7)$
3	54	$(2)(3)^3$
4	-23	$(-1)(23)$
5	89	89
6	-90	$(-1)(2)(3)^2(5)$
7	21	$(3)(7)$
8	-10	$(-1)(2)(5)$

You will notice that B has not changed since the prime factorization for $k = 7$ and 8 have not introduced any primes that are not already included in B. So, we still have $B = \{-1, 2, 3, 5, 7\}$. The vector form of the first nine iterations of k not including $k = 0$, 4, and 5 are as follows[1].

k	$p_k^2 \pmod{8131}$	Vector Form
1	126	$(0, 1, 2, 0, 1)$
2	-35	$(1, 0, 0, 1, 1)$
3	54	$(0, 1, 3, 0, 0)$
6	-90	$(1, 1, 2, 1, 0)$
7	21	$(0, 0, 1, 0, 1)$
8	-10	$(1, 1, 0, 1, 0)$

It is evident that $v_6 + v_8 \pmod 2 =$ zero vector since v_6 and v_8 are exactly the same vector when reduced modulus two. As before, we will proceed by calculating x

$$x \equiv (4655)(3916) \pmod{8131} \equiv 7409 \pmod{8131}$$

and now y^2

$$\begin{aligned} y^2 &= [(-1)(2)(3)^2(5)] \cdot [(-1)(2)(5)] \\ &= [(-1)^2(2)^2(3)^2(5)^2] \\ &= [(2)^2(3)^2(5)^2] \\ &= [(2)(3)(5)]^2 \end{aligned}$$

In this case, we have $y = 30$. Since $7409 \neq \pm 30 \pmod{8131}$ we are finished. The factors of 8131 are found by evaluating one last step

$$gcd(7409 \pm 30, \quad 8131) = 47 \text{ or } 173 \tag{5.3.16}$$

We have successfully factored 8131 into (47)(173).

[1]The prime factorizations of $k = 0$, 4, and 5 contain primes that do not appear in B.

Chapter 6

CFRAC - A Deeper Look

Now that we are able to implement the algorithm it is important to understand why it works. Recall that we are trying to solve $x^2 \equiv y^2 \pmod{n}$ where $x \neq y \pmod{n}$. In the CFRAC algorithm we are letting the numerator of the convergents represent values for x. The reason we are using the numerator of the convergents is because of theorem 4.0.7. This theorem says that the numerator of the convergents squared is bounded. That is, the numerator of the convergents squared $\pmod{n}$ is going to be greater than $-2\sqrt{n}$ and less than $2\sqrt{n}$. This is important because this will in turn create smaller prime factorizations. If we did not have this bound then we might be having to try to find the prime factorization of a number that is 49 digits long. This, of course, is a problem because it is very difficult to factor numbers of this length.

So, we know that the numerators of the convergents squared are bounded which helps when finding the prime factorizations. We also know that these values are represented by x^2. What we will want to see next is that $x^2 \equiv y^2$ all the time in this algorithm. This is actually pretty obvious when we look at how x^2 and y^2 are determined. x^2 is determined by multiplying the numerator of the convergents squared that correspond to the vectors, v_k, that were used in obtaining the zero vector. y^2 is determined by multiplying the prime factorizations of the p_k terms. Thus, the CFRAC algorithm is generating numbers such that $x^2 \equiv y^2 \pmod{n}$. This is extremely helpful in that the algorithm is generating values of x where $x^2 \equiv y^2$. The difficult part in the algorithm is finding a combination of vectors which results in the zero vector mod 2. Although difficult, this part of the algorithm is very important as we have seen. The reason is because we want to be able to factor a square term out of the product of the prime factorizations so that we have something of the form t^2, where t is the product of the prime factorizations after factoring a square term out. We can then let $y = t$. The last step is to make sure that $x \neq y \pmod{n}$. If so then we are finished and have successfully factored n.

Chapter 7

Conclusion

The continued fraction factoring algorithm is a very powerful tool in factoring large numbers. Since this algorithm can be used to decrypt messages that were encoded using RSA[1] it may seem peculiar as to why it would be legal to implement these kinds of algorithms. One possible reason is because the developers of RSA and other security algorithms want to be confident that the information they are protecting is not at risk. If it so happens that someone is able to break a code, they are helping the security companies by letting them know that they need to upgrade their algorithms. We can hope that the person that breaks the code will inform the security companies rather than try to prosper from say, someone's bank account. This is due to the fact that informing the companies is legal and is usually rewarded with some kind of prize. This is the reason why RSA is constantly increasing the length of their numbers as new factoring algorithms are developed. So, it may seem that the continued fraction factoring algorithm is somewhat useless these days because RSA is now implementing numbers around 300 or even 600 digits. This is not entirely true because faster and better algorithms have been developed based on the idea of the CFRAC algorithm. It is also a very fun algorithm to use when you have some free time and would like to factor an integer that is less than fifty digits long.

[1]We are assuming that the RSA number is around fifty digits which is not the case these days.

Bibliography

[1] David M. Bressoud. *Factorization and Primality Testing.* Springer Verlag, New York, Inc., 175 Fifth Avenue, New York, NY 10010, 1989.

[2] David M. Burton. *Elementary Number Theory, Fourth Edition.* McGraw-Hill Companies, Inc., New York, 1998.

[3] Neil Koblitz. *A Course in Number Theory and Cryptography, Second Edition.* Springer Verlag, New York, Inc., 175 Fifth Avenue, New York, NY 10010, 1994.

[4] Carl Pomerance and Samuel S. Wagstaff Jr. *Implementation of the Continued Fraction Integer Factoring Algorithm.*

[5] Jorn Steuding and Rasa Slezeviciene. *Factoring with Continued Fractions, The Pell Equation, and Weighted Mediants.* 2003.