SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Integer Factorization

av

Rasmus Persson

2024 - No K6

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Integer Factorization

Rasmus Persson

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Gregory Arone

2024

Abstract: Integer factorization is crucial for understanding the security of the most widely known cryptosystems. These systems rely on the difficulty of factoring large integers. Therefore, it is important to understand the current methods for factoring integers, in order to know if the currently used encryption methods are still secure. In the first part of this thesis we present the idea of public key cryptography. In the second part we review some necessary theoretical background from abstract algebra. In the third and main part we present a selection of four methods for factoring integers. The simplest one is Pollard's $p-1$ algorithm. It works for some numbers, and highlights that for an integer $N = pq$ to be difficult to factor, we need to ensure that $p-1$ or $q-1$ does not factor into small primes. The other algorithms are based on trying to find a pair of numbers a and b so that N divides $a^2 - b^2$, but does not divide $a-b$ or $a+b$. If we find such a pair, we can factor N by finding $\gcd(a-b, N)$. The most sophisticated algorithm that we discuss is the number field sieve. It is currently the fastest method for factoring integers larger than 2^{450}. The details of the number field sieve are very complicated, and we only outline the main ideas behind this algorithm.

Contents

1. Introduction

The internet is used by billions of people every day to communicate and send information to each other. The information is sent all around the world through cables that are owned by companies and states. This means that everyone with access to the cable can see what information is being sent through them. However, there is a need to communicate and send information without anyone being able to read and tamper with the information. Some examples include bank transactions or state and business secrets. However, there are currently no good alternatives to the cables that run through all of the major countries of the world. They are either under constant surveillance, or they are controlled by states that do not have friendly relations with each other.

A part of the solution to this problem is to use cryptography to encrypt the messages and information to prevent any third parties from understanding the contents of the communication. However, even with this technology, there are often security and reliability issues that need to be considered when using cryptography to protect confidential communications. One of the most widely used and well-known cryptosystems is the RSA public-key cryptosystem, which is named after its public inventors. RSA relies on the fact that factoring large integers is much more time-consuming than finding large primes and performing arithmetic modulo for a large integer. However, computers are becoming faster and processing power is getting cheaper to rent or otherwise acquire. Therefore we still need to be aware of the methods of integer factorization for large numbers. We also need to know in what situations they are most efficient and useful. Then we can make sure that we still can rely on our current cryptosystems. The mathematics behind factoring large numbers relies for some methods on clever insights in the properties of the factors, like in Pollard's $p-1$ method (5.1). Surprisingly, some of the most powerful and useful methods for factoring large numbers rely on basic mathematical identities. However, those methods also need to be supplemented by methods for finding numbers with certain relationships like the quadratic (5.3) and number field sieve (5.4).

The thesis is outlined as follows. The first section is this introduction. The second section states the problem formulation. Afterward comes the motivation section. We will there briefly present the RSA public-key cryptosystem. We do this to give the necessary context to understand why we need to understand factorization algorithms. After that, we describe the necessary background theory that underlines the motivation as well as helps us to describe the factorization methods for example some of the properties of rings and quotient rings. We then proceed by describing four different factorization methods. This thesis is then concluded by a discussion and comparison of the four methods with their respective strengths and weaknesses.

2. Problem Formulation

We will present four different factorization methods for large integers. We will also list their respective advantages and disadvantages to compare them and discuss when they are appropriate to use in practice. To explain the factorization methods satisfactorily we will also give some theory of the mathematical concepts that are used in the different techniques.

3. Motivation - Applications to Cryptography

3.1. **Private- and Public-Key cryptosystems.** If two persons want to communicate without anyone else finding out what they are talking about; they can use cryptography to keep their messages secret. Historically this was achieved with private-key cryptography. This form of cryptography requires that the two persons, Bob and Alice, first meet and exchange the private key before they can begin to communicate. However, in the 1970s, public-key cryptography was born. In a public-key system, Bob has two keys, K^{Public} and K^{Private}. Bob can then give everyone access to the public key used for encryption. Alice can encrypt the messages with the public key and send them to Bob, which Bob can easily decrypt with the help of the private key [HPS16, p. xiii]. This method relies on the fact that the mathematical problem the cryptosystem uses is very easy to solve for Bob because Bob has an extra bit of information. Conversely, the problem is very hard to solve without this extra bit of information. Thus an eavesdropper, Eve, will have a hard time finding out the contents of the messages that Alice and Bob are sending each other.

3.2. **Finding Large Primes.** If we want to use a public-key cryptosystem, like for example the RSA cryptosystem, then Bob needs to find some very large prime numbers. This is possible for Bob to do since there exist several efficient methods that can give us a good indication of whether or not a number is prime or not. An example of a really simple method for checking primality is using Fermat's little theorem 4.6. It says that if $n > 2$ is a prime then we will have:

$$2^{n-1} \equiv 1 \mod n.$$

If $n > 2$ is a prime then it has to fulfill this condition. However, it is not a sufficient condition to determine primality. But in practice, this test can determine primality with a very high probability. There of course exist more sophisticated methods for primality testings. We also note that we can calculate:

$$a^{n-1} \mod n$$

in $2 \log_2 n - 1$ steps by squaring $a \mod n$ repeatedly and using the binary expansion of $n - 1$. This is sometimes called the fast powering algorithm [HPS16, p. 24].

3.3. **RSA.** One public-key cryptosystem is the RSA cryptosystem. It is the first invented public-key cryptosystem and also the most widely known. It is named after its public inventors: Ron Rivest, Adi Shamir, and Leonard Adleman. They described the cryptosystem in 1977 but the mathematician Clifford Cocks had developed an equivalent system in secret within the British intelligence unit GCHQ already in 1973.

In the RSA public key cryptosystem, Bob will have a secret key that is the primes p and q. His public key will be the numbers N and e. Bob can give his public key to anyone he wants to be able to receive encrypted messages from. The public key consists of the $N = pq$ and the encryption exponent e which is an integer that is relatively prime to $(p - 1)(q - 1)$. Let us say that Alice wants to send a message to Bob. She will take her plain text, or any sort of message, and convert it to an integer m between 1 and N. Then she encrypts it by calculating:

$$c \equiv x^e \mod N.$$

The integer c is called a ciphertext, which is what she will send to Bob. Bob can then just solve the congruence $x^e \equiv c \mod N$ for x and will then have recovered Alice's message m.

The RSA outlies as follows:

- Bob will take two large primes p and q, which will be known only to him.
- He then calculates $N = pq$ and creates an encryption exponent e with $\gcd(e, (p - 1)(q - 1)) = 1$. Bob has now created his public key (N, e) that he gives to everyone, both Alice and Eve will know it.
- Alice can now use Bob's public key to encrypt her message x by calculating $x^e \mod N$. We call the integer $c \equiv x^e \mod N$ the ciphertext. Alice then sends the ciphertext c to Bob.

- Bob can now decrypt the ciphertext by calculating d with
$$ed \equiv 1 \mod (p-1)(q-1).$$
- He can then calculate:
$$x' \equiv c^d \mod N.$$
He will then have recovered the unencrypted message x since $x' = x$.
- To summarize, it is very easy for one person who has a bit of extra information to solve the problem $x^e \equiv c \mod N$ for x but hard for everyone else, like Eve. This means that we can use this dichotomy to send someone messages only they can read. We will show that this is truly the case later with proposition 4.9.

3.4. **The reasons why it is easy for Bob to solve $x^e \equiv c \mod N$.** We have seen that Bob just needs to find the integer d such that $de \equiv 1 \mod (p-1)(q-1)$. This is something we will show how to do in proposition 4.8. The reason why it is enough for Bob to find d is described in proposition 4.9, which says that $x^{ed} = x \mod pq$ for all x.

3.5. **Factoring $N = pq$.** We know that it is easy for Bob, who knows the factoring of $N = pq$, to solve the congruence $x^e \equiv c \mod N$. But why can't Eve just factor N and solve it easily as well? If Eve tries to factor N by trying to divide it with every number starting from 2 then Eve will have to divide N a total of $O(\sqrt{N})$ times. Eve can of course divide by only primes instead and will then have to divide approximately $O\left(\frac{\sqrt{N}}{\log(\sqrt{N})}\right)$ times, as per the famous prime-counting approximation. This is clearly way slower for large N than performing the Euclidean algorithm for finding the modular inverse which will take a maximum of $2\log_2((p-1)(q-1))+2$ times to perform, as described by Hoffstein et al. ([HPS16, p. 13]). We will now continue this thesis by presenting and studying some algorithms that might bridge this gap and make factoring N significantly faster than the naive ways. To do that we will now first present the necessary theoretical background that the factorization methods rely on.

4. Theoretical Background

In this section, we will present some of the key theorems, propositions, and definitions that are used in the factorization algorithms.

4.1. **The Euclidean Algorithm.** We first begin by describing the Euclidean algorithm. This is because it is one of the key reasons why it is easier for Bob to solve $x^e \equiv c \mod N$ as previously described. We also need the Euclidean algorithm to help us show Bézout's identity later.

Theorem 4.1 (The Euclidean Algorithm [HPS16, p. 13])**.** *The Euclidean algorithm calculates the greatest common divisor (gcd) of two integers a and b with $a \geq b$. It will do this in a finite number of steps. The algorithm has the following steps:*

(1) *Let $r_0 = a$ and $r_1 = b$.*
(2) *Begin with letting $i = 1$ and calculate:*
$$r_{i-1} = r_i \cdot q_i + r_{i+1},$$
with $0 \leq r_{i+1} < r_i$. This is of course the same as dividing r_{i-1} by r_i and calculating the quotient and remainder. Here q_i is known as the quotient and r_{i+1} the remainder.
(3) *If $r_{i+1} = 0$ then $gcd(a, b) = r_i$.*
(4) *Otherwise we will increment i by 1 and repeat the step of calculating the quotient and remainder.*

The division in step 2 is repeated at most:

$$2\log_2(b) + 2$$

times, according to Hoffstein.

4.2. **The Chinese Remainder Theorem.** The Chinese remainder theorem is needed for us to show that the number d exists that Bob uses to decipher messages, as we mentioned in the motivation section. However, before that, we show Bézout's identity as that will make the task of showing the Chinese remainder theorem significantly easier.

Theorem 4.2 (Bézout's identity)**.** *If we have integers a and b with $a \geq b$ and let $c = \gcd(a, b)$ then there exists integers x and u such that:*

$$ax + by = c$$

.

Proof. Since we assumed that there exists a greatest common divisor c we must according to the Euclidean algorithm (4.1) have been able to do the following calculations where $a = r_0$ and $b = r_1$:

$$\begin{aligned} r_0 &= r_1q_1 + r_2 \\ r_1 &= r_2q_2 + r_3 \\ &... \\ r_{i-4} &= r_{i-3}q_{i-3} + r_{i-2} \\ r_{i-3} &= r_{i-2}q_{i-2} + r_{i-1} \\ r_{i-2} &= r_{i-1}q_{i-1} + r_i \\ r_{i-1} &= r_iq_i + r_{i+1} \end{aligned}$$

where $r_{i+1} = 0$ and $r_i = c$. We can then perform these steps backward and substitute all r_{i-a} until we get back to our original integers $a = r_0$ and $b = r_1$ while keeping track of the remainders and get:

$$\begin{aligned} r_i &= r_{i-2} + (-q_{i-1})r_{i-1} \\ &= r_{i-2} + (-q_{i-1})(r_{i-3} - r_{i-2}q_{i-2}) \\ &= r_{i-2} + (q_{i-1}q_{i-2})r_{i-2} + (-q_{i-1})r_{i-3} \\ &= (r_{i-4} - q_{i-3}r_{i-3}) + (q_{i-1}q_{i-2})(r_{i-4} - q_{i-3}r_{i-3}) + (-q_{i-1})r_{i-3} \\ &= r_{i-4} - q_{i-3}r_{i-3} + q_{i-1}q_{i-2}r_{i-4} - q_{i-1}q_{i-2}q_{i-3}r_{i-3} - q_{i-1}r_{i-3} \\ &= (1 + q_{i-1}q_{i-2})r_{i-4} + (-q_{i-3} - q_{i-1}q_{i-2}q_{i-3} - q_{i-1})r_{i-3} \\ &= ... \\ &= (q_{i-1}q_{i-2} + ...)r_0 + (-q_{i-3} - q_{i-1}q_{i-2}q_{i-3} - q_{i-1} - ...)r_1. \end{aligned}$$

With that, we have found our x and y and thereby the proof is complete. □

We are now ready to describe the Chinese remainder theorem.

Theorem 4.3 (Chinese Remainder Theorem [HPS16, p. 83])**.** *If we have multiple linear congruences:*

$$x \equiv a_i \mod m_i$$

where $m_1, m_2, ...m_k$ are integers and m_i is pairwise relatively prime with all m_j where $i \neq j$. Meaning:

$$gcd(m_i, m_j) = 1 \text{ where } i \neq j.$$

Also let $a_1, a_2, ...a_k$ be integers. Then all the linear congruences will have a solution $x = c$ and if it has another solution $x = c'$ then:

$$c \equiv c' \mod \prod_{i=1}^{k} m_i.$$

Proof. For a system with only one congruence, we can select a_1 as a solution. Systems with more than one congruence require a bit to solve. We will begin by looking at systems with two congruences. We know that Diophantine equations on the form:

$$ax + by = c$$

have a solution if the greatest common divisor of a and b divides c (4.2). This means that we are able to find two integers n_1, n_2 such that:

$$n_1 m_1 + n_2 m_2 = 1$$

because we know from our assumptions that m_1 and m_2 are coprime. With this, we can create solutions to a system with two linear congruences:

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \end{aligned}$$

A solution is given by:

$$x = a_1 n_2 m_2 + a_2 n_1 m_1$$

since

$$x = a_1 n_2 m_2 + a_2 n_1 m_1$$

we now use the fact that $n_1 m_1 + n_2 m_2 = 1$ and get:

$$\begin{aligned} &= a_1(1 - n_1 m_1) + a_2 n_1 m_1 \\ &= a_1 - a_1 n_1 m_1 + a_2 n_1 m_1 \\ &= a_1 + (a_2 - a_1) n_1 m_1. \end{aligned}$$

Here we clearly see that $x - a_1$ is divisible by m_1 and that we can repeat the steps but with a_2 instead of a_1 to show that it is a solution to the second congruence. Now let our particular solution be noted by c and assume that there exists another solution c'. We have that:

$$\begin{aligned} m_1 &\mid c' - c \\ m_2 &\mid c' - c \end{aligned}$$

since m_1 and m_2 are coprime we have that

$$m_1 m_2 \mid c' - c$$

thereby we have

$$c \equiv c' \mod m_1 m_2.$$

This means that a system of k systems can be reduced to solve one less congruence because any pair of them will always have a solution. Furthermore, since all m_i are coprime, it is also coprime to $m_j \cdot m_k$ where $i \neq j, k$. Therefore by iteration, we will get the solution to the whole system and also get:

$$c \equiv c' \mod \prod_{i=1}^{k} m_i..$$

Thereby have we proven the Chinese remainder theorem. □

4.3. **Modular Inverse and the Fermat-Euler Theorem.**

Definition 4.1 (Euler's Totient Function [HPS16, p. 22])**.** The function $\varphi(n)$ counts the number of positive integers that are relatively prime to n and less than the integer n. This function is known as Euler's totient function or sometimes Euler's phi function.

Theorem 4.4 (Multiplicativity of Euler's Totient Function [, p.])**.** *Euler's totient function is multiplicative with $\varphi(pq) = \varphi(p)\varphi(q)$ if p and q are relatively prime.*

Proof. We will only show the case when p and q are primes. Let S_{pq} be the set of positive integers that are less than pq. We have:

$$S_{pq} = \{1, 2, ..., pq - 1\}.$$

The set of numbers that are not relatively prime to pq is the set of numbers:

$$S_p = \{p, 2p, ..., (q - 1)p\}$$

and

$$S_q = \{q, 2q, ..., (p - 1)q\}.$$

These sets do not overlap. Because if p and q are relatively prime they can not be equal to each other. So we have $p \neq q$. Therefore $S_p \cap S_q = \emptyset$. This means that:

$$\begin{aligned}\varphi(pq) &= \text{the number of elements in the set } S_{pq} - S_p - S_q \\ &= pq - 1 - (q - 1) - (p - 1) \\ &= pq - q - p + 1 \\ &= (p - 1)(q - 1)\end{aligned}$$

With that, the proof is complete since $\varphi(p) = p - 1$ if p is a prime. □

Theorem 4.5 (Fermat-Euler Theorem [, p.])**.** *Let a and n be positive integers with $\gcd(a, n) = 1$ and let $\varphi(n)$ be Euler's totient function (4.1). Then:*

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Proof. Let $R_x = \{x_1, x_2, ..., x_{\varphi(n)}\}$ be all integers where $1 \leq x_i < n$ and $\gcd(x_i, n) = 1$, meaning all positive integers that are coprime with n. Furthermore, let $aR_x = \{ax_1, ax_2, ..., ax_{\varphi(n)}\}$ with $1 \leq x_i < n$ and $\gcd(x_i, n) = 1$. We have that $\gcd(a, n) = 1$ and $\gcd(x_i, n) = 1$. This means that both a and x_i are coprime with n and have no common factors with n. If we multiply the integers they still will not have any common factors with n so we have that $\gcd(ax_i, n) = 1$. If we reduce aR_x by mod n to the least residue we would have that the elements of $aR_x \mod n$ would all be between 1 and less than n. Furthermore, all elements would be coprime to n and the number of elements is exactly the same as R_x. We also know that all the elements are unique since if we had, for $i \neq j$ that:

$$ax_i \equiv ax_j \mod n$$

we arrive at a contradiction that

$$a(x_i - x_j) \equiv 0 \mod n$$

which can not be true since a is coprime n and both x_i and x_j are less than n they can not be a multiple of n. This implies that:

$$\prod_{1}^{\varphi(n)} x_i \equiv \prod_{1}^{\varphi(n)} ax_i = a^{\varphi(n)} \prod_{1}^{\varphi(n)} x_i \mod n$$

since the products are coprime to n we can divide both sides with it and get

$$1 \equiv a^{\varphi(n)} \mod n.$$

With that the proof is complete.

□

Theorem 4.6 (Fermat's Little Theorem [HPS16, p. 30])**.** *Let p be a prime and a an integer with* $\gcd(p, a) = 1$. *Then:*

$$a^{p-1} \equiv 1 \mod p$$

Proof. This is a special case of the Fermat-Euler theorem (4.5) since $\varphi(p) = p - 1$ if p is a prime. This is because all other integers are coprime to a prime. □

Theorem 4.7 (Euler's Formula for pq [HPS16, p. 118])**.** *Let $n = pq$ with p and q as two different primes and let a be an integer with:*

$$gcd(a, n) = 1.$$

Then:

$$a^{(p-1)(q-1)} \equiv 1 \mod pq.$$

Proof. This also follows from the Fermat-Euler theorem (4.5) as $\varphi(pq) = (p-1)(q-1)$, like we showed in theorem 4.4. With that the proof is complete. □

Proposition 4.8 ([HPS16, p. 20])**.** *For the integers a and $m \geq 1$, there exists an integer b such that:*

$$ab \equiv 1 \mod m$$

if and only if:

$$gcd(a, m) = 1.$$

Proof. We know from Bezout's identity (4.2) that if $\gcd(a, m) = 1$ then there exist integers u and v such that:

$$au + mv = 1.$$

To find u and v we just have to perform the Euclidean algorithm in reverse. Therefore $au - 1 = -mv$. Since $-mv$ is obviously divisible by m then $au - 1$ must also be divisible by m. By the definition of congruence, we now have that:

$$au \equiv 1 \mod m.$$

We now let $u = b$, which completes the first direction of the proof.

Let us now assume that there exists a modular inverse b such that:

$$ab \equiv 1 \mod m$$

. Then, by the definition of congruence, we have that:

$$ab - 1 = cm$$

for some integer c. $\gcd(a, m)$ must obviously divide both a and m and because:

$$ab - cm = 1$$

it must also divide the right-hand side of the equation. The right-hand side of the equation is 1 in this case so the only possible $\gcd(a, m)$ is 1. We have now proved the proposition.

□

Proposition 4.9 ([HPS16, p. 120])**.** *If p and q are distinct primes and let e satisfy:*

$$gcd(e, (p-1)(q-1)) = 1.$$

Proposition 4.8 says that e will have an inverse d so that:

$$de \equiv 1 \mod (p-1)(q-1).$$

Then for any integer c the congruence:

$$x^e \equiv c \mod pq$$

has the solution:

$$x \equiv c^d \mod pq.$$

Proof. Since $c \equiv x^e \mod pq$, we are able to restate $c^d \equiv x \mod pq$ as:

$$(x^e)^d \equiv x \mod pq \iff$$
$$x^{de} \equiv x \mod pq.$$

We can now let $g = \gcd(x, pq)$. There are four possible values for g. This is because p and q are distinct primes so our values for g are:

$$1, p, q, pq.$$

We begin by studying the case where $g = 1$. Euler's formula for pq 4.7 then tells us that:

$$x^{(p-1)(q-1)} \equiv 1 \mod pq.$$

We also know that since:

$$de \equiv 1 \mod (p-1)(q-1),$$

there must exist an integer k such that:

$$de = 1 + k(p-1)(q-1).$$

We now have:

$$\begin{aligned} x^{de} &\equiv x^{1+k(p-1)(q-1)} && \mod pq \\ &\equiv x \cdot \left(x^{(p-1)(q-1)}\right) && \mod pq \\ &\equiv x \cdot 1 && \mod pq. \end{aligned}$$

Thereby the proof for the case where $g = 1$ is complete. Now let us assume that $g = \gcd(x, pq) = p$. This means that:

$$x \equiv 0 \mod p$$

and

$$x \not\equiv 0 \mod q.$$

The Chinese remainder theorem 4.3 means that we can show that:

$$x^{ed} \equiv x \mod pq$$

by showing that:

$$x^{ed} \equiv x \mod p$$

and

$$x^{ed} \equiv x \mod q.$$

Since:

$$x \equiv 0 \mod p$$

we can quickly see that

$$x^{ed} \equiv x \equiv 0 \mod p.$$

Since:

$$de \equiv 1 \mod (p-1)(q-1)$$

the Chinese remainder theorem 4.3 implies that:

$$de \equiv 1 \mod (q-1).$$

We can now apply the same arguments as with $g = 1$, and there must exist an integer k such that:

$$de = 1 + k(q-1).$$

We now, thanks to Fermat's little theorem 4.6, have:

$$\begin{aligned} x^{de} &\equiv x^{1+k(q-1)} && \mod q \\ &\equiv x \cdot x^{(q-1)} && \mod q \\ &\equiv x \cdot 1 && \mod q. \end{aligned}$$

The case where $g = q$ is shown the same way. Thereby we have shown this proposition for the case where $g = p$ and $g = q$. The case where $g = pq$ is straightforward since if:

$$x \equiv 0 \mod pq$$

we can quickly see that

$$x^{ed} \equiv x \equiv 0 \mod pq.$$

Therefore the proof is complete. □

We can now clearly see that because of proposition 4.9, it will truly be very easy for Bob solve the congruence since it will be straightforward for Bob to use Euler's algorithm and get the modular inverse d.

4.4. **Number of roots to a quadratic residue.**

Definition 4.2 (Quadratic residue [Kyl17, p. 1])**.** A number a is called a quadratic residue $\mod p$ if it is a square of another number $b \mod p$. If on the other hand, a is not a square $\mod p$ then it is called a quadratic nonresidue.

Proposition 4.10 (Number of roots to a quadratic residue [Kyl17, p. 1])**.** *If a number a is a quadratic residue $\mod p$ and $gcd(a, p) = 1$. Then it will have two roots if p is an odd prime. If p is even it will have one solution.*

Proof. We begin by looking at the case where p is odd. If there exists a solution to the quadratic residue $x^2 \equiv a \mod p$ then an equivalent statement is that $x^2 - a$ has roots modulo p. If we assume that there exist a square root b to a in modulo p then we have:

$$x^2 - a \equiv (x + b)(x - b) \mod p.$$

Since p is a prime we know that the equation

$$(x + b)(x - b) \equiv 0 \mod p$$

is equivalent to

$$x + b \equiv 0 \mod p$$

or

$$x - b \equiv 0 \mod p.$$

If p was not prime then we would not be able to split the equation like this. This means that the only roots to:

$$x^2 - a \mod p$$

are

$$x \equiv \pm b \mod p.$$

We can also deduce that $b \not\equiv -b \mod p$ since if:

$$b \equiv -b \mod p$$

then it would imply that

$$2b \equiv 0 \mod p.$$

If p is an odd prime we obviously have that

$$2 \neq p.$$

Therefore we have that

$$b \equiv 0 \mod p.$$

But this leads to a contradiction since we assumed that

$$b^2 \equiv a \mod p.$$

However, if p is an even prime then we would have that

$$p = 2.$$

Then all b satisfy the congruence and the argument does not hold for that particular case.

Let us now try to understand how many solutions there exist to the congruence when $p = 2$. We have assumed that:

$$\gcd(a, p) = 1.$$

This implies that:

$$a \neq 0$$

for every p and

$$a \neq 2$$

when $p = 2$. It also implies that x^2 is not divisible by 2 since if it were then a would have to equal 0. Then a must be an odd number and we know that an odd number subtracted by another odd number is even. In the least residue system, we only use one representative for each residue class modulo n. Therefore 1 is the only odd number that is an eligible solution. Therefore the solution to the congruence

$$x^2 \equiv a \mod 2,$$

is

$$x^2 \equiv a \equiv 1 \mod 2$$

which is to say that

$$x \equiv 1.$$

We have thereby proved that there only exist two solutions to:

$$x^2 \equiv a \mod p$$

for odd primes and one for when $p = 2$. □

4.5. **Rings and Ideals.** The number field sieve is the factorization method that uses a ring that is larger than integers. Since this factorization method relies substantially on rings we will begin this section by covering the necessary theory on rings and quotient rings. The number field sieve is the fastest factorization method as long as N is large enough and p and q are roughly the same size.

Definition 4.3 (Ring [HPS16, p. 95])**.** A ring is a set with two operations, usually denoted by $+$ for the additive operation and $\star$ for the multiplicative operation. The operation $+$ will have the following properties:

- The ring contains an additive identity element 0 such that:

$$0 + a = a + 0$$

for every a in the ring.

- The ring contains an additive inverse element b such that:
$$b + a = a + b = 0$$
for every a in the ring.
- The associative property.
- The commutative property.

The operation $\star$ only needs the associative property for the definition of a ring. However, we will only work with commutative rings with multiplicative identity. To be less verbose, everything referred to as a ring henceforth in this thesis will be a ring with those properties as well. Therefore our rings have the following properties:

- The ring contains a multiplicative identity element 1 such that:
$$1 \star a = a \star 1 = a$$
for every a in the ring.
- The associative property.
- The commutative property.

Instead of writing $a \star b$ we will note it as ab for the multiplicative operation.

Definition 4.4 (Field [HPS16, p. 96])**.** A field is a ring (a commutative ring with multiplicative identity) where for every nonzero element a there exists a multiplicative inverse for the operation $\star$ such that:
$$a \star \frac{1}{a} = 1$$
and
$$\frac{1}{a} \star a = 1.$$

Definition 4.5 (Unit [HPS16, p. 97])**.** If we let R be a ring then an element u in the ring is called a unit if there exists another element v in the ring such that:
$$u \star v = 1.$$
If some element a in R is not a unit and for every factorization of
$$a = b \star c$$
either b or c is a unit, then a is said to be irreducible.

Example 4.1. An example of units, if we look at the ring of integers $\mathbb{Z}$, is 1 and -1 as $1 \star 1 = 1$ and $-1 \star -1 = 1$. They are the only units in $\mathbb{Z}$. In $\mathbb{Z}$ the prime numbers are irreducible elements as they can only be factored as themselves multiplied by 1. For example:
$$7 = 7 \star 1.$$

Definition 4.6 (Ideal [Wal01, p. 168])**.** Let I be an additive subgroup of the ring R. We call the additive subgroup I an ideal if it has the properties described below.

For all
$$x \in R$$
and all
$$a \in I$$
we have that
$$ax, xa \in I.$$

This means that R itself is an ideal to R. The subgroup 0 consisting only of the additive element 0 in R is also an ideal. We call an Ideal proper if we have that:

$$I \neq R$$

Example 4.2. We can note that for the ring of integers $\mathbb{Z}$, all sub-rings $m\mathbb{Z}$ will be an ideal of $\mathbb{Z}$. Clearly, if we take some number m and multiply it with another integer that number will still be a multiple of m.

Definition 4.7 (Congruence in rings [Hun13, p. 145])**.** Let I be an ideal in a ring R and let $a, b \in R$. Then a is congruent to b modulo I if $a - b \in I$.

Theorem 4.11 (The relation of congruence modulo I [Hun13, p. 146])**.** *Let I be an ideal in a ring R. Then the relation of congruence modulo I is:*

(1) *reflexive, meaning $a \equiv a \mod I$ for every $a \in R$*
(2) *symmetric, meaning if $a \equiv b \mod I$ then $b \equiv a \mod I$*
(3) *transitive, meaning if $a \equiv b \mod I$ and $b \equiv c \mod I$ then $a \equiv c \mod I$*

Proof. We will now show the 3 different cases.

(1) Since $a - a = 0$ and 0 would always be in the ideal due to the definition ideal. An additive subgroup would always contain the identity element which for addition is 0. So we have $0 \in I$. Since $a - a \in I$ and per 4.7 we have proven that $a \equiv a \mod I$.
(2) Since $a \equiv b \mod I$ then there exists an element $a - b = i \in I$ per 4.7. Per the definition of ideals, $-i$ would also be in the ring. Therefore $b - a = -i \in I$ which per the definition of congruence for rings means that $b \equiv a \mod I$ and we have proven symmetry.
(3) By the definition of congruence there exists elements $i, j \in I$ such that $a - b = i$ and $b - c = j$. Conveniently if we study $i + j$ we get:

$$i + j = a - b + b - c = a - c$$

Since a group is closed under addition we know that $i + j \in I$. Per the definition of congruence in rings, we know that $a \equiv c \mod I$. With that, the proof is complete.

□

Theorem 4.12 (Ideal cosets [Hun13, p. 147])**.** *Let I be an ideal in a ring R and let a, $c \in R$. Then $a \equiv c \mod I$ if and only if $a + I = c + I$*

Proof. There are two cases we need to show to prove this theorem. The first one is where we first assume that $a \equiv c \mod I$ and show that this implies that $a+I = c+I$. The second case is the other way around where we assume $a+I = c+I$ and show that this implies that $a \equiv c \mod I$. We begin by proving the first case. To prove this we are going to first show that $a + I \subseteq c + I$ and via symmetry that $c + I \subseteq a + I$. Let us begin by assuming that $a \equiv c \mod I$. Since $a + I$ is the congruence class of a modulo I that is, a subset of I. We can choose an element b that belongs to the same congruence class. So that $b \in a + I$. By definition, we have:

$$b \equiv a \mod I.$$

Due to transitivity 4.11 we then have:

$$b \equiv c \mod I.$$

This implies that $b \in c + I$ which means that $a + I \subseteq c + I$. If we reverse the roles a and c we also have that $c + I \subseteq a + I$ which means that:

$$a + I = c + I.$$

Now we will show the second case where we begin by assuming that $a+I=c+I$. By reflexivity, we know that the element a is congruent to itself modulo I, $a \equiv a \mod I$. We have that $a \in a+I$ but since $a+I=c+I$ we also have $a \in c+I$. This means that $a \equiv c \mod I$ and the proof is complete. □

Definition 4.8 (Quotient Rings [Wal01, p. 173])**.** Let R have an ideal I. We say that R/I is the set of cosets of I in R. We define two binary operations for R/I as:

$$(x+I)+(y+I)=x+y+I$$

for the additive operation and

$$(x+I)(y+I)=xy+I$$

for the multiplicative operation.

That means that R/I is a ring and this type of ring is known as a factor ring or quotient ring.

Example 4.3. For example, if the ring $R=\mathbb{Z}$ and ideal $I=m\mathbb{Z}$. Then R/I would be the congruence classes modulo m. This means we would have:

$$R/I=\mathbb{Z}/m\mathbb{Z}=\{\overline{0}_m,\overline{1}_m,...,\overline{m-1}_m\}.$$

Example 4.4. We will show an example of multiplication and addition for the ring $Z[x]/(f(x))$. Let $f(x)=1+3x-2x^3+x^4$. We now want to add the elements u and v in the ring. Let:

$$u=2-4x+7x^2+3x^3$$

and

$$v=1+2x-4x^2-2x^3.$$

To add them we just add the coefficients since the degree of the elements is lower than $f(x)$. We get:

$$u+v=3-2x+3x^2+x^3.$$

To multiply we first multiply u and v outside of the quotient ring so we get:

$$uv=2-9x^2+29x^3-14x^4-26x^5-6x^6.$$

Then we perform a polynomial division of uv by $f(x)=1+3x-2x^3+x^4$ and only keep the remainder. This is because uv before the division will have a higher degree than $f(x)$ and thus we need to find what congruence class it actually belongs to. We then finally get:

$$uv=92+308x+111x^2-133x^3.$$

Theorem 4.13 (Congruence modulo $p(x)$ in $F[x]$[Hun13, p. 127])**.** *Let F be a field and $p(x)$,$g(x)$ and $f(x)$ be polynomials in $F[x]$ and $p(x)$ be nonzero. Then $f(x) \equiv g(x) \mod p(x)$ if and only if they belong to the same congruence class that is $f(x)+I=g(x)+I$ or using brackets to symbolize congruence classes $[f(x)]=[g(x)]$.*

Proof. This proof is identical in method to the proof in 4.12. □

Theorem 4.14 (Distinctness of congruence classes modulo $p(x)$ in $F[x]$[Hun13, p. 128])**.** *Let F be a field and $p(x)$ be a polynomial in $F[x]$ with degree n. Let $r(x)$ be the reminder when a polynomial in $F[x]$ is divided by $p(x)$. Let S be the set consisting of the zero polynomial and all the polynomials of degree less than n in $F[x]$. Then every congruence class modulo $p(x)$ is the class of some polynomial in S, and the congruence classes of different polynomials in S are distinct.*

Proof. Let $r(x)$ be the reminder when dividing a polynomial in $F[x]$ with $p(x)$. $r(x)$ will be the zero polynomial or a nonzero polynomial with degree less than n.

There are multiple ways of reaching this conclusion, for example taking a close look at the division algorithm for polynomials. Another way is to consider that the reminders will be in the ring $\mathbb{F}[x]/p(x)$. The ideal of this rings are all multiples of $p(x)$, of course including multiples of other non stationary polynomials. Therefore, the elements in the ring consists of the zero polynomial and polynomials with a degree less than n. Therefore we know that $r(x) \in S$. Two remainders $r_1(x)$ and $r_2(x)$ will not be congruent modulo $p(x)$ as the degree of $r_1(x) - r_2(x)$ will also be less than n and therefore not divisible by $p(x)$. Theorem 4.13 then tells us that all polynomials in S belong to distinct congruence classes. □

Example 4.5. Let's take a look at an interesting example that will highlight a property that will come in handy later in this thesis. The ring $\mathbb{R}[x]/(x^2+1)$ consist of all congruence classes modulo x^2+1 for all polynomials with real coefficients. This equivalent with saying that the ring consist of all polynomials that are reminders after division with x^2+1. The reminders after division will be on the form $(rx+s)+I$, where $r, s \in \mathbb{R}$. This is because, as shown above, the degree of the reminder will be lower than x^2+1. Now for the interesting insight: Theorem 4.13 shows that all congruence classes can be uniquely stated on the form $(rx+s)+I$.

Definition 4.9 (Homomorphism [Hun13, p. 75])**.** A ring R is homomorphic to a ring S if there is a function $f : R \to S$ with the property:

$$f(a+b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b) \text{ for all } a, b \in R$$

A homomorphism is an unital homomorphism if the identity element in a ring R is mapped to the ring S by the function f.

Definition 4.10 (Isomorphism [Hun13, p. 72])**.** A ring R is isomorphic to a ring S if there is a homomorphism $f : R \to S$ with the extra properties that:

(1) f is injective.
(2) f is surjective.

Definition 4.11 (Kernel [Hun13, p. 154])**.** Let $f : R \to S$ be a homomorphism of rings. Then the kernel of f is the set K that is defined by:

$$K = \{r \in R | f(r) = 0\}$$

Theorem 4.15 (The Natural Homomorphism [Hun13, p. 156])**.** *Let I be an ideal in a ring R. Then the map $\pi : R \to R/I$ given by $\pi(r) = r + I$ is a surjective homomorphism with kernel I.*

Proof. We know that the map is surjective as for every $r \in R$ we of course have a corresponding coset $r + I$ since r is on both sides of the equal sign. In other words, for any given coset $r+I$ in R/I we have have $\pi(r) = r+I$. We can also quite easily show that it is a homomorphism, beginning with addition:

$$\pi(r+s) = (r+s) + I = (r+I) + (s+I) = \pi(r) + \pi(s)$$

Continuing with multiplication:

$$\pi(rs) = rs + I = (r+I)(s+I) = \pi(r)\pi(s)$$

and with that the proof is complete. □

Theorem 4.16 (First Isomorphism Theorem [Hun13, p. 157])**.** *Let $f : R \to S$ be a surjective homomorphism of rings with kernel K. then the quotient ring R/K is isomorphic to S.*

Proof. Our strategy to prove this is by defining a function φ from R/K to S and show that it's an isomorphism based on what we know of rings and f. Let's define φ as:

$$\varphi(r+K) = f(r)$$

where $r \in R$. We could potentially have many different representatives for the congruence class $r+K$. So we now need to show that this function only depend on the congruence class and not the representative for the congruence class. If the function φ does depend on the representative then φ would not define a function as one element in R/K would be mapped to more than one element in S.

Let t be different representatives for the congruence class $r+K$. This means that:

$$r+K = t+K.$$

Theorem 4.12 tells us that:

$$r \equiv t \mod K.$$

Which by the definition of congruence means that:

$$r - t \in K.$$

Also, since f is a homomorphism we also have that:

$$f(r) - f(t) = f(r-t)$$

and together with we fact that $r - t \in K$ have

$$f(r-t) = 0.$$

Which means that we now know that:

$$r+K = t+K \implies f(r) = f(t).$$

Therefore the function φ is well defined. We will now proceed to show that φ is surjective (1), injective (2) and a homomorphism (3).

(1) Let $s \in S$, this implies that $s = f(r)$ for some $r \in R$ since f is surjective. Per the definition of φ we have:

$$s = f(r) = \varphi(r+K).$$

This means that φ is surjective.

(2) To show that φ is injective we must show that if we assume that $\varphi(r+K) = \varphi(c+K)$ then $r+K = c+K$. This is since injective means that there cannot be more than one distinct element for which φ has the same value. We have:

$$\varphi(r+K) = \varphi(c+K).$$

The definition of φ implies that:

$$f(r) = f(c) \implies$$
$$f(r) - f(c) = 0.$$

Since f is a homomorphism and just as when we showed that φ is well defined we have that:

$$f(r-c) = 0 \implies$$
$$r - c \in K \implies$$
$$r \equiv c \mod K.$$

Then theorem 4.12 gives us $r \equiv c \mod K \iff r+K = c+K$. Which means that:

$$\varphi(r+K) = \varphi(c+K) \implies r+K = c+K$$

and φ is injective.

(3) The fact that f is a homomorphism let's us easily show that φ is. With $c, d \in R$ for multiplication we have:

$$\begin{aligned}\varphi((c+K)(d+K)) &= \varphi(cd+K)\\ &= f(cd)\\ &= f(c)f(d)\\ &= \varphi(c+K)\varphi(d+K)\end{aligned}$$

For addition we have:

$$\begin{aligned}\varphi((c+K)+(d+K)) &= \varphi((c+d)+K)\\ &= f(c+d)\\ &= f(c)+f(d)\\ &= \varphi(c+K)+\varphi(d+K)\end{aligned}$$

Thereby φ is a homomorphism and the proof is complete.

□

5. Factorization Methods

5.1. **Pollard's $p-1$ Factorization Algorithm.** One algorithm for factoring some large numbers is the *Pollard's $p-1$ method*. It does not work for all large numbers but it demonstrates that not all large numbers are suitable to use for the RSA cryptosystem. This method works when $p-1$ is a product of many small primes. Let $N = pq$ and let L have the property:

$$p-1 \text{ divides } L \text{ and}$$

$$q-1 \text{ does not divide } L.$$

Then we know that for some integers i, j,, $k \neq 0$ and $k < (q-1)$:

$$L = i(p-1)$$

and

$$L = j(q-1)+k.$$

If we now take the random integer a and study a^L with Fermat's little theorem (4.6) we see that:

$$\begin{aligned}a^L &= a^{i(p-1)} = (a^{p-1})^i \equiv 1^i \equiv 1 \mod p\\ a^L &= a^{j(q-1)+k} = a^k(a^{q-1})^j \equiv a^k \cdot 1^j \equiv a^k \mod q.\end{aligned}$$

This means that p divides a^L-1, it is also very unlikely that for some $k \neq 0$ that $a^k \equiv 1 \mod q$. This means that it is very unlikely that q divides a^L-1. Therefore we can get p by calculating the greatest common denominator:

$$p = \gcd(a^L-1, N).$$

We can find a number L with the stated properties by using Pollard's observation that if $p-1$ is a product of small primes it will divide $n!$ for some n that is not so large that we won't be able to reasonably calculate it. That is because as long as we choose n to be larger than $p-1$ it will include at least the same primes and prime powers as $p-1$. This means that if we choose a random integer a and calculate:

$$\text{gdc}(a^{n!}-1, N)$$

we will have found our p if the greatest common denominator equals something other than 1 or N. In practice, the number $a^{j!}-1$ would quickly become extremely large. But since we are interested in $\gcd(a^{j!}-1, N)$ we can work with $a^{j!}-1 \mod N$ instead as the gcd will be the same. To summarize, do the following steps in Pollard's $p-1$ factorization algorithm:

(1) Set a to some value that makes it easy to do the rest of the calculations. In practice, $a = 2$ is often used.
(2) Calculate $d = \gcd(a^{j!}-1, N)$, where j is an integer which is greater or equal to 2. In practice, $d = \gcd(a^{j!}-1 \mod N, N)$ is calculated instead.
(3) If d is greater than 1 and less than N, a factor of N is found and the process can be stopped.
(4) Go trough $j = 2, 3, 4, ...$ to some upper bound so that you either find a factor to N or run out of time you want to spend to try and find a factor.

Example 5.1. For this example, we will factor the number $97 \cdot 101 = 9797$. We will use $a = 2$ for the calculations.

$$2^{2!}-1 \equiv 3 \mod 9797, \quad \gcd(3, 9797) = 1$$

$$2^{3!}-1 \equiv 63 \mod 9797, \quad \gcd(63, 9797) = 1$$

$$2^{4!}-1 \equiv 4751 \mod 9797, \quad \gcd(4751, 9797) = 1$$

$$2^{5!}-1 \equiv 7467 \mod 9797, \quad \gcd(7467, 9797) = 1$$

$$2^{6!}-1 \equiv 2619 \mod 9797, \quad \gcd(2619, 9797) = 97$$

Success! Since $\gcd(2619, 9797) = 97$ satisfy $1 < 97 < 9797$ we have found a factor of 9797.

5.2. **Factorization via Difference of Squares.** Factorization via the difference of squares relies on the basic identity:

$$x^2 - y^2 = (x+y)(x-y)$$

We can use this identity for factoring a number N by finding an integer b such that:

$$N + b^2 = a^2$$

therefore

$$N = a^2 - b^2 = (a+b)(a-b).$$

In practice, it is hard to find a b so that $N + b^2$ is a square. One technique that can help us is by looking at multiples kN instead of N. This is because if:

$$kN = a^2 - b^2 = (a+b)(a-b),$$

then it is not unlikely that N has a factor in common with both $(a+b)$ and $(a-b)$. We now only need to calculate the greatest common divisor of N and each of $(a+b)$ and $(a-b)$ to find those factors. We know that for integers A, B, C the statement:

$$A \equiv B \mod C$$

is equivalent to the statement that for some K

$$A = B + K \cdot C.$$

Therefore searching for numbers that satisfy:

$$a^2 \equiv b^2 \mod N$$

is an equivalent problem formulation as the previous one. However, we do not care about the case when

$$b \equiv -a \mod N$$

since that would imply that

$$b + a \equiv 0 \mod N$$

which implies that

$$\gcd(N, b + a) = N$$

which in turn makes it quite likely that

$$\gcd(N, b - a) = 1.$$

To utilize this method for factoring large numbers in practice we have to employ some smart methods for finding numbers that satisfy

$$a^2 \equiv b^2 \mod N,$$

because testing numbers randomly will be very slow. A common three-step method for finding these numbers is:

(1) Find integers $a_1, ..., a_r$ where $a_i > \sqrt{N}$ with the property that $c_i \equiv a_i^2 \mod N$ factors with small primes. The reason why we want c_i to factor into a product of small primes is so that we easily can find c_i factorization quite quickly instead of having to use one of the algorithms in this thesis if c_i is somewhat large.
(2) Multiply some of the c_i numbers found in the first step so that every prime appears to an even power. Then we will have a square $c_{i_1}...c_{i_s} = b^2$.
(3) Then let $a = a_{i_1}...a_{i_s}$ and compute the greatest common divisor $d = \gcd(N, a - b)$.

Because of the fact that:

$$\begin{aligned} a^2 &= (a_{i_1}...a_{i_s})^2 \\ &\equiv a_{i_1}^2...a_{i_s}^2 \\ &\equiv c_{i_1}...c_{i_s} \\ &\equiv b^2 \mod N, \end{aligned}$$

there is a good chance that d is a factor of N with $1 < d < N$.

We can elaborate more as to why there is a good chance that d is a proper factor of N. Suppose we have the numbers a, b such that:

$$(a - b)(a + b) = kN = kpq.$$

To make the argument easier to follow we also assume that $\gcd(k, N) = 1$. In this expression we can see that there are four different possibilities:

(1) p divides $a - b$ and q divides $a + b$
(2) p divides $a - b$ and q divides $a - b$
(3) p divides $a + b$ and q divides $a + b$
(4) p divides $a + b$ and q divides $a - b$

Based on this let us assume probability of each possibility is equal and independent of each other. In that case there is a $\frac{1}{2}$ probability that p and q divide a different factor of $(a - b)(a + b)$. This correspond to possibility 1 and 4 above. This means that if we have pairs $(a_1, b_1), ..., (a_n, b_n)$. Then the probability that p and q belong to different factors $(a_i - b_i)(a_i + b_i)$ for at least one of the pairs (a_i, b_i) is $1 - \frac{1}{2^n}$ which will quickly approaches 1 when n increases.

5.3. **Quadratic Sieve and Smooth Numbers.** To use factorization via the difference of squares we need a way to find numbers that factor into small primes, as described in step one of the three-step method in the previous section about the factorization via the difference of squares 5.2. We will begin by giving a formal definition of the numbers we want to find and then present what a sieve is and give a simple method that we will then modify to be able to find numbers we can use for the factorization via the difference of squares.

The numbers we are looking for that factor into primes smaller than some number B are called smooth numbers. Let us give the definition.

Definition 5.1 (Smooth Numbers [HPS16, p. 150])**.** An integer n is $B - smooth$ if all of its prime factors are less than or equal to B.

An efficient way of finding these numbers is Pomerance's *quadratic sieve*. Pomerance's quadratic sieve will help us find $B - smooth$ numbers that also fulfill the quality $c \equiv a^2 \mod N$. To explain the quadratic sieve we can start by looking at a sieve for finding primes and then one for finding $B - smooth$ numbers without worrying about the additional quality. One sieving method for finding *B-smooth* numbers is a modification of the *Sieve of Eratosthenes.*

The Sieve of Eratosthenes is a method of finding primes by successively going through a list of numbers and crossing out numbers that are divisible by the current one.

Example 5.2 (Sieve of Eratosthenes)**.** If we have a list of numbers of for example 2 to 20 then we start by looking at 2 and then cross out every number which have the number as a factor. Then we go to the next number that is not crossed out, which must be a prime, and repeat the process. After we have repeated this process enough times we will no longer find numbers to cross out or we have reached a prime that is larger than the root of the largest number. Then we know that the remaining uncrossed numbers are all prime. For this example, we get:

$$\begin{array}{cccccccccc} \boxed{2} & \boxed{3} & \cancel{4} & 5 & \cancel{6} & 7 & \cancel{8} & \cancel{9} & \cancel{10} & 11 \\ \cancel{12} & 13 & \cancel{14} & \cancel{15} & \cancel{16} & 17 & \cancel{18} & 19 & \cancel{20} & \end{array}$$

We can now modify the sieve of Eratosthenes to suit our needs. The goal is to find enough numbers on the form $a^{\equiv}b^2$ where b^2 is a product of small primes so that we can use the factorization via the difference of squares. The *quadratic sieve* finds $B - smooth$ numbers that are congruent to some number $a^2 \mod N$. It is similar to the sieve of Eratosthenes we saw in example 5.2. But instead of crossing out the numbers we divide by the prime we currently use to sieve our list of numbers. Meaning for our example 6 would be divided by both 2 and 3. This means all the numbers that are divided down to 1 would be $B - smooth$, where B is the largest prime we used to sieve. However, with this strategy, we will miss the $B - smooth$ numbers that are divisible by powers of small primes. So the key difference with the quadratic sieve is instead of just sieving the numbers by primes we will also sieve with powers of primes. Meaning when we get to the number 4 in example 5.2 we would sieve all eligible numbers by 2 again since the prime factorization of 4 is 2^2. Another example is if we have the interval 2 to 16 we will have to divide 16 by 2 each time when we sieve with $2, 4, 8$ and 16 for a grand total of 4 times. With this, we have found that 16 is $2 - smooth$.

We do not want just $B - smooth$ numbers, we want to find numbers that are $B - smooth$ and are congruent to some number $a^2 \mod N$. To do this we use the polynomial:

$$F(T) = T^2 - N$$

We use this particular polynomial since it will let us find numbers that are squares modulo N, which is what we need. Then we let:

$$a = \left\lfloor \sqrt{N} \right\rfloor + 1$$

which is the smallest integer that is larger than the square root of N. Here the brackets denote rounding down to the integer less than the number within the brackets. After that, we create the sequence of numbers:

$$F(a), F(a+1), ..., F(b).$$

We decide b based on how many $B - smooth$ numbers that are congruent with a^2 mod N that we need. We need enough $B - smooth$ numbers to be able to factor N.

Definition 5.2 (factor base [HPS16, p. 157])**.** The set of primes and powers of primes less than B is called the *factor base*.

Let's say we have the prime p in our factor base, meaning it is the prime we currently want to sieve with. Then the problem we need to solve is which of the numbers in our sequence of numbers are divisible by p? A completely equivalent statement is, which numbers T between a and b have the property:

$$T^2 \equiv N \mod p.$$

This is an equivalent statement as $T^2 \equiv N \mod p$ because it means that there is some k such that $T^2 - N = kp$. $F(T) = T^2 - N$ is how we generated the numbers for our sequence so if there exists a k such that $T^2 - N = kp$ then that number in the sequence would be divisible by p. If there are no solutions to the congruence, then the prime p divides no numbers in our sequence of numbers and is not a candidate to sieve with. Otherwise, if p is greater than 2 then the congruence will have two solutions modulo p. As per proposition 4.10 We call the solutions, if they exists:

$$T_1 = \alpha_p$$
$$T_2 = \beta_p.$$
$$T_2 = p - \alpha_p$$

It then follows that all the numbers in our sequence on the form:

$$F(\alpha_p), F(\alpha_p + p), F(\alpha_p + 2p), ...$$

and

$$F(\beta_p), F(\beta_p + p), F(\beta_p + 2p), ...$$

are divisible by p. Thereby we can sieve all the numbers on that form by p from our original list.

Now that we have explained what we need to do we will explain how we go about doing this. We need to find for which $a \leq T \leq B$, $T^2 - N$ is $B - smooth$. As we mentioned above, we need to solve the congruence $T^2 \equiv N \mod p$ for each prime and power of primes in the factor base of B. When p is odd, the congruence has either 0 or 2 solutions 4.10. If there are two solutions then they are:

$$\alpha_p$$

and

$$p - \alpha_p$$

The values of T for which $T^2 - N$ are divisible by p is on the form:

$$T_1 = pn + \alpha_p$$
$$T_2 = pn + p - \alpha_p$$

for $n \in \mathbb{Z}$. For each $a \leq T \leq b$ on this form we can then divide $T^2 - N$ by p. The numbers that reach 1 after repeating this process for every p in our chosen factor base B are *B-smooth*. With this method, we are able to find enough to be able to use the factorization via the difference of squares method. We can do this process much more efficiently by sieving the numbers systematically, which we will now illustrate with an example:

Example 5.3. We will now show the quadratic sieve in action for the number $N = 9797$. We begin by calculating our a and get $a = 99$ since:

$$\begin{aligned} a &= \left\lfloor \sqrt{9797} \right\rfloor + 1 \\ &= 98 + 1 \\ &= 99. \end{aligned}$$

For this number, we will use the polynomial:

$$F(T) = T^2 - 9797$$

and calculate $F(99)$ to $F(114)$ to get a handful of numbers to have a good chance of finding enough *B-smooth* numbers on the form $a^2 \mod N$. As we saw in section 5.2 we do not have to find that many *B-smooth* numbers to have a good chance of factoring N. We get our list of numbers to be:

4	203	404	607	812	1019	1228	1439
1652	1867	2084	2303	2524	2747	2972	3199

We can now begin the sieving process from 2 to 29. One thing to note is that we will also sieve the numbers that are prime powers within this interval. Meaning we will sieve by 2 again when we arrive at 2^2. We start with $p = 2$. We check that:

$$t^2 \equiv 9797 \mod 2$$

have a solution, which it does. Every number on the form $2n + 1$ is a solution, meaning every odd number. Thereby we can divide every other number from our list by 2. This is because the first value of t that we used to create our list is 99, an odd number. We get:

2	203	202	607	406	1019	614	1439
826	1867	1042	2303	1262	2747	1486	3199

We now continue with 3. Since:

$$t^2 \equiv 9797 \equiv 2 \mod 3$$

does not have any solution no numbers in the list are divisible by 3. Now for 2^2 Since:

$$t^2 \equiv 9797 \equiv 1 \mod 4$$

has solutions we will sieve away 2 again from every other number in the list and get:

1	203	101	607	203	1019	307	1439
413	1867	521	2303	631	2747	743	3199

We now repeat the process for $p = 5$. The congruence:

$$t^2 \equiv 9797 \equiv 2 \mod 5$$

has no solutions. We will now test if we can sieve with 7. We see that:

$$t^2 \equiv 9797 \equiv 4 \mod 7$$

has two solutions:

$$t = 7n + 2$$

and

$$t = 7n + 5.$$

This means we can sieve $F(100)$ since $t = 7 \cdot 14 + 2 = 100$ and every seventh number. We can of course also sieve $F(103)$ by the same argument for the second solution to the congruence. We then get:

1	29	101	607	29	1019	307	1439
59	1867	521	329	631	2747	743	457

We can now repeat the process for $p = 11, 13, 17, 19, 23, 29$. For those primes only $p = 29$ have the solutions:

$$t = 29n + 13$$

and

$$t = 29n + 16.$$

That means we can sieve $F(100)$ and $F(103)$ again and get:

1	1	101	607	1	1019	307	1439
59	1867	521	329	631	2747	743	457

We can now see which numbers has been sieved to 1. The input values of t squared for those numbers are therefore products of small primes in modulo $N = 9797$. We have:

$$\begin{aligned} 99^2 &\equiv 2^2 && \mod 9797 \\ 100^2 &\equiv 7 \cdot 29 && \mod 9797 \\ 103^2 &\equiv 2^2 \cdot 7 \cdot 29 && \mod 9797. \end{aligned}$$

We can now combine these congruences so that we get a congruence $a^2 \equiv b^2 \mod N$ which we need for the actual factorization. We can for example use:

$$(100 \cdot 103)^2 \equiv (2 \cdot 7 \cdot 29)^2 \mod 9797$$

so that we can then calculate:

$$\gcd(N, a - b)$$

to have a high chance for a factor of N. We get:

$$\gcd(9797, 100 \cdot 103 - 2 \cdot 5 \cdot 7) = \gcd(9797, 9894) = 97.$$

Since $N = 9797 = 97 \cdot 101$ we have successfully factored N using the quadratic sieve.

5.4. **The Number Field Sieve.** We have now covered the necessary theory on rings and quotient rings to be able to explain the number field sieve. However, the complete method is very complicated so we will only explain the key aspects regarding how we can use rings to find some very useful homomorphisms. These homomorphisms enables us to find pairs of numbers $a^2 \equiv b^2 \mod N$ that we can use to have a good chance of factoring N. The rings we will be using primarily are. $\mathbb{Z}[x]/(f(x))$ and $Z[\beta]$, where β is a complex root of $f(x)$

To find numbers for factoring N with the number field sieve we first choose an integer m with $m \neq 0$. We also need to choose an irreducible monic polynomial $f(x)$, in the polynomial ring. That means that the polynomial satisfies the properties of irreducibility in definition 4.5. Another way of thinking about this is to find a prime function in the ring. A monic polynomial is a polynomial where the coefficient of the term with the highest degree is 1. The polynomial should also have the property:

$$f(m) \equiv 0 \mod N.$$

Let β be a complex root of $f(x)$ and let d be the degree of $f(x)$. According to Lenstra et al. [LL, p. 11], the method works best for N that are on the form $N = r^e - s$ where r and s are small and e is large.

Now let $\mathbb{Z}[x]$ be the ring of polynomials with integer coefficients. There exists a unital homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{C}$ that is determined by $\varphi(x) = \beta$. This means that it maps every polynomial to a combination of powers of β. The reason why there is a homomorphism between these rings is because we can very easily construct a unital homomorphism from a polynomial ring to another ring by mapping all integers to the same integer and then choose to map the element x in $\mathbb{Z}[x]$ to a specific element in the other ring.

Since $f(\beta) = 0$ it follows that $f(x)$ is in the kernel of φ, and therefore the ideal $(f(x))$ is contained in the kernel of φ. Furthermore, since $f(x)$ is irreducible, it is the minimal polynomial of β. It follows that every polynomial $g(x)$ in the kernel of φ is a multiple of f. Therefore $(f(x)) = \ker(\varphi)$. Let ψ be the natural homomorphism 4.15 between $\mathbb{Z}[x]$ and $\mathbb{Z}[x]/(f(x))$ given by $\psi(x) = x + (f(x))$. From this it follows that φ factors through ψ and an injective ring homomorphism:

$$\pi : \mathbb{Z}[x]/(f(x)) \to \mathbb{C}$$

that satisfies $\pi(x+(f(x))) = \beta$. Let $\mathbb{Z}[\beta]$ be the image of φ and π. Now thanks to the first isomorphism theorem 4.16 we know that π defines an isomorphism between $\mathbb{Z}[x]/f(x)$ and $Z[\beta]$. Clearly, $Z[\beta]$ is the subring of $\mathbb{C}$ generated by $\mathbb{Z}$ and β.

Next, we have to find a large number of pairs of integers:

$$(a_1, b_1), ..., (a_k, b_k)$$

that have the property:

$$\prod_{i=1}^{k}(a_i - b_i m) = A^2$$

and

$$\prod_{i=1}^{k}(a_i - b_i \beta) = \alpha^2$$

where

$$A \in \mathbb{Z}$$

and

$$\alpha \in \mathbb{Z}[\beta].$$

For this sieve we look for numbers that are $B - smooth$ on the form $a - bm$ and also numbers that are $B - smooth$ in the quotient ring $\mathbb{Z}[\beta] = \mathbb{Z}[x]/(f(x))$. From our definition of $\mathbb{Z}[\beta]$ we can create an expression α on the form:

$$\alpha = c_0 + c_1\beta + c_2\beta^2 + ... + c_{d-1}\beta^{d-1} \tag{1}$$

with

$$c_0, c_1, ..., c_{d-1} \in \mathbb{Z}. \tag{2}$$

Since $f(m) \equiv 0 \mod N$ there is a homomorphism $\phi : \mathbb{Z}[x]/(f(x)) \to \mathbb{Z}/N$. Satisfying $\phi(x) = m$. Since $\mathbb{Z}[x]/(f(x))$ is isomorphic to $\mathbb{Z}[\beta]$ we are able to think of ϕ as a homomorphism from $\mathbb{Z}[\beta]$ to $\mathbb{Z}/N$ satisfying $\phi(\beta) = m$. The kernel of this homomorphism will be all the polynomials where β is a root.

This means that elements on the form:

$$\prod_{i=1}^{k}(a_i - b_i\beta)$$

will be mapped by ϕ to elements on the form:

$$\prod_{i=1}^{k}(a_i - b_i m)$$

The idea of the number field sieve is to find pairs of numbers (a_i, b_i) that are $B - smooth$ in $\mathbb{Z}[\beta]$ and $\mathbb{Z}$. In the quadratic sieve we aimed to find numbers on the form $a^2 \mod N$ that are $B - smooth$. This time we will look for numbers on the form $a_i - b_i\beta$ whose products are $B - smooth$ in $\mathbb{Z}[\beta]$ and then we will know that independently products of $a_i - b_i m$ will be $B - smooth$ in $\mathbb{Z}$. We will now demonstrate this relation.

Since a ring homomorphism preserves multiplication we know that if:

$$\prod_{i=1}^{k}(a_i - b_i\beta)$$

is a square in $\mathbb{Z}[\beta]$ then:

$$\prod_{i=1}^{k}(a_i - b_i m)$$

will be a square in Z/N.

Since we now know that the element β can be substituted by $m \mod n$ we can find an element $A^2 \equiv B^2$ by the following relation:

$$\begin{aligned} B^2 \equiv \phi(\alpha)^2 &= \phi(\alpha^2) \\ &= \phi(\prod_{i=1}^{k}(a_i - b_i\beta)) \end{aligned}$$

by the definition of our homomorphism ϕ we know that this will be congruent to a number on the following form:

$$\equiv \prod_{i=1}^{k}(a_i - b_i m) = A^2 \mod N.$$

With that, we have created a congruence $A^2 \equiv B^2 \mod N$. Like with our other factorization methods, there is a high probability that $\gcd(A - B, N)$ will be a factor of N. To find the pairs of numbers (a_i, b_i) that we need for our factorization we can use a similar method to the quadratic sieve. But instead of numbers on the form $a^2 \mod N$ that is $B - smooth$ we will look for numbers on the form $a_i - b_i\beta$ and $a_i - b_i m$ which products are $B - smooth$.

6. Discussion

6.1. **Comparison of Algorithms.** We have in this thesis presented four different ways to factor large integers. Three of the methods: the quadratic sieve, the rational sieve, and the number field sieve, can be used for factoring most numbers. They use the same algorithm for the last step of actually factoring the numbers. They use the factorization via difference of squares. The difference between them is how they find the relationships between pairs of numbers that are needed for factoring via the difference of squares. These four methods are good in different situations. We will now analyze and compare them with each other.

6.1.1. *Pollard's $p-1$ Factorization Algorithm.* We begin by itemizing Pollard's $p-1$ methods strengths and weaknesses.

Strengths: It is the simplest factorization method of the ones presented in this thesis. This is because factorization with the difference of squares method requires us to also build relations of number pairs. For example with the help of the quadratic sieve, we can find numbers on the form $c \equiv a^2 \mod N$ with c being a product of small primes. Likewise, with the number field sieve, we have to first find numbers on the form $a - bm$ that are B - *smooth* in addition to then also find numbers that are on the form $A^2 \equiv B^2 \mod N$. This method highlights the fact that we have to consider how $p-1$ and $q-1$ factors. It is not directly obvious that we would need to be careful how those numbers factor when we select $N = pq$ for the RSA cryptosystem. But thanks to this method we just have to check that $p-1$ $q-1$ does not factor into small primes. Because just as we saw in example 5.1, Pollard's $p-1$ factorization algorithm only gives us a meaningful result when $a^{j!} \mod N$ factors into a product of small primes. It also gives us a good reason to continue to study factorization methods since there might exist other non-obvious cases like this where a number that might seem completely secure to use for encryption might actually be really easy to factor.

Weaknesses: The most obvious limitation of Pollard's $p-1$ factorization algorithm is the fact that it only works for numbers $N = pq$ where it is true that one and only one of the numbers $p-1$ and $q-1$ is a product of small primes. This means that Pollard's algorithm is not very useful if we are tasked with the problem of factoring a random $N = pq$.

6.1.2. *Factorization via Difference of Squares.* Now we will list some of the strengths and weaknesses of the factorization via the difference of squares method of factoring large integers.

Strengths: This is the factorization method is the most powerful method that we currently know of for factoring large numbers. according to Hoffstein et al. [HPS16, p. 98]. Factorization via difference of squares is able to factor any number $N = pq$ as opposed to Pollard's $p-1$ factorization algorithm. This means that this method is versatile for the task of finding nontrivial factors.

Weaknesses: This method requires that you find a couple of number pairs $a^2 \equiv b^2 \mod N$ to actually be useful. The process of finding those numbers is not straightforward. The method requires the use of one of the sieving methods that were discussed in this thesis to be able to be used in practice.

6.1.3. *The Quadratic Sieve.* Now we will list some of the strengths and weaknesses of the quadratic sieve method of factoring large integers.

Strengths: The quadratic sieve, in combination with factorization via difference of squares, is the quickest way of factoring numbers up to about 2^{350} [HPS16, p. 156].

Weaknesses: The method takes many operations to sieve the numbers which means that it can be quite computationally intensive to run in practice.

6.1.4. *The Number Field Sieve.* Lastly, we will now list some of the strengths and weaknesses of the number field sieve method of factoring large integers.

Strengths: This is the fastest method for factoring integers for numbers that are a fair bit larger than 2^{350} like 2^{450} and above [HPS16, p. 156].

Weaknesses: The method is complicated and there are numerous challenges in implementing it in practice.

6.2. **Conclusions.** To summarize the strengths and weaknesses, the best factorization method of course depends on the specific characteristics of the integer and what computational resources we have available if we want to put the methods into practice. Pollard's $p-1$ factorization is great for certain numbers where $p-1$ is a product of many small primes. The Quadratic Sieve in combination with factorization via difference of squares is more versatile and quite easy to understand and would be straightforward to implement. For the largest integers then the Number Field Sieve stands out as the fastest method, although its implementation complexity and resource requirements would make it a lot harder to put into practice. Luckily for our ability to communicate secrets to each other with the RSA cryptosystem, no method still provides an easy way of quickly factoring large integers based on this summary of some of the most well known methods of factoring integers. In conclusion, we can still feel safe knowing that our RSA encrypted messages will remain only readable for their intended audience.

Acknowledgments

I can't thank Gregory Arone enough for his helpfulness and patience during the long process of completing this thesis.

References

[HPS16] J. Hoffstein, J. Pipher, and J.H. Silverman, *An introduction to mathematical cryptography*, Undergraduate Texts in Mathematics, Springer New York, 2016.

[Hun13] T. Hungerford, *Abstract algebra: An introduction*, third ed., Cengage Learning, 2013.

[Kyl17] Kyle Miller, *Quadratic residues and quadratic nonresidues*, https://math.berkeley.edu/~kmill/math55sp17/qnr.pdf, 2017, Accessed: 2021-12-28.

[LL] A.K. Lenstra and H.W.J. Lenstra, *The development of the number field sieve*, Lecture Notes in Mathematics.

[Wal01] D.A.R. Wallace, *Groups, rings and fields*, Springer Undergraduate Mathematics Series, Springer London, 2001.

Department of Mathematics, Stockholm University
Email address: rasmus@persson.io