The Work of Sophie Germain and Niels Henrik Abel on Fermat’s Last Theorem

Lene-Lise Daniloff
Master’s Thesis, Spring 2017
This master’s thesis is submitted under the master’s programme Mathematics, with programme option Mathematics, at the Department of Mathematics, University of Oslo. The scope of the thesis is 60 credits.

The front page depicts a section of the root system of the exceptional Lie group $E_8$, projected into the plane. Lie groups were invented by the Norwegian mathematician Sophus Lie (1842–1899) to express symmetries in differential equations and today they play a central role in various parts of mathematics.
Abstract

In this thesis, we study what can be said about Fermat’s Last Theorem using only elementary methods. We will study the work of Sophie Germain and Niels Henrik Abel, both who worked with Fermat’s Last Theorem in the early 1800s. Abel claimed to have proven four partial results of Fermat’s Last Theorem, but mentioned nothing about how he had proved them. The aim of this thesis is to rediscover these four proofs. We will show that using only elementary methods, we are able to prove parts of Abel’s theorems, but we have not found it possible to prove them in full generality. We will see that allowing ourselves to use some non-elementary methods one can prove more of Abel’s claims, but still not in full generality.
Acknowledgements

First of all I would like to thank my supervisor Arne B. Sletsjøe for suggesting the topic, and guiding me through the process of writing the thesis. Your enthusiasm is contagious and I have had a lot of fun!

I would also like to thank Yngve, who kindly offered to help me with proofreading. Stine and Hanne also did some damage control, correcting my grammar and non-mathematical typos.

I have a lot of great people in my life who has kept me motivated, and I am grateful for each and every one of you. A special thanks goes to Ellinor the dog, whom I can always count on when my stress level flies through the roof. And last, but not least, I want to thank my girlfriend Lina, who is always encouraging me to do my very best.
iv
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>i</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>iii</td>
</tr>
<tr>
<td><strong>1 Introduction</strong></td>
<td>1</td>
</tr>
<tr>
<td>1.1 Basic tools</td>
<td>2</td>
</tr>
<tr>
<td><strong>2 Sophie Germain</strong></td>
<td>7</td>
</tr>
<tr>
<td>2.1 Sophie Germain's Theorem</td>
<td>7</td>
</tr>
<tr>
<td>2.2 The grand plan to prove FLT</td>
<td>9</td>
</tr>
<tr>
<td>2.3 Large Size Solutions</td>
<td>16</td>
</tr>
<tr>
<td><strong>3 Niels Henrik Abel</strong></td>
<td>21</td>
</tr>
<tr>
<td>3.1 Theorem II</td>
<td>21</td>
</tr>
<tr>
<td>3.2 Theorem I</td>
<td>24</td>
</tr>
<tr>
<td>3.3 Theorem III</td>
<td>32</td>
</tr>
<tr>
<td>3.4 Theorem IV</td>
<td>33</td>
</tr>
<tr>
<td><strong>4 Other approaches to Abel's Theorem I</strong></td>
<td>35</td>
</tr>
<tr>
<td>4.1 Inkeri's approach</td>
<td>35</td>
</tr>
<tr>
<td>4.2 Ribenboim's Approach</td>
<td>42</td>
</tr>
<tr>
<td>4.3 Cyclotomic integers</td>
<td>44</td>
</tr>
<tr>
<td><strong>5 Historical note</strong></td>
<td>51</td>
</tr>
<tr>
<td>5.1 Niels Henrik Abel</td>
<td>51</td>
</tr>
<tr>
<td>5.2 Sophie Germain</td>
<td>52</td>
</tr>
<tr>
<td><strong>Bibliography</strong></td>
<td>55</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

Fermat’s Last Theorem is one of the most famous mathematical problem of all times, and it is widely known for several reasons. It is easily formulated, and the concepts involved are not abstract nor difficult. The problem is therefore easily accessible to anyone, no matter their background in mathematics. The story of the quest for a proof is also a fascinating one, including several failed attempts and a long line of frustrated mathematicians.

Pierre de Fermat (1601 - 1665) was a French lawyer who studied number theory on his spare time. He formulated the theorem bearing his name by simply making a note in the margin of a book. He claimed that "I have discovered a truly marvelous proof of this, which this margin is too narrow to contain". Fermat made several other number theoretic claims without writing out complete proofs, and mathematicians have over the years rediscovered the proofs to all of these - with only one exception:

**Theorem 1.0.1** (Fermat’s Last Theorem). *For any integers* $a, b, c$, *and any integer* $n > 2$, *there exists no solution to the equation*

$$a^n = b^n + c^n$$

(1.1)

The theorem goes by the name of Fermat’s Last Theorem (abbreviated to FLT), not because it was the last theorem Fermat proposed or worked with, but because it was the last of his theorems to be proven. Mathematicians have tried to solve this problem for hundreds of years, but it was not until 1995 that Andrew Wiles finally published a complete proof. Wiles used techniques far beyond what was available to Fermat, and it is therefore a common belief that Fermat thought he had a proof that was in fact false.

In this thesis, we focus on the work done on FLT by Sophie Germain and Niels Henrik Abel in the beginning of the 1800’s. Germain was trying to prove the theorem in full generality, but as we will see, her plan fails. However, she was still a pioneer in the work on FLT, taking the focus away from specific exponents, and turning it into more general cases.
Niels Henrik Abel was working on FLT during his stay in Copenhagen, the summer of 1823. In a letter to his former teacher in mathematics, Abel claims to have proven four partial results of Fermat’s Last Theorem. He does not however, write anything about the proofs. In this thesis we will try to rediscover Abel’s proofs of these four theorems. We will also see that the methods used by Abel and Germain in may cases are very similar.

Both Abel and Germain worked on Fermat’s Last Theorem in the early 1800s, a time where little was known about its validity. Fermat himself had proven the insolubility of the equation $a^n = b^n + c^n$ for the exponent $n = 4$. In 1770 Euler proved the statement for the exponent $n = 3$. These two special cases were the only ones known to Germain and Abel.

The structure of the thesis is as follows. In the rest of chapter 1 we introduce some basic and important concepts required in the rest of the thesis. In chapter 2 we analyze and discuss Germain’s work on Fermat’s Last Theorem. We prove the theorem named after her, investigate her plan to prove FLT in general and prove that her plan fails. In chapter 3 we will look into Abel’s four theorems, and give proofs where we have found it possible. In this section we use only elementary methods available for Abel at the time. In chapter 4 we will investigate the work done by Inkeri and Ribenboim on Abel’s first theorem. We will also explore whether expanding the investigation of Fermat’s Last Theorem into the ring of cyclotomic integers can give us new insight in Abel’s way of reasoning. For the interested reader, a short historical note is placed at the end of the thesis, in chapter 5.

1.1 Basic tools

Without any loss of generality, we are always allowed to make the following two assumptions when we work on Fermat’s Last Theorem. The first is that $n$ is a prime. This is because if $n = mp$ for some prime $p$, and if $a^n = b^n + c^n$ then we would also have that $(a^m)^p = (b^m)^p + (c^m)^p$. So if we can prove that FLT holds for all primes, then it will also hold in general. The second assumption is that $a, b, c$ are pairwise relatively prime. If $a$ and $b$ have a common factor, then because $a^n = b^n + c^n$, we see that $c$ must also have this common factor. Then we can simply just divide it out of the equation. We will make these two assumptions throughout the thesis. The equation $a^n = b^n + c^n$ will be referred to as Fermat’s equation.

Fermat originally stated the theorem for natural numbers, but it is easily observed that the theorem holds for natural numbers if and only if it hold for integers in general. Obviously, if Fermat’s equation holds for all integers, it also holds for natural numbers. Conversely, if we have a solution set which contain one or more negative integer, then we can always rewrite the equation so it becomes an equality of positive numbers. This is because we can always
1.1. BASIC TOOLS

assume that $n$ is prime. Since $n > 2$, we will always have that $n$ is odd. Hence $(-a)^n = -a^n$.

It is also a common practice to divide Fermat’s Last Theorem into two separate cases. We do this by looking at divisibility by $n$. Since $a, b, c$ are pairwise relatively prime integers, then either none or one of them is divisible by $n$. So we split the theorem into the two following cases:

Case I None of $a, b$ and $c$ are divisible by $n$

Case II One of $a, b$ or $c$ is divisible by $n$

Whenever we are referring to case I or case II without further specification, we are referring to these two cases.

Fermat’s and Euler’s Theorems

We will frequently make use of Fermat’s Little Theorem which is stated below.

**Theorem 1.1.1.** Let $a$ be an integer and $p$ a prime coprime to $a$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Euler defined a function $\phi : \mathbb{Z}_+ \rightarrow \mathbb{Z}_+$ that is commonly called Euler’s $\phi$-function. It is defined such that $\phi(n)$ gives the number of positive integers smaller than $n$ that is coprime with $n$. With this definition he showed a generalization of Fermat’s Little Theorem:

**Theorem 1.1.2.** Let $a$ be an integer relatively prime to the integer $n$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

The proof of these two theorems are omitted, but can be found in every book about basic algebra. Theorem 1.1.1 is considered so elementary that we will use it without making a reference to the exact theorem. Note that for a prime $p$ we have $\phi(p) = p - 1$.

**Primitive root modulo $n$**

We will use the notion of a primitive root frequently in Chapter 2. In this section we give the definition and some important properties. Following notation from above $\phi$ will denote Euler’s $\phi$-function.

**Definition 1.1.1.** Let $n$ and $g$ be relatively prime integers. Then $g$ is a primitive root modulo $n$ if $k = \phi(n)$ is the smallest number such that $g^k \equiv 1 \pmod{n}$.

The following proposition gives the important properties of primitive roots that we will make use of in this thesis.
Proposition 1.1.1.

1. For any prime $p$ there exists exactly $\phi(p - 1)$ primitive roots modulo $p$.

2. Let $n$ be an integer and $g$ a primitive root modulo $n$. Then for all numbers $m$ coprime to $n$ there exists a number $k$ such that $m \equiv g^k \pmod{n}$.

3. Let $p$ be a prime, and let $g$ be a primitive root modulo $p$. Then every nonzero residue modulo $p$ appear exactly once in the list $g, g^2, ..., g^{p-1}$.

4. There exists a primitive root modulo $n$ if and only if $n = 2, n = 4, n = p^k$ or $n = 2p^k$ for some prime $p > 2$ and a natural number $k > 0$.

Proof. See for example chapter 8 in [Bur06]. ■

Note that for any prime $p$, a primitive root $g$ modulo $p$ will have the property that $g^{p-1} = 1$.

**nth power residues modulo $p$**

Another important concept is the $n$th power residue modulo $m$, where $n$ and $m$ are a natural numbers. Here we give the definition and a few examples of the concept.

**Definition 1.1.2.** Let $a, n, m$ be nonzero integers. We say that $a$ is an **$n$th power residue modulo** $m$ if there is a solution to the equation $x^n \equiv a \pmod{m}$.

**Example 1.** Look at the case $n = 3$ and $m = 5$. Then the following table shows that the 3rd power residues modulo 5 are 1, 2, 3 and 4.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$x^3 \pmod{5}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>27</td>
</tr>
<tr>
<td>4</td>
<td>64</td>
</tr>
</tbody>
</table>

**Example 2.** Set $n = 3$ and $m = 7$. The following table shows that the 3rd power residues modulo 7 are 1 and 6.

<table>
<thead>
<tr>
<th>$x$</th>
<th>$x^3 \pmod{7}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>27</td>
</tr>
<tr>
<td>4</td>
<td>64</td>
</tr>
<tr>
<td>5</td>
<td>125</td>
</tr>
<tr>
<td>6</td>
<td>216</td>
</tr>
</tbody>
</table>
We will see in later chapters, that there is a crucial distinction between these two examples. The key observation is that in the first example, the 3rd power residues are consecutive modulo 5, but in the second example, when considering residues modulo 7, they are not consecutive. This fact gives a different relationship between the primes 3 and 7, than between 3 and 5. The primes \( p \) with no consecutive \( n \)th power residues modulo \( p \), will be of particular interest when we study the work of Sophie Germain.
Chapter 2

Sophie Germain

In this chapter we will look at Sophie Germain’s main work in number theory. We start by stating and proving the theorem that is named after her. We proceed by looking at her plan to prove Fermat’s Last Theorem in general, and prove that it was doomed to fail. We will also look at her attempts to find a lower limit to hypothetical solutions of Fermat’s equation. Even though Germain’s work often suffered from mistakes, she was undoubtedly a talented mathematician who made great progress with the work on proving Fermat’s Last Theorem. Because of her gender she could not access the same education as her male peers, and she therefore worked mostly in solitude, without the opportunity to discuss her ideas with others. I have included several proofs because I believe they paint a good picture not just of Germain’s way of thinking and of her talent, but also show the magnitude of her mathematical ambitions.

Before we begin we set some notation that we will use throughout this thesis. Let $u, v$ be integers and let $n$ be a natural number. We will denote $\phi(u, v) = \frac{u^n - v^n}{u - v}$. Obviously $u^n - v^n = (u - v)\phi(u, v)$, which gives a factorization we will use many times throughout the thesis. We also observe that $\phi(u, v)$ is an integer:

$$\phi(u, v) = \frac{(u - v)(u^{n-1} + u^{n-2}v + ... + uv^{n-1} + v^{n-1})}{u - v} = u^{n-1} + u^{n-2}v + ... + uv^{n-1} + v^{n-1}$$

2.1 Sophie Germain’s Theorem

In this section we will give the proof of the theorem which is named after Sophie Germain, following the work of [Edw96]. The theorem can be formulated in different ways, but the most common is to use the notion of Case I of Fermat’s Last Theorem. That is, the case where $n$ does not divide $xyz$, as described in the previous chapter. With this in mind, we are ready to state Sophie Germain’s Theorem.
CHAPTER 2. SOPHIE GERMAIN

Theorem 2.1.1 (Sophie Germain’s Theorem). Let \( n \) be an odd prime. If there is another prime \( p \) such that:

(1) \( x^n + y^n + z^n \equiv 0 \mod p \) implies that \( x \equiv 0 \) or \( y \equiv 0 \) or \( z \equiv 0 \mod p \),
(2) \( x^n \equiv n \mod p \) is impossible for any value of \( x \),
then case I of Fermat’s Last Theorem is true for \( n \).

Proof. We divide the proof into several steps to make it easier to see the overall structure.

Preliminaries: We assume that none of \( x, y, z \) are divisible by \( n \) and that they also are pairwise relatively prime. Moving \( z^n \) to the left side of Fermat’s equation, the assumption is that \( x^n + y^n + z^n \equiv 0 \mod n \) has some non-zero integer solution under the conditions of the theorem. We want to show that this leads to a contradiction.

Finding \( n \)th powers: We start by rewriting the equation like this: \( -x^n = y^n + z^n = (y+z)(y^{n-1} - y^{n-2}z + \ldots - yz^{n-2} + z^{n-1}) = (y+z)\phi(y, -z) \). Assume that \( q \) is a prime number dividing both factors on the right hand side. Then \( y \equiv -z \mod q \) and \( \phi(y, -z) \equiv 0 \mod q \), which implies that \( n y^{n-1} \equiv 0 \mod q \). So either we have \( q | n \) or \( q | y^{n-1} \). If \( q | n \) then \( q = n \) since they are both primes. This is impossible because we have assumed that \( n \nmid xyz \). But as \( x \) and \( y \) are assumed to be relatively prime it is also impossible that \( n | y \). Hence \( y + z \) and \( \phi(y, -z) \) are relatively prime numbers, and consequently they are both \( n \)th powers.

Existence of numbers: A similar argument as above can also be used in the cases of \( -y^n = (x+z)\phi(x, -z) \) and \( -z^n = (x+y)\phi(x, -y) \). Hence there exist numbers \( a, b, c, \alpha, \beta, \gamma \) such that:

\[
\begin{align*}
y + z &= a^n \\
x + y &= b^n \\
x + z &= c^n
\end{align*}
\]
\[
\begin{align*}
\phi(y, -z) &= \alpha^n \\
\phi(x, -y) &= \beta^n \\
\phi(x, -z) &= \gamma^n
\end{align*}
\]

Also observe that

\[
\begin{align*}
-x &= a\alpha \\
-y &= b\beta \\
z &= c\gamma
\end{align*}
\]
2.2. THE GRAND PLAN TO PROVE FLT

**Arithmetic modulo** $p$: From the equations above one can deduce that $2x = b^n + c^n - a^n$. From condition (1) we may assume, without loss of generality, that $x \equiv 0 \pmod{p}$. Hence $b^n + c^n + (-a)^n \equiv 0 \pmod{p}$. Using condition (1) again we see that either $a$, $b$, or $c$ must be divisible by $p$. If $b$ or $c$ is divisible by $p$, then we get a contradiction to the fact that $x$, $y$, or respectively that $x$, $z$ are relatively prime. So assume $a \equiv 0 \pmod{p}$.

Then, since $y + z = a^n$, we have that:

\[
y \equiv -z \pmod{p}
\]
\[
\alpha^n = \phi(y, -z) \equiv ny^{n-1} \pmod{p}
\]
\[
\beta^n = \phi(x, -y) \equiv y^{n-1} \pmod{p}
\]
\[
\Rightarrow \alpha^n \equiv n\beta^n \pmod{p}
\]

Since $\beta \not\equiv 0 \pmod{p}$ there exists a number $g$ such that $g\beta \equiv 1 \pmod{p}$. Now we multiply eq. (2.4) by $g^n$ to get $\alpha^n g^n \equiv n \pmod{p}$. This is a contradiction to assumption (2) in the theorem, hence we are done.

Sophie Germain’s Theorem gives us an explicit method for proving case I for specific exponents. Germain herself proved case I for all primes $n < 100$ by finding other primes $p$ satisfying the two conditions of her theorem.

In example 3 below we include a table showing the 5th power residues modulo 11. From this we can easily see that if $n = 5$, then $p = 11$ is a prime number satisfying the condition (2) of Sophie Germain’s Theorem. We may also see from the same table that 11 satisfy condition (1). This is because all 5th powers are 1, 0 or $-1$ modulo 11, and $\pm 1 \pm 1 \pm 1 \equiv 0$ is impossible. Then, by Sophie Germain’s Theorem, case I of Fermat’s Last Theorem holds for the exponent $n = 5$.

Sophie Germain’s Theorem does not say anything about case II. Even though her theorem was a great improvement in the quest of a more general proof of FLT, it was clear that it was still a long way to go.

2.2. The grand plan to prove FLT

In my work on this section I have looked at results and proofs from [LP08, section 3]. I have included several proofs because they give an interesting insight in Germain’s thinking. They are also explanatory and will hopefully give the reader a better intuition of the concepts involved. I have written out more details in some cases, and also tried to make the structure of the main proofs clearer. Results from other sources than the one mentioned above are specified in the text.
Non-consecutivity

In her manuscripts, Germain often consider whether or not a prime satisfy what we will call the non-consecutive condition, or NC-condition for short. We begin by defining it:

**Definition 2.2.1** (Non-consecutivity condition). Let $n$ and $p$ be prime numbers. If there does not exist two non-zero, consecutive $n$th power residues modulo $p$, then we say that $p$ satisfy the non-consecutivity condition relative to $n$. If $p$ is such a prime, we say that it is an auxiliary prime to $n$.

Sometimes we will call a prime $p$ an auxiliary prime, but then it should always be clear from the context to which prime $n$ it is relative to. The definition of the NC-condition may seem a bit strange and unmotivated, but it turns out to be both useful and important, and we will use non-consecutivity in several proofs. Observe that the non-consecutivity of a prime $p$ is always relative to another prime $n$. We will consider two examples, one of a prime not satisfying the NC-condition, and one example of a prime that does.

**Example 3.** Let $n = 5$ and $p = 11$. To see if 11 satisfy the NC-condition relative to 5, we need to consider the $5$th power residues modulo 11:

<table>
<thead>
<tr>
<th>$x$</th>
<th>$x^5$</th>
<th>$(\text{mod } 11)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>32</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>243</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1024</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>3125</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>7776</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>16807</td>
<td>10</td>
</tr>
<tr>
<td>8</td>
<td>32768</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>59049</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>100000</td>
<td>10</td>
</tr>
</tbody>
</table>

We see that the only $5$th power residues modulo 11 are 1 and 10, and these two integers are not consecutive. Hence 11 satisfy the NC-condition relative to 5.

**Example 4.** As in the previous example, we again consider the prime $n = 5$, but now we let $p = 7$. The $5$th power residues modulo 7 are:
2.2. THE GRAND PLAN TO PROVE FLT

Here the 5th power residues modulo 7 are 1, 2, 3, 4, 5, 6. These integers are consecutive, hence 7 does not satisfy the NC-condition relative to 5.

The non-consecutive condition turns out to be equivalent to the first condition we put on the prime \( p \) in Sophie Germain’s Theorem. So even though the definition of the NC-condition may seem strange, its importance will be clear after proving this equivalence. We will also discuss how this leads to Germain’s plan to prove Fermat’s Last Theorem in general. The following result and proof are from [Rib08, p.110], and in our notation it is stated as follows:

**Proposition 2.2.1.** Let \( n \) be an odd prime, and \( p \) a prime. Then the following are equivalent:

i) If for some integers \( x, y \) and \( z \) we have that \( x^n + y^n + z^n \equiv 0 \pmod{p} \), then either \( x \equiv 0 \pmod{p} \), \( y \equiv 0 \pmod{p} \) or \( z \equiv 0 \pmod{p} \).

ii) \( p \) is an auxiliary prime to \( n \).

**Proof.** We show each implication separately:

i) \( \Rightarrow \) ii) We assume for a contradiction that \( p \) does not satisfy the NC-condition relative to \( n \). That is, assume there exists two non-zero integers \( a \) and \( b \) such that \( a^n \equiv b^n + 1 \pmod{p} \), where \( 1 \leq a, b \leq p - 1 \). This implies that \( a^n - b^n - 1^n \equiv 0 \pmod{p} \) which by assumption implies that either \( a \) or \( b \) is divisible by \( p \). This is impossible since \( a, b < p \).

ii) \( \Rightarrow \) i) We assume that \( p \) satisfy the NC-condition relative to \( n \) and that \( x^n + y^n + z^n \equiv 0 \pmod{p} \). Also, assume for a contradiction that neither \( x, y \) nor \( z \) is divisible by \( p \). Then there exist integers \( a, b \) such that \( ax \equiv y \pmod{p} \) and \( bx \equiv z \pmod{p} \). Observe that \( p \) does not divide any of the integers \( a \) and \( b \), because if it did it would contradict the assumption that \( y, z \) are not divisible by \( p \). Hence we get

\[
x^n + (ax)^n + (bx)^n \equiv 0 \pmod{p}
\]

\[
\Rightarrow 1 + a^n + b^n \equiv 0 \pmod{p}
\]

which contradicts the fact that \( p \) satisfy the NC-condition relative to \( n \). \( \blacksquare \)
As mentioned above, the motivation for Germain’s idea to prove Fermat’s Last Theorem lies in the previous proposition. This is because it tells us that for any nontrivial solution \( x^n + y^n + z^n = 0 \), all auxiliary primes to \( n \) will divide either \( x, y \) or \( z \). Therefore, if Germain could prove that there existed infinitely many auxiliary primes for any exponent \( n \), then one of \( x, y, z \) had to be divisible by an infinitely number of primes. This would be a contradiction, proving Fermat’s Last Theorem. However, her plan fails, as we will see in theorem 2.2.3. First we will prove another interesting fact about primes satisfying the NC-condition. This proof is from [Rib08], but is adapted to our notation and I have included more details.

**Proposition 2.2.2.** Let \( n \) be a prime and \( p \) an auxiliary prime to \( n \). Then \( p = 2Nn + 1 \) for some positive integer \( N \).

**Proof.** We will make use of the following claim:

*Claim.* Let \( p \) and \( n \) be prime numbers, and assume \( p \) is odd. If \( n \) and \( p - 1 \) are relatively prime, then \( p \) does not satisfy the NC-condition.

Now assume \( p \) is a prime satisfying the NC-condition. Note that if \( p = 2 \) then the only nonzero residue modulo \( p \) is 1. Hence a prime satisfying the NC-condition, must always be odd. Now the claim implies that \( n \) and \( p - 1 \) have some common factor \( m \). That is: \( n = Km \) and \( p - 1 = Mm \) for some integers \( K, M \). Keeping in mind that \( p \) is odd, combining these facts give \( p - 1 = \frac{M}{K}n = 2Nn \) where \( 2N = \frac{M}{K} \). Hence \( p = 2Nn + 1 \).

To finish the proof we need to prove the claim above. So let \( n \) and \( p \) be primes such that \( p - 1 \) and \( n \) are relatively prime. Then there exists integers \( a, b \) such that \( a(p - 1) + bn = 1 \). Choose integers \( u, v, w \) not divisible by \( p \) such that \( u + v + w \equiv 0 \) (mod \( p \)). Then, by Fermat’s Little Theorem, we get

\[
\begin{align*}
u^{bn} &\equiv u(u^{p-1})^{-a} \equiv u \pmod{p} \\
\end{align*}
\]

Similarly we get \( v^{bn} \equiv v \pmod{p} \) and \( w^{bn} \equiv w \pmod{p} \). Hence

\[
\begin{align*}(u^b)^n + (v^b)^n + (w^b)^n &\equiv 0 \pmod{p} \\
\end{align*}
\]

and by proposition 2.2.1 we get that \( p \) does not satisfy the NC-condition (because \( p \) does not divide \(uvw \)).

**Failure of Germain’s plan**

In this section we will make use of the notions of primitive roots modulo a prime and \( n \)th power residues modulo a prime. Both are defined and explained in section [1.1].

Before we embark on the task of proving the failure of Germain’s plan to prove FLT, we will need the following two lemmas. These are taken from [Alk], but as this is not a published article I have included the proofs.
2.2. THE GRAND PLAN TO PROVE FLT

Lemma 2.2.1. Let \( p = 2Nn + 1 \) be a prime, where \( n \) is also a prime and \( N \) is a natural number. Then there are \( 2N \) different non-zero \( n \)-th power residues modulo \( p \).

Proof. The first step is to show that there is a solution of \( x^n \equiv b \pmod{p} \) if and only if \( b^{2N} \equiv 1 \pmod{p} \), where \( 0 < b < p \). So assume we have a solution to \( x^n \equiv b \pmod{p} \). Then, by Fermat’s Little Theorem, we have that \( b^{2N} \equiv (x^n)^{2N} \equiv x^{p-1} \equiv 1 \pmod{p} \).

Conversely, assume that we have \( b^{2N} \equiv 1 \pmod{p} \). If \( b = 1 \), then \( x = 1 \) is a solution of the equation \( x^n \equiv b \pmod{p} \). So suppose \( b \neq 1 \). Since \( p \) is prime there is a primitive root modulo \( p \) which we will denote by \( g \). That is, \( g^{p-1} \equiv 1 \pmod{p} \) and \( p - 1 \) is the smallest number with this property. By assumption we now have that \( 1 \equiv b^{2N} \equiv g^{p-1} = g^{2Nn} = (g^n)^{2N} \pmod{p} \), which implies that \( b \equiv g^n \pmod{p} \).

From this argument we see that in order to prove the lemma, it is sufficient to prove there are \( 2N \) different values of \( b \) such that \( b^{2N} \equiv 1 \pmod{p} \). Since \( g \) is a primitive root modulo \( p \) we have by proposition 1.1.1 that all of \( g^n, g^{2n}, ..., g^{2Nn} \) are different solutions to the desired equation. ■

Lemma 2.2.2. Let \( k \) be an \( n \)-th power residue modulo \( p \), where \( p = 2Nn + 1 \) is a prime.

i) If \( n \) is odd, then \( p - k \) is also an \( n \)-th power residue modulo \( p \).

ii) If \( n \) is even, then \( (p - k)^n \equiv k^n \pmod{p} \).

Proof. Assume \( n \) is odd. By assumption, we know that \( k \equiv x^n \pmod{p} \) has a solution. Hence we have \( p - k \equiv -k \equiv -x^n = (-x)^n \pmod{p} \) and we can conclude that \( p - k \) is an \( n \)-th power residue.

Now assume \( n \) is even. Then

\[
(p - k)^n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} p^{n-i} k^i \equiv k^n \pmod{p}
\]

The following theorem tells us that Germain’s plan of proving Fermat’s Last Theorem does not work, at least for the case \( n = 3 \). This proof is due to Germain herself. She writes out the proof in a letter to Legendre, where she also thanks him for "telling her yesterday" that her plan will fail for \( n = 3 \). As we will see, it is quite impressive work for only one night.

Theorem 2.2.3. Let \( N \) be a positive integer. For any prime \( p > 13 \) of the form \( p = 6N + 1 \), there are non-zero consecutive cubic residues.

Proof. Again we split up the proof in several paragraphs to make it easier to see the structure.
Preliminaries and assumptions: We consider the non-zero residues 1, 2, \ldots, 6N and make two assumptions:

1. Assume that there are no consecutive pairs of cubic residues amongst these residues.
2. Also assume that there are no pair of cubic residues whose difference is 2.

Gaps of non-cubic residues: Clearly 1 is a cubic residue, and by lemma 2.2.2 we know that \( p - 1 = 6N \) is a cubic residue too. From lemma 2.2.1 we know that there are a total of \( 2N \) cubic residues, with \( 2N - 1 \) gaps between them. These gaps together contains the \( 4N \) non-cubic residues. By assumption 2 there are at least two non-cubic residues in each gap. Hence we have used all but \( 4N - 2(2N - 1) = 2 \) of the non-cubic residues.

Finding the cubic residues: We want to find which gaps the two remaining non-cubic residues belong to. Since \( p > 13 \) we have that 1 and \( 2^3 = 8 \) are cubic residues. By assumption 2 we know that 2 and 3 are not cubic residues. Since \( \frac{2}{3} = 2 \) is not a cubic residue, we see that 4 can not be either. Then, to get an appropriate size of gaps between 1, a cubic residue and 8, we see that 5 is a cubic residue, and 6 and 7 are not. By lemma 2.2.2 the cubic residues has to be symmetric about \( \frac{6N}{2} \), hence we have the following cubic residues:

\[
1, 5, 8, 11, \ldots, 6N - 10, 6N - 7, 6N - 4, 6N
\]

Contradiction to assumption 2: Consider the special case \( N \geq 5 \), that is the primes \( p \geq 31 \). In this case, \( 27 = 3^3 \) is a cubic residue and \( 27 \equiv 0 \pmod{3} \). But if we look at the list of the cubic residues above, we see that all residues except 1 and 6N are congruent to 2 modulo 3. This is a contradiction, hence we must have \( p < 31 \). Then the only possible value of \( p \) is 19. In this case 7 is a cubic residue since \( 4^3 = 64 \equiv 7 \pmod{19} \). But this is a contradiction to the list of cubic residues we deduced above. Hence all values of \( p \) will give a contradiction, so one of our two initial assumptions must be wrong. If it is assumption 1 the proof is done. So we assume assumption 2 is wrong.

Primitive root modulo \( p \): Then there exists some cubic residues \( r, s \) such that \( r - s = 2 \). Let \( g \) be a primitive root modulo the prime \( p \). Then by proposition 1.1.1 there exists a positive integer \( q \) such that \( g^q = 2 \). Since 2 is not a cubic residue we see that \( 3 \not| q \). So either \( q = 3k + 1 \) or \( q = 3k - 1 \) for some positive integer \( k \).

Consider \( r + s \). If \( r + s \equiv 0 \pmod{p} \) then \( 2 = r - s \equiv 2r \pmod{p} \) which implies that \( r \equiv 1 \pmod{p} \), and since \( r < p \) we have \( r = 1 \). But this is impossible since \( r - s = 2 \). Hence \( r + s \not\equiv 0 \pmod{p} \) and by proposition 1.1.1 there exists a number \( m \) such that \( r + s \equiv g^m \pmod{p} \).
Contradiction to assumption 1  If $3|m$ then $r+s$ is a cubic residue. Since $r+s \equiv g^m \pmod{p}$ we get that $rs^{-1} + 1 \equiv g^{-1}s^{-1} \pmod{p}$, which contradicts assumption 1. Hence $m = 3l + 1$ or $m = 3l - 1$ for $l \in \mathbb{N}$.

First we will look at the case where either $m = 3l + 1$ and $q = 3k - 1$, or $m = 3l - 1$ and $q = 3k + 1$. We denote this case of opposite signs by $m = 3l \pm 1$ and $q = 3k \mp 1$. Then

$$r^2 - s^2 = (r-s)(r+s) = 2(r+s) \equiv g^{3(k+1)}g^{3l\pm 1} \pmod{p} = g^{3(k+l)}$$

and we get that $r^2s^{-2} - 1 \equiv g^{3(k+l)}s^{-2} \pmod{p}$. By assumption 1 we see that this is impossible.

So either we must have $m = 3l + 1$ and $q = 3k + 1$, or $m = 3l - 1$ and $q = 3k - 1$. We denote these cases of similar signs $3l \pm 1$ and $3k \pm 1$.

$$2r = (r-s) + (r+s) \Rightarrow g^{3k\pm 1}r \equiv g^{3k\pm 1} + g^{3l\pm 1} \pmod{p} \Rightarrow r \equiv 1 + g^{3(k-l)} \pmod{p}$$

Which contradicts assumption 1.

What we have proved here is that for the exponent $n = 3$ there exists only two auxiliary primes, namely 7 and 13. All other primes on the form $p = 6N + 1$ will not satisfy the NC-condition. Hence Germain’s plan to prove Fermat’s Last Theorem will fail for $n = 3$.

Even though Germain was aware that her grand plan would not work for $n = 3$, she still tried to find a proof of FLT for $n > 3$. As we know, she was not able to prove this claim, but she was still convinced that her grand plan would work. She justified this by a comprehensive analysis of primes on the form $2Nn + 1$ (from proposition 2.2.2 we know that the only primes that can satisfy the NC-condition will be on this form). For example she is able to prove that if $n > 3$ is a prime and 2 is not an $n$th power residue modulo $p = 2Nn + 1$, then the NC-condition is satisfied for $N = 1, 2, 4, 5$.

Germain also claims (but is not able to prove) that for each fixed $N$ there would be only a finite number of primes $n$ such that $p = 2Nn + 1$ is a prime satisfying the NC-condition. Note that this claim, if it were to be true, would not be enough to prove Fermat’s Last Theorem. What is required is that for each fixed $n$, there exists infinitely many values $N$ making $p = 2Nn + 1$ a prime satisfying the NC-condition.
2.3 Large Size Solutions

After Germain had proved that her plan to prove Fermat’s Last Theorem could not work, she tried to give estimates on how large a hypothetical solution set would be. We will state her proposition. The proof turns out to contain a mistake, but gives a fruitful insight into Germain’s way of thinking. It will also be important when we in the next chapter explore the work of Niels Henrik Abel, as it shows the similarities of their work on Fermat’s Last Theorem. Therefore we include it nonetheless. We will also give a short discussion on how one might try to fix Germain’s mistake and how it affects the generality of the proposition. This section is also due to the work in [LP08].

**Proposition 2.3.1.** Let \( n \) be an odd prime, and \( p \) an auxiliary prime satisfying the two conditions in Sophie Germain’s Theorem. If \( x^n + y^n = z^n \) then at least one of \( x + y, z - y \) or \( z - x \) is a multiple of \( n^{2n-1} \) and the \( n \)th power of all auxiliary primes.

Before going through the proof and the mistake in the proof, let us assume that the proposition holds and look at the consequences. Germain writes in a letter to Gauss, dated 1819, that she had been able to prove that any numbers providing a solution to Fermat’s equation, are numbers "whose size frightens the imagination". Let us look at the smallest possible value for the exponent. For \( n = 5 \) we have the auxiliary primes 11, 41, 71 and 101. Assume that the proposition above holds, and that \( x + y \) is divisible by the \( n \)th power of all auxiliary primes. Then, since \( z^n = (x + y)^\phi(x, -y) \), we see that \( z^n \) is divisible by \( 5^5 \cdot 11^5 \cdot 41^5 \cdot 71^5 \cdot 101^5 \) which gives a 39 digit number. Certainly this is a number whose size can frighten anyone.

**Germain’s attempt to prove proposition 2.3.1**

We will now go through Germain’s attempted proof step by step, and indicate where and why it does not work.

**Preliminaries** Assume \( x^n + y^n = z^n \) where \( x, y, z \) are natural numbers. We assume that \( x, y \) or \( z \) are pairwise relatively prime. By Sophie Germain’s Theorem we know that at least one of \( x, y, z \) is divisible by \( n \). We will show that if \( n \mid z \), then \( x + y \) is a multiple of \( n^{2n-1} \) and the \( n \)th power of all auxiliary primes. With a similar argument, one can show the same for \( z - y \) and \( z - x \), assuming that \( n \) divides \( x \) or \( y \) respectively.

**Equations** From the proof of Sophie Germain’s Theorem we have the following equations, given that none of \( x, y, z \) is divisible by \( n \):
2.3. LARGE SIZE SOLUTIONS

\[ x + y = a^n \quad \phi(x, -y) = \alpha^n \quad a\alpha = z \tag{2.5} \]
\[ z - x = b^n \quad \phi(x, z) = \beta^n \quad b\beta = y \tag{2.6} \]
\[ z - y = c^n \quad \phi(y, z) = \gamma^n \quad c\gamma = x \tag{2.7} \]

But assuming that \( n \) divides \( z \), the argument that we used to deduce eq. (2.5) fails. We want to modify it using the divisibility of \( n \). By assumption \( x + y \equiv x^n + y^n = z^n \equiv 0 \pmod{n} \). Let \( s = x + y \). Then

\[ \phi(x, -y) = \frac{x^n + y^n}{x + y} = \frac{(s - y)^n + y^n}{s} \]
\[ = \frac{1}{s} \sum_{i=0}^{n-1} (-1)^i \binom{n}{i} s^{n-i} y^i \]
\[ = s^{n-1} - \left( \frac{n}{1} \right) s^{n-2} y + \ldots + \left( \frac{n}{n-1} \right) y^{n-1} \tag{2.10} \]

From the last equation we observe that \( \phi(x, -y) \) is divisible by \( n \), but not of any higher power of \( n \). Then, since \( z^n = (x + y)\phi(x, -y) \), we observe that \( x + y \) is divisible by \( n^{mn-1} \) for some integer \( m \). Hence eq. (2.5) above needs to be replaced by the following:

\[ x + y = n^{mn-1} a^n \quad \phi(x, -y) = n\alpha^n \tag{2.5'} \]

Where both \( a \) and \( \alpha \) are integers relatively prime to \( n \).

**Divisibility by** \( n^2 \) We will now show that \( z \equiv 0 \pmod{n^2} \). From eq. (2.6) and eq. (2.7) we can see that \( b^n + c^n = 2z - (x + y) \equiv 0 \pmod{n} \). Hence \( b + c \equiv 0 \pmod{n} \) and we can write \( b = kn - c \) for some \( k \in \mathbb{Z} \). Then

\[ b^n = (kn)^n - \left( \frac{n}{1} \right) (kn)^{n-1} c + \ldots + \left( \frac{n}{n-1} \right) kn c^{n-1} - c^n \]

From this we can conclude that \( b^n \equiv -c^n \pmod{n^2} \). Then

\[ 2z - (x + y) = b^n + c^n \equiv 0 \pmod{n^2} \]

and since we already know that \( x + y \equiv 0 \pmod{n^2} \) we see that we must also have \( z \equiv 0 \pmod{n^2} \).
Closing argument that goes wrong  Germain now proceeds to do a final argument based on eq. (2.5), eq. (2.6) and eq. (2.7), seemingly forgetting that the first equation should be replaced by eq. (2.5') according to the changed assumption on \( z \). We will follow her reasoning in this paragraph, but the reader should keep in mind that this is based on a false assumption.

We want to prove that \( z \equiv 0 \pmod{p} \), where \( p \) denotes any auxiliary prime to \( n \) that also satisfies the second condition in Sophie Germain’s Theorem. Since \( p \) satisfy the NC-condition, and \( z^n + (-y)^n + (-x)^n \equiv 0 \pmod{p} \), we know that \( p|xyz \). Assume for contradiction that \( p|y \). Using equation eq. (2.5) and eq. (2.7) gives

\[
a^n - c^n = (x + y) - (z - y) \\
\equiv -(z - x) \pmod{p} \\
\equiv -b^n \pmod{p} \\
\Rightarrow a^n + b^n + (-c)^n \equiv 0 \pmod{p}
\]

Since \( p \) is an auxiliary prime to \( n \), it must divide \( abc \), and since \( x, y, z \) are assumed to relatively prime, \( p \) must divide \( b \). This further implies that \( z \equiv x \pmod{p} \). Then \( \beta^n = \phi(x, z) \equiv nx^{n-1} \) and \( a^n = x + y \equiv x \pmod{p} \). Using this we see that

\[
\beta^n \equiv n(a^{n-1})^n \pmod{p}
\]

Since \( a \not\equiv 0 \pmod{p} \), we also have that \( a^{n-1} \not\equiv 0 \pmod{p} \). Then there exists a number \( g \) such that \( ga^{n-1} \equiv 1 \pmod{p} \). Thus we have

\[
g^n \beta^n \equiv ng^n(a^{n-1})^n \equiv n \pmod{p}
\]

which contradicts the second condition on \( p \), namely that \( x^n \equiv n \pmod{p} \) is impossible for any integer \( x \). So clearly our assumption that \( y \equiv 0 \pmod{p} \) was wrong. A similar argument also proves that \( p|x \), hence we can conclude that \( z \equiv 0 \pmod{p} \).

This means that \( z \) is divisible by any auxiliary prime \( p_i \). Assuming there are finitely many of these, we have that

\[
y + x = \frac{z^n}{\phi(x, -y)} \\
= \frac{p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k} n^{2n} m}{na^n}
\]

where \( m \in \mathbb{Z} \), and where we used (2.5'), and not eq. (2.5). The result is appealing and the proof as well, but it is also clear to us that it is not complete. Note however, that it is only the part where we prove that \( z \equiv 0 \pmod{p} \) that
is false. The divisibility with \( n^2 \) is correct, and is sometimes referred to as the strong version of Sophie Germain’s Theorem. In the case where \( n = 5 \), it implies that if \( n | z \), then

\[
x + y = \frac{z^n}{n^{\alpha n}} = \frac{(kn^2)^n}{n^{\alpha}} = \frac{k^n}{\alpha^n} n^{2n-1}
\]

i.e. \( x + y \) is divisible by \( 5^0 = 1953125 \). It is not as big as the 39 digit number we would get using proposition 2.3.1, but it can still be seen as an indication that any solution to Fermat’s equation must be large.

**Proof of proposition 2.3.1 under the right conditions**

We will now explore what happens if we make the same kind of argument as in the last paragraph, but using (2.5') instead of equation eq. (2.5).

Similarly as the previous paragraph, we assume for contradiction that \( y \equiv 0 \) (mod \( p \)). Then we add equation eq. (2.7) and (2.5') to get

\[
n^{mn-1}a^n - c^n = (x + y) - (z - y) \equiv -(z - y) = -b^n
\]

which gives

\[
c^n - b^n \equiv n^{mn-1}a^n \pmod{p}
\]

To get the desired contradiction, Germain used the first condition on \( p \), namely that \( x^n + y^n + z^n \equiv 0 \pmod{p} \Rightarrow x \equiv 0, y \equiv 0 \) or \( z \equiv 0 \pmod{p} \). But as we have a factor \( n^{mn-1} \) in the present case, this condition will not give us a contradiction. It appears that an additional condition on \( p \) is required. The obvious one is to say that there are no two non-zero \( n \)th power residues whose difference is \( n^{mn-1} \pmod{p} \).

Working under this new additional condition, we easily get the desired contradiction. Because \( a \not\equiv 0 \) (mod \( p \)), so there exists a number \( g \) such that \( ag \equiv 1 \) (mod \( p \)). Then

\[
(c^n - b^n)g^n \equiv n^{mn-1}a^n g^n \pmod{p}
\]

\[
\Rightarrow (cg)^n - (bg)^n \equiv n^{mn-1} \pmod{p}
\]

which is a contradiction. So the proposition we are able to prove by these method is:

**Proposition 2.3.2** (modified version of proposition 2.3.1). Let \( n \) be an odd prime, and \( p \) an auxiliary prime to \( n \) satisfying the second condition of Sophie Germain’s Theorem, and the additional condition that there does not exist any two non-zero \( n \)th power residues whose difference is \( n^{n-1} \). If \( x^n + y^n = z^n \) then either \( x + y, z - y \) or \( z - x \) is a multiple of \( n^{2n-1} \) and the \( n \)th power of all auxiliary primes.
One may wonder if there exists many such auxiliary primes satisfying all three conditions. Looking back at example 2 in chapter 1, we have $n = 3$, $p = 7$ and the 3rd power residues modulo 7 are 1 and 6. Since $6 - 1 = 5$ and $n^{n-1} = 9 \equiv 2 \pmod{7}$, we see that 7 is a prime satisfying this new condition. It is also easy to see that it satisfies the conditions in Sophie Germain’s Theorem.

However, we will quickly find an example where our new condition fails. We already know that 11 is an auxiliary prime to 5, but it fails for the added condition. This is because $n^{n-1} = 5^4 = 625 \equiv 9 \pmod{11}$ and $2^5 - 1^5 = 32 - 1 = 31 \equiv 9 \pmod{11}$.

Therefore we think it is fair to say that the generality of the new proposition is not as good as what we may initially have hoped for.
Chapter 3

Niels Henrik Abel

In this chapter we will investigate Abel's four theorems, and give proofs where we have found it possible. Some of the proofs are given in literature and some are not, we will specify which. For some of Abel's statements there has not yet been found a direct proof. In this chapter we will restrict ourselves to use only elementary methods, as the goal is to rediscover Abel's proofs. We will discover that using similar methods as Germain, we are able to prove much of Abel's theorems, but that it is not enough to prove them all in full generality. As we will use what Abel calls Theorem II several times later, we will prove that first, before investigating Theorem I, III and VI.

Abel does not say much in the letter about his efforts to prove Fermat's Last Theorem, so we include his only comment:

Besides reading, I have done some work myself. I have tried to prove the impossibility of the equation $a^n = b^n + c^n$ in whole numbers when $n$ is larger than 2, but I have been tied up. I could not go beyond the attached theorems, which are quite curious.

3.1 Theorem II

In Theorem II, Abel investigates restrictions on hypothetical solutions to the equation $a^n = b^n + c^n$ under different assumptions on $a$, $b$ and $c$. Three out of five of the relations Abel discovered, was already published by an English mathematician, Peter Barlow, in 1811.

We will give the proof of Theorem II as described by Ribenboim in [Rib08]. Ribenboim only gives the proofs for the first three cases of the theorem. We will argue that the last two cases of the theorem is superfluous. Observe that the methods used here are very similar to the ones Germain used.
Theorem 3.1.1 (Theorem II). If you have positive integers $a, b, c$ such that $a^n = b^n + c^n$ for some odd prime $n$, then you can always find factorizations $a = t\alpha$, $b = r\beta$ and $c = s\gamma$ such that each pair of integers $(t, \alpha)$, $(r, \beta)$ and $(s, \gamma)$ are relatively prime, and such that one of the following five cases always applies:

Case 1:
$$a = \frac{t^n + r^n + s^n}{2} \quad b = \frac{t^n + r^n - s^n}{2} \quad c = \frac{t^n - r^n + s^n}{2}$$

Case 2:
$$a = \frac{n^{mn-1}t^n + r^n + s^n}{2} \quad b = \frac{n^{mn-1}t^n + r^n - s^n}{2} \quad c = \frac{n^{mn-1}r^n + s^n}{2}$$

Case 3:
$$a = \frac{t^n + r^{mn-1}n^n + s^n}{2} \quad b = \frac{t^n + r^{mn-1}r^n - s^n}{2} \quad c = \frac{t^n - r^{mn-1}r^n + s^n}{2}$$

Case 4:
$$a = \frac{n^{mn-1}t^n + r^n + s^n}{2} \quad b = \frac{n^{mn-1}(t^n + r^n) - s^n}{2} \quad c = \frac{n^{mn-1}(t^n - r^n) + s^n}{2}$$

Case 5:
$$a = \frac{t^n + r^{mn-1}(n^n + s^n)}{2} \quad b = \frac{t^n + r^{mn-1}(n^n - s^n)}{2} \quad c = \frac{t^n - r^{mn-1}(n^n - s^n)}{2}$$

Proof: Case 1, 2 and 3. We put restrictions on the divisibility of $n$ and $a, b, c$ to get the different cases.

**Case 1: $n$ does not divide $abc$** Suppose that $n$ does not divide $abc$. We write $a^n = b^n + c^n = (b + c)\phi(b, -c)$. Assume $q$ is a prime dividing both $b + c$ and $\phi(b, -c)$. Then $b \equiv -c \pmod{q}$ and hence $\phi(b, -c) \equiv nb^{n-1} \equiv 0 \pmod{q}$. Hence either $b \equiv 0$ or $n \equiv 0 \pmod{q}$. The first is a contradiction to the assumption that $a$ and $b$ are relatively prime, and the latter is impossible since we have assumed that $n \not| abc$. Hence $b + c$ and $\phi(b, c)$ are relatively prime which again implies that they are both $n$th powers. The exact same argument works for $b^n$ and $c^n$. Hence there exists positive integers $s, r, t, \alpha, \beta, \gamma$ such that:

$$b + c = t^n \quad \phi(b, -c) = \alpha^n$$
$$a - c = r^n \quad \phi(a, c) = \beta^n$$
$$a - b = s^n \quad \phi(a, b) = \gamma^n$$

Solving for $a$ in the equations above we get
$$2a = t^n + s^n + r^n$$

Hence $a = \frac{t^n + s^n + r^n}{2}$ as desired. A similar argument gives us the expressions for $b$ and $c$. 

3.1. **Theorem II**

**Case 2: \( n \) divides \( a \)**  Now suppose that \( n \) divides \( a \). Then a similar argument as in the previous case gives us that \( a - c = r^n \) and \( a - b = s^n \). But when trying to prove that \( b + c \) and \( \phi(b, -c) \) are relatively prime our changed assumption makes us unable to say that \( n \equiv 0 \pmod{q} \) is impossible. We clearly need another approach. Setting \( k = b + c \) we see that \( n \) divides \( k \) since \( k = b + c \equiv b^n + c^n \equiv 0 \pmod{n} \). Then

\[
\phi(b, -c) = \frac{b^n + c^n}{b + c} = \frac{(k - c)^n + c^n}{k} = \sum_{i=0}^{n-1} (-1)^i \binom{n}{i} k^{n-i-1} c^i
\]

\[
= k^{n-1} - \binom{n}{1} k^{n-2} c + \ldots + \binom{n}{n-1} c^{n-1}
\]

Since \( n \) does not divide \( c \) we see from the last expression that \( \phi(b, -c) \) is divisible by \( n \), but not of any higher power of \( n \). Hence \( \phi(b, -c) = n \alpha^n \) and \( b + c = n^{nm-1} t^n \) for some integers \( t, \alpha \) both relatively prime to \( n \). With this new expression for \( b + c \), we get the desired relations by solving the equations for \( a, b, c \) as in the previous case.

**Case 3: \( n \) divides \( b \)**  The proof is similar to the case when \( n \) divides \( a \). We get that \( a - b = r^n \) and \( b + c = t^n \). Setting \( k = a - c \) and investigating \( \phi(a, c) = \frac{a^n - c^n}{a - c} = \frac{(k+c)^n - c^n}{k} \) we get that \( a - c = n^{nm-1} r^n \).

Of course the case where \( n \) divides \( c \) would give completely similar expressions as in case 2 and 3, but with the factor \( n^{nm-1} \) being multiplied with \( s^n \) instead of \( t^n \) or \( r^n \) respectively. Including this case, we have no cases left to explore when trying to prove case 4 and 5.

If we use the expressions given in the theorem for \( a, b, c \) in case 4 and 5, we can evaluate the different sums of \( a, b \) and \( c \). For example, in case 4 we have

\[
a + b = n^{nm-1} (t^n + r^n)
\]

so \( n \) must divide \( a + b \). Similarly we get that \( n \) must divide \( b + c \) and \( a - c \), which of course implies that \( n \) divides both \( a \) and \( b \). But then \( n \) must also divide \( c \), and therefore we can simply divide some multiple of \( n \) out of the equation \( a^n = b^n + c^n \) and end up in case 1. So even though it may be possible to write \( a, b, c \) as given in case 4 and 5, it seems like these cases are somewhat unnecessary.
3.2 Theorem I

We start our investigation of Theorem I by stating it the way Abel did it himself.

**Theorem 3.2.1 (Theorem I).** The equation \( a^n = b^n + c^n \), where \( n \) is a prime number, does not have a solution when one or more of the numbers \( a, b, c, \sqrt[n]{a}, \sqrt[n]{b}, \sqrt[n]{c}, a + b, a + c, b - c \), are prime numbers.

In 1946, Inkeri proved the six first cases under the assumption that \( n \nmid abc \), but as he uses non-elementary methods, this proof could not have been the one that Abel discovered. However, we have found that using methods similar to Germain, it is possible to prove the cases where \( a, b, \sqrt[n]{a} \) and \( \sqrt[n]{b} \) are primes in full generality. We have also combined some lemmas from [Ink46] and obtained a proof for the case of \( c \) when \( n \nmid abc \), using only elementary methods. For the three last cases, we have not succeeded in proving them in full generality, but making some additional assumptions takes us at least somewhat closer to the goal.

We will start by stating and proving a simple, but useful lemma.

**Lemma 3.2.2.** If \( a, b, c \) are pairwise relatively prime positive integers such that \( a^n = b^n + c^n \) for some odd prime \( n \), then \( b, c < a \) and \( a < b + c \).

**Proof.** The first claim is obvious since if \( a \leq b \), then \( b^n \geq a^n = b^n + c^n \).

For the second statement, if \( a \geq b + c \) then \( a^n \geq (b + c)^n \). Then \( b^n + c^n \geq b^n + \sum_{i=1}^{n-1} \binom{n}{i} b^{n-i} c^n + c^n \) which would imply that \( \sum_{i=1}^{n-1} \binom{n}{i} b^{n-i} c^n \leq 0 \). This is obviously a contradiction since \( a, b, c \) are all positive integers. \( \blacksquare \)

We will shortly give a proof for the cases where \( a \) and \( b \) are prime powers, where we have assumed that \( 0 < c < b < a \). Abel mentions nothing of such an assumption, but we will see that it is crucial. Since we are only working with positive integers, we see that \( a - c \neq 1 \), but it may happen that \( a - b = 1 \). We hope the proofs will clarify the importance of this distinction.

**Proposition 3.2.1.** The equation \( a^n = b^n + c^n \), where \( n \) is an odd prime, does not have a solution when one or more of the numbers \( a, b, \sqrt[n]{a} \) or \( \sqrt[n]{b} \) are prime numbers.

**Proof.** We make the usual assumptions when dealing with Fermat’s Last Theorem. That is, we assume that \( a, b, c \) are pairwise relatively prime, \( n \) is an odd prime and that they are all positive integers.

\( a \) is prime \quad Assume \( a \) is a prime number. Since \( n \) is odd we can factor the equation:

\[
a^n = b^n + c^n = (b + c)(b^{n-1} - b^{n-2}c + \ldots + bc^{n-2} + c^{n-1}) = (b + c)\phi(b, -c)
\]
3.2. THEOREM I

Observe that \( b + c \neq 1 \). Since \( a \) is prime, both \( b + c \) and \( \phi(b, -c) \) have to be powers of \( a \). From lemma 3.2.2 we get that \( b + c < 2a \). Since \( b + c \) has to be a power of \( a \) the only alternative is that \( b + c = a \). But this is a contradiction to the fact that \( a < b + c \).

**b is prime** Since \( b^n = a^n - c^n = (a - c)\phi(a, c) \) and \( a - c > 1 \) we see that \( a - c \) has to be a power of \( b \). From lemma 3.2.2 we see that \( a - c < b \) which is a contradiction.

**\( \sqrt{a} \) is prime** Suppose \( \sqrt{a} = p \), where \( p \) is a prime number. Using the same factorization as in the case where \( a \) is prime, we get that \( b + c \) has to be a power of \( p \). Then \( b \equiv -c \pmod{p} \) and \( b^{n-1} - b^{n-2}c + \ldots + c^{n-1} \equiv 0 \pmod{p} \). Furthermore \( b^{n-1} - b^{n-2}c + \ldots + c^{n-1} \equiv n b^{n-1} \equiv 0 \pmod{p} \), which implies that either \( n \equiv 0 \) or \( b \equiv 0 \pmod{p} \). The latter is impossible because we are assuming that \( a \) and \( b \) are relatively prime. Hence \( n \equiv 0 \pmod{p} \) and since \( n \) is a prime we have that \( n = p \).

From the lemma 3.2.2 we have that \( b + c < 2a = 2p^m < p^{m+1} \), where we used the fact that \( n \) is an odd prime to get the last inequality. We also know that \( a < b + c \), hence \( p^m < b + c < p^{m+1} \) which contradicts the fact that \( b + c \) is a power of \( p \).

**\( \sqrt{b} \) is prime** By assumption \( b^m = p \) for some prime number \( p \). In this case we see that \( a - c \) and \( \phi(a, c) \) have to be powers of \( p \). So we have \( a \equiv c \pmod{p} \) which implies that \( \phi(a, c) \equiv na^{n-1} \pmod{p} \). It is impossible that \( a \equiv 0 \pmod{p} \) since \( a, b \) are assumed to be relatively prime. Hence \( n \equiv 0 \pmod{p} \) which implies that \( n = p \) since both numbers are prime.

Now set \( s = a - c \). Observe that \( s \equiv 0 \pmod{p} \). Then

\[
\phi(a, c) = \frac{b^n}{a - c} = \frac{a^n - c^n}{s} = \frac{(s + c)^n - c^n}{s} = \frac{1}{s} \sum_{i=0}^{n-1} \binom{n}{i} s^{n-i} c^i = s^{n-1} + \frac{n}{1} s^{n-2} c + \ldots + \frac{n}{n-2} s^2 c^{n-2} + \frac{n}{n-1} c^{n-1}
\]

implies that \( \phi(a, c) \) is divisible by \( p \), but not by any higher power of \( p \). Hence \( \phi(a, c) = p \) and \( a - c = p^{m-1} \). But from lemma 3.2.2 we know that \( a - c < b = p^m \) so we have a contradiction.

\[\blacksquare\]
It is clear that the proofs above all relied on the fact that $b + c$ or $a - c$ were both larger than 1. Of course one may prove the case where $c$ is a power of a prime in exactly the same way as we did for $b$, but then we have to make the additional assumption that $a - b \neq 1$.

By combining results from [Rib79] and [Ink46], we have found it possible to prove Abel’s assertion also in the case when $a - b = 1$ under the additional assumption that $n \nmid abc$. This approach uses several lemmas proved by Inkeri. But where Inkeri’s argument rests on a result from class field theory, we will show that it is possible to complete the proof with only elementary methods. This proof was therefore within the reach of Abel.

We will include all proofs so that the reader may be certain that only elementary methods is used.

**Lemma 3.2.3.** If $a, b, c$ are positive integers such that $a^n = b^n + c^n$ for some odd prime $n$, and if $0 < c < b < a$, then we have

1. $0 < a - b < a - c < b + c$
2. $\phi(b, -c) < \phi(a, c) < \phi(a, b)$

**Proof.** Since $c < b$ we obviously have that $a - b < a - c$. Using lemma 3.2.2 we see that $a - c < a < b + c$, so the first statement in our lemma holds.

For the last statement, we see that since $c < b < a$ we have

$$\phi(b, -c) = b^{n-1} - b^{n-2}c + \ldots - bc^{n-2} + c^{n-1}$$

$$< b^{n-1} + b^{n-2}c + \ldots + bc^{n-2} + c^{n-1}$$

$$< a^{n-1} + a^{n-2}c + \ldots + ac^{n-2} + a^{n-1}$$

$$= \phi(a, c)$$

$$< a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}$$

$$= \phi(a, b)$$

The next lemma is due to Grünert (1856), and a proof can be found in [Rib79] p.226.

**Lemma 3.2.4.** Let $a, b, c$ be integers such that $0 < c < b < a$ and $a^n = b^n + c^n$ for some odd prime $n$. Then $n < c$.

**Proof.** We have that

$$c^n = a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1}) > (a - b)nb^{n-1}$$

and since $\frac{c}{b} < 1$, this implies that

$$a - b < \frac{c^n}{nb^{n-1}} < \frac{c}{n}$$
Thus

\[ a < b + \frac{c}{n} \]

We also have that \( b + 1 \leq a \), and therefore also that

\[ b + 1 < b + \frac{c}{n} \]

This gives us the desired inequality.

Finally we prove an inequality due to Inkeri [Ink46, section 22], which will be of great importance.

**Lemma 3.2.5** (Inkeri’s Inequality). *Let \( u, v \) be positive real numbers and let \( n > 5 \). If \( u + v \leq 1 \) then*

\[ (u^n + v^n + 1)^n < (1 + u^n - v^n)^n + (1 - u^n + v^n)^n \]

**Proof.** We will essentially check for all possible values of \( u \) and \( v \), but first we define the following:

\[
\begin{align*}
    f_1 &= f_1(u, v) = (1 + u^n - v^n)^n \\
    f_2 &= f_2(u, v) = (1 - u^n + v^n)^n \\
    f_3 &= f_3(u, v) = (1 + u^n + v^n)^n
\end{align*}
\]

Observe that

\[
\begin{align*}
    f_1 + f_2 &= \sum_{i=0}^{n} \binom{n}{i}(u^n - v^n)^i + \sum_{i=0}^{n} (-1)^i \binom{n}{i}(u^n - v^n)^i \\
    &= 2 + 2 \sum_{i=1}^{n-1} \binom{n}{2i}(u^n - v^n)^{2i} \\
    &> 2
\end{align*}
\]

First we consider the case when \( u, v \leq \frac{1}{2} \). Then
\[ f_3 \leq f_3 \left( \frac{1}{2}, \frac{1}{2} \right) \]
\[ = (1 + \frac{1}{2^{n-1}})^n \]
\[ < \sum_{i=1}^{n} \binom{n}{i} \left( \frac{1}{2^{n-1}} \right)^i \]
\[ < \frac{1}{2^{n-1}} \sum_{i=1}^{n} \binom{n}{i} \]
\[ = \frac{1}{2^{n-1}} (2^n - 1) \]
\[ < 2 \]

so we get \( f_3 < f_1 + f_2 \) as desired.

In general, we may assume that \( u > \frac{1}{2} \). Then we always have \( v \leq 1 - u \).

We see that \( f_3 \leq f_3(u, 1 - u) \) and using eq. (3.2) we also observe that

\[ f_1(u, 1 - u) + f_2(u, 1 - u) \leq f_1 + f_2 \]

So to prove the lemma it will be enough to consider the case where \( v = 1 - u \).

Observe that for two positive numbers \( a, b \) where \( a > b \), we have that

\[ nb^{n-1} < \phi(a, b) < na^{n-1} \]

and since \( \phi(a, b) = \frac{a^n - b^n}{a - b} \), this implies that

\[ n(a - b)b^{n-1} < a^n - b^n < n(a - b)a^{n-1} \]  \hspace{1cm} (3.4)

Now since \( f_3 > f_1 > 0 \) and from eq. (3.4) we get that

\[ f_3 - f_1 < 2nv^n(1 + u^n + v^n)^{n-1} \]  \hspace{1cm} (3.5)

Also observe that

\[ f_2 > (1 - u^n)^n = ((1 - u)\phi(1, u))^n = v^n \phi(1, u)^n \]  \hspace{1cm} (3.6)

These two last relations, eq. (3.5) and eq. (3.6), will be used several times for the remaining parts of the proof.

Consider the case \( \frac{3}{4} \leq u < 1 \). Remember that \( u + v = 1 \) so we also have that \( u^n + v^n < (u + v)^n = 1 \). Then eq. (3.5) gives us that

\[ f_3 - f_1 < n(2v)^n \]

Using the sum of a geometric series gives
3.2. THEOREM I

\[ \phi(1, u) \geq \phi(1, \frac{3}{4}) = \sum_{i=0}^{n-1} \left( \frac{3}{4} \right)^i = 4 \left( 1 - \left( \frac{3}{4} \right)^n \right) > 3 > 2 \sqrt[5]{5} > 2 \sqrt[5]{n} \]

where we have used the fact that \( \sqrt[5]{l} > \frac{l+1}{\sqrt[5]{l+1}} \) for all \( l \geq 3 \) to get the last inequality. Then, by eq. (3.6), we see that

\[ f_2 > n(2v)^n \]

and thus that \( f_1 + f_2 > f_3 \) as desired.

Finally we consider the case where \( \frac{1}{2} < u < \frac{3}{4} \). Then

\[ u^n + v^n = u^n + (1-u)^n < \left( \frac{3}{4} \right)^5 + \left( \frac{1}{4} \right)^5 < \frac{1}{4} \]

hence

\[ f_3 - f_1 < 2nv^n \left( 1 + \frac{1}{4} \right)^{n-1} = 8nv^n \left( \frac{5}{4} \right)^n \]

Since \( n > 5 \) we also have that

\[ \phi(1, u) = \frac{1 - u^n}{1 - u} > \frac{1 - \frac{1}{2}}{2} = \frac{31}{16} > \frac{5}{4} \sqrt[5]{8} > \frac{5}{4} \sqrt[5]{8n} \]

which implies that

\[ f_2 > \frac{8}{5}nv^n \left( \frac{5}{4} \right)^n \]

Hence \( f_1 + f_2 > f_3 \) as desired. \[ \square \]

Now we are able to prove the following:

**Proposition 3.2.2.** Let \( a, b, c \) be integers such that \( 0 < c < b < a \), and assume that \( n \not| abc \). Then the equation \( a^n = b^n + c^n \) has no solutions in the case where \( c \) or \( \sqrt[5]{c} \) is a prime number.

**Proof.** Using the exact same methods as in the proof of proposition 3.2.1 one can prove this theorem when \( a - b \neq 1 \). So we may assume that \( a - b = 1 \).

From Theorem II we know that there exist relatively prime positive integers \( s, \gamma \) such that \( c = s^n \gamma^n \). But since \( s^n = a - b = 1 \) we see that \( s = 1 \). Then, using the expressions for \( a, b \) and \( c \) from Theorem II, we get that

\[ (t^n - r^n + 1)^n = (t^n + r^n + 1)^n - (t^n + r^n - 1)^n \]

Since \( a - c < b + c \) we have that \( r < t \). Dividing by \( t^n \) and setting \( u = \frac{r}{t} \) and \( v = \frac{1}{t} \) we get
\[(1 - u^n + v^n) = (1 + u^n + v^n)^n - (1 - u^n + v^n)^n\]

Since \(u, v\) are positive real numbers and \(u + v = \frac{r + 1}{n} \leq 1\), this contradicts Inkeri's inequality.

We have seen that using the methods of Germain, we were able to prove the cases for \(a\) and \(b\) being prime, but for the smaller number \(c\), the proof becomes more complicated. It is impossible to know whether Abel proved his theorem using Inkeri's inequality or not, but we can see that it was definitely within his reach mathematically. Also note that even though we only used elementary methods, the proof shares little similarities with Germain's techniques.

The reason why this proof does not work for case II, is that Inkeri's inequality requires that \(u + v \leq 1\). In the proof of proposition 3.2.2 this condition was ensured because \(r < t\). But in case II we would for example have divisibility of \(a\), hence we would get that \(r < \sqrt{n^m - 1}\), which is not enough to fulfill the condition in Inkeri's inequality.

We will now turn our focus to the three remaining cases of Theorem I, namely that \(b - c\), \(a + b\) or \(a + c\) is a prime number.

**Proposition 3.2.3.** The following two cases holds:

i) Assume that \(a + b\) is a prime number. If \(n \nmid ab\), then the equation \(a^n = b^n + c^n\) has no solutions.

ii) Assume that \(a + c\) is a prime number. If \(n \nmid ac\), then the equation \(a^n = b^n + c^n\) has no solutions.

**Proof.** We prove only the first case, as the proof of the second is similar.

By Abel's Theorem II we know that there exist positive integers \(r, t\) such that \(a - c = r^n\) and \(b + c = t^n\). This implies that

\[a + b = (a - c) + (b + c) = r^n + t^n = (r + t)\phi(r, -t)\]

Since \(a + b\) is a prime number, and \(r + t > 1\) this implies that \(r + t = a + b\) and \(\phi(r, -t) = 1\). But \(\phi(r, -t) = r^{n-1} - r^{n-2}t + ... - rt^{n-2} + t^{n-1}\) and since \(r < t\) we can see easily that \(\phi(r, -t) > 1\). So we have a contradiction.

Observe that if \(n\) divides \(b\), we get \(a + b = n^{nm-1}r^n + t^n\) which does not enable us to deduce a contradiction the same way as in the proof above.

The same occur when \(n\) divides \(a\), hence these two cases requires a different approach. It may seem tempting to prove the special case \(a + b = n\), but since we also would have the restriction \(n|ab\), we would have \(n\) as a factor in both \(a\) and \(b\). This is of course impossible.

Some difficulties also arise in the case where \(b - c\) is a prime number. Then \(b - c = r^n - s^n\), so to use the same proof as above, one would have to make
3.2. **THEOREM I**

the additional assumption that \( r - s > 1 \). This leaves us with the case where \( r - s = 1 \). We have not succeeded in proving these cases, but includes the following as a proposition:

**Proposition 3.2.4.** Assume that \( b - c \) is a prime number. Assume that \( n \nmid bc \). Then we know there exist numbers \( r, s \) such that \( b - c = r^n - s^n \). Assume that \( r - s > 1 \). Then the equation \( a^n = b^n + c^n \) has no solutions.

**Proof.** We write \( b - c = (a - c) - (a - b) = r^n - s^n = (r - s)\phi(r, s) \). Allowing the assumption \( r - s > 1 \), we see that \( r - s = p \) and \( \phi(r, s) = 1 \). Then we can go through the proof exactly the same way as for the proposition above. ■

Before proceeding we will sum up the results from this chapter. We have proven the following:

<table>
<thead>
<tr>
<th>The equation ( a^n = b^n + c^n ) does not have any solutions when one or more of the numbers ( a, b, \sqrt[n]{a} ) or ( \sqrt[n]{b} ) are prime numbers. The same also holds in the following cases:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ( c ) is a prime and ( n \nmid abc )</td>
</tr>
<tr>
<td>• ( \sqrt[n]{a} ) is a prime and ( n \nmid abc )</td>
</tr>
<tr>
<td>• ( a + b ) are prime and ( n \nmid ab )</td>
</tr>
<tr>
<td>• ( a + c ) are prime and ( n \nmid ac )</td>
</tr>
<tr>
<td>• ( b - c ) are prime, ( n \nmid bc ) and ( r - s &gt; 1 ).</td>
</tr>
</tbody>
</table>

Observe that the cases of Theorem I that we have not been able to prove, are all associated to case II of Fermat’s Last Theorem. That is, the difficulties always seem to arise when \( n \) divides \( abc \).

**Some additional cases to Theorem I**

What if one of \( a - b \), \( a - c \) and \( b + c \) are prime numbers?

**Proposition 3.2.5.** Let \( a, b, c \) be positive integers, and let \( n \) be an odd prime. If either of the numbers \( b + c \), \( a - b \) or \( a - c \) are prime, then the equation \( a^n = b^n + c^n \) have no solutions.

**Proof.** We prove only the case where \( b + c \) is a prime. The others can be shown in a similar way.

Let \( b + c = p \), where \( p \) is a prime. As before, write \( a^n = (b + c)\phi(b, -c) \) where \( \phi(b, -c) = b^{n-1} - b^{n-2}c + \ldots + c^{n-1} \). Assume \( q \) is a prime dividing both \( b + c \) and \( \phi(b, -c) \). Then \( q = p \) and since \( \phi(b, -c) \equiv nb^{n-1} \pmod{p} \) and \( p \) does not divide \( b \), we get that \( p = n \). Now write:
\[
\phi(b, -c) = \frac{a^n}{b - c} = \frac{b^n + c^n}{p} = \frac{(p - c)^n + c^n}{p} = \sum_{i=0}^{n-1} (-1)^i \binom{n}{i} p^{n-1-i} c^i = p^{n-1} - \binom{n}{1} p^{n-2} c \ldots + nc^{n-1}
\]

Since \( p \) divides \( a \) we have that it does not divide \( c \). Hence \( \phi(b, -c) \) is divisible by \( p \), but not by any higher power of \( p \). Thus we can write \( \phi(b, -c) = pa \) where \( p \) does not divide \( a \). Hence \( a^n = p^\alpha \). But \( n \) is assumed to be an odd prime, so this is a contradiction. ■

We see that the case \( b + c \) is prime is much easier than the case which Abel included, namely that \( b - c \) is a prime number. We can only wonder why Abel chose to include the case \( b - c \) instead of \( b + c \).

3.3 Theorem III

Theorem III turns out to be a reformulation of Theorem II, and therefore does not require a separate proof. Abel states the theorem as follows:

**Theorem 3.3.1 (Abel’s Theorem III).** If the equation \( a^n = b^n + c^n \) have a solution, then \( a \) can be written in one of the following ways:

1) \( a = \frac{x^n + y^n + z^n}{2} \)

2) \( a = \frac{x^n + y^n + n^{nm-1} z^n}{2} \)

3) \( a = \frac{x^n + n^{nm-1}(y^n + z^n)}{2} \)

where the integers \( x, y, z \) are all pairwise relatively prime.

If we assume \( n \ not divide abc \) we get case i) and assuming that \( n|a, n|b \) or \( n|c \) we can prove that \( a \) can be written on the form in case ii). The last case corresponds to case 4 and 5 of Theorem II, which we have already argued is somewhat unnecessary.
3.4 Theorem IV

This theorem gives an estimate for a hypothetical solution for the equation \( a^n = b^n + c^n \). It is formulated as follows:

**Theorem 3.4.1.** The least value that \( a \) can take is \( a = \frac{5^n + 3^n + 2^n}{2} \), and the smaller value of \( b \) and \( c \) must be bigger than or equal to \( \frac{5^n - 3^n - 2^n}{2} \).

Obviously this is also an application of Theorem II, and no further proof is required. Abel simply takes the three smallest natural numbers that are pairwise relatively prime and computes the value using Theorem II. Abel then provides the reader with an example.

Let \( n = 7 \). Then \( a \geq \frac{5^7 + 3^7 + 2^7}{2} = 40092 \). Now if we assume \( n \nmid abc \) we can calculate the values of \( b \) and \( c \) using Theorem II:

\[
\begin{align*}
    b &\geq \frac{5^7 + 3^7 - 2^7}{2} = 40092 \\
    c &\geq \frac{5^7 - 3^7 + 2^7}{2} = 38033
\end{align*}
\]

But one can with a calculator (or do as Abel and calculate by hand) easily see that

\[
40092^7 + 38033^7 = 2.816 \cdot 10^{32} \neq 1.705 \cdot 10^{32} = 40220^7
\]

Even though this is not a proof of Fermat’s Last Theorem, it gives an estimate on a solution set, given the exponent \( n \). We see that the smallest possible value for \( a \) when \( n = 7 \) will not provide a solution set to \( a^n = b^n + c^n \). So one might try the next triple of natural numbers which are pairwise relatively prime.

\[
\begin{align*}
    a &\geq \frac{5^7 + 4^7 + 3^7}{2} = 48348 \\
    b &\geq \frac{5^7 + 4^7 - 3^7}{2} = 46161 \\
    c &\geq \frac{5^7 - 4^7 + 3^7}{2} = 31964
\end{align*}
\]

Which gives

\[
46161^7 + 31964^7 = 4.807 \cdot 10^{32} \neq 6.175 \cdot 10^{32} = 48348^7
\]

Again this does not provide a solution set. So taking the next possible values for \( a, b, c \):
Of course one can continue this way forever, only obtaining a larger and larger lower limits for the value of $a$, but never proving Fermat’s Last Theorem in general. It does however provide us with a good estimate. Also observe that if we are in the case $n|abc$, then from Theorem III the value of $a$ will still be greater than these values we calculated here.

We may also observe, that both Abel and Germain investigated limits of the hypothetical solutions to Fermat’s equation, and what they both found was that a solution must be very large. Remember that even though Germain’s proof of proposition 2.3.1 contained a mistake, parts of the proof are complete. From Germain we get that if $n$ divides $a$, then $b + c$ is divisible by $n^{2n-1}$. So to compare with Abel’s estimate, let us consider the case $n = 7$. Then $b + c$ would be divisible by $7^{13} = 9689010407$. Whereas using Abel’s results we get that $b + c \geq 2430483 + 2352486 = 4782969$. Germain’s estimate did however rest on the assumption of an auxiliary prime satisfying the two conditions of her theorem.

\[
\begin{align*}
a &\geq \frac{9^7 + 5^7 + 2^7}{2} = 2430611 \\
b &\geq \frac{9^7 + 5^7 - 2^7}{2} = 2430483 \\
c &\geq \frac{9^7 - 5^7 + 2^7}{2} = 2352486
\end{align*}
\]
Chapter 4

Other approaches to Abel’s Theorem I

In this chapter we will present some of the attempts to prove Abel’s Theorem I that have been done after Abel’s death. We will only consider six of the nine cases of Theorem I. Therefore we will refer to the following proposition as Abel’s Conjecture.

Proposition 4.0.1 (Abel’s Conjecture). Let $a, b, c$ be positive integers, and let $n$ be an odd prime. Then the equation $a^n = b^n + c^n$ has no solutions if either of $a, b, c$ is a power of a prime.

It may seem strange to call this a conjecture, especially when we have excluded the three cases which we in the previous chapter were not able to prove. The reason for calling it a conjecture is simply because it is what Ribenboim calls it in [Rib08], and we have chosen to follow his example.

We will look at three different approaches. The two first ones gives alternative proofs of the case where $c$ is a power of a prime, assuming that $n \nmid abc$. The first and the last approach goes a little beyond what was available theory for Abel, but can still give a fruitful insight into the problem.

4.1 Inkeri’s approach

In this section we follow the work of Inkeri from [Ink46]. Some places we have included more details in the proofs to make it clearer, and some of Inkeri’s work has already been presented in chapter 3. Where we have used other sources then the one mentioned above, we have specified it in the text.

Inkeri made progress on Abel’s Conjecture in both case I and case II. First we will give his proof of Abel’s Conjecture in case I. We will also give Inkeri’s proof showing that there can only be finitely many solutions to Fermat’s equation, when $a, b$ or $c$ is a power of a prime.
Inkeri’s proof relies on Furtwängler’s first theorem. In [Rib79, p.169] it is stated as follows:

**Theorem 4.1.1** (Furtwängler’s first theorem). Let \( n \) be an odd prime, and let \( a, b, c \) be pairwise relatively prime integers such that \( a^n + b^n + c^n = 0 \) and \( n \nmid c \). If \( r \) is a natural number such that \( r \mid c \), then we have that \( r^{n-1} \equiv 1 \pmod{n^2} \).

The statement sounds simple enough, but as the proof relies on class field theory, we will not go through it here. Furtwängler proved this theorem in 1912, so it seems highly unlikely that Abel had any knowledge about this result.

We will also need a few lemmas.

**Lemma 4.1.2.** Let \( a, b, c \) be pairwise relatively prime integers such that \( a^n = b^n + c^n \), and such that \( n \) does not divide \( abc \). Let \( t, r, s \) be numbers as defined in theorem 3.1.1 case I. Then \( t < r + s \).

**Proof.** We know that \( b + c = t^n \), \( a - c = r^n \) and \( a - b = s^n \). Using this we get that

\[
2a = t^n + r^n + s^n \quad 2b = t^n + r^n - s^n \quad 2c = t^n - r^n + s^n
\]

which, since \( a^n = b^n + c^n \), gives that

\[
(t^n + r^n + s^n)^n = (t^n + r^n - s^n)^n + (t^n - r^n + s^n)^n \quad (4.1)
\]

Now we define the numbers \( u = \frac{t}{r} \) and \( v = \frac{s}{r} \). These are positive real numbers. We assume for contradiction that \( t \geq r + s \). Then \( u + v \leq 1 \) so by lemma 3.2.5 we have that \((1 + u^n + v^n)^n < (1 - u^n + v^n)^n + (1 + u^n - v^n)^n\).

But by dividing equation (4.1) by \( r^n \) we get \((1 + u^n + v^n)^n = (1 - u^n + v^n)^n + (1 + u^n - v^n)^n\) which is impossible. Hence \( t < r + s \). \( \blacksquare \)

The following lemma is quite elementary, but useful.

**Lemma 4.1.3.** If \( q \) is a prime number, and \( u, v \) are integers such that \( u^{l-1} + v^{l-1} \neq 0 \) and \( u^l + v^l \equiv 0 \pmod{q} \) for some positive integer \( l \), then \( q \equiv 1 \pmod{l^n} \).

**Proof.** [Ink46, p.27] \( \blacksquare \)

The last lemma we will need is actually due to Sophie Germain. Inkeri just briefly refers to this result, so the proof follows the work of Ribenboim in [Rib79, p.58].

**Lemma 4.1.4.** Let \( a, b, c \) be pairwise relatively prime integers such that \( a^n = b^n + c^n \) for some odd prime \( n \), and assume \( n \nmid abc \). Let \( t, s, r, \alpha, \beta, \gamma \) be as defined in theorem 3.1.1 case 1. Then \( \alpha \equiv 1 \pmod{n^2} \), \( \beta \equiv 1 \pmod{n^2} \), and \( \gamma \equiv 1 \pmod{n^2} \).
4.1. INKERI’S APPROACH

Proof. We prove that $\gamma \equiv 1 \pmod{n^2}$. A similar argument works for $\alpha$ and $\beta$.

Let $q$ be a prime dividing $\gamma$. We show that $q \equiv 1 \pmod{n^2}$. The fact that $q$ divides $\gamma$ implies that $q$ divides $c$ which again implies that $q$ does not divide $ab$. Since $s, \gamma$ are relatively prime, we also have that $q$ does not divide $a - b$.

That $q|c$ implies that

$$\beta^n = \phi(a, c) \equiv a^{n-1} \pmod{q} \quad\alpha^n = \phi(b, -c) \equiv b^{n-1} \pmod{q}$$

hence

$$0 \equiv c^n = a^n - b^n \equiv a^{\beta^n} - b^{\alpha^n} \pmod{q}$$

which implies that

$$a^{\beta^n} \equiv b^{\alpha^n} \pmod{q} \quad (4.2)$$

Since $q$ divides $\gamma$, it also divides $a^n - b^n$ since $\gamma^n = \phi(a, b) = \frac{a^n - b^n}{a - b}$. So we have $a^n + (-b)^n \equiv 0 \pmod{q}$ and $a^n + (-b)^n = a - b \equiv 0 \pmod{q}$. Hence by lemma 4.1.3 we must have $q \equiv 1 \pmod{n}$. So there exist some integer $m$ such that $q = mn + 1$, and we see easily that $\frac{q-1}{n} \in \mathbb{Z}$.

Since $a^{\beta^n} \equiv b^{\alpha^n} \pmod{q}$ we get the following:

$$a^{\frac{q-1}{n}} b^{s-1} \equiv b^{\frac{q-1}{n}} a^{s-1} \pmod{q}$$

which by Fermat’s Little Theorem implies that

$$a^{\frac{q-1}{n}} \equiv b^{\frac{q-1}{n}} \pmod{q}$$

Because $q \nmid b$ there exists a number $b'$ such that $bb' \equiv 1 \pmod{q}$. Since $a^n - b^n \equiv 0 \pmod{q}$ it follows that

$$(ab')^n \equiv (bb')^n \equiv 1 \pmod{q}$$

But we also have that

$$(ab')^{\frac{q-1}{n}} \equiv (bb')^{\frac{q-1}{n}} \equiv 1 \pmod{q}$$

Hence $n$ has to divide $\frac{q-1}{n}$, which implies that $q \equiv 1 \pmod{n^2}$.  \[\blacksquare\]

We are now ready for the main results from [ink46, section III]. The first two theorems consider case I of Fermat’s Last Theorem. From Abel’s Theorem II we know that if $n \nmid abc$, there exist numbers $t, r, s, \alpha, \beta, \gamma$ such that

$$b + c = t^n \quad a - c = r^n \quad a - b = s^n \quad (4.3)$$

$$\phi(b, -c) = \alpha^n \quad \phi(a, c) = \beta^n \quad \phi(a, b) = \gamma^n \quad (4.4)$$

With this in mind we state the first theorem.
**Theorem 4.1.5.** Let $a, b, c$ be positive integers that are pairwise relatively prime and such that $a^n = b^n + c^n$ for some odd prime $n$. Assume that $n$ does not divide $abc$, and let $t, r, s, \alpha, \beta, \gamma$ be the integers as described above. Then all numbers $t, s, r$ contains a prime factor on the form $2mn^2 + 1$ for some integer $m$.

**Proof.** We split the proof into several steps to make the overall structure easier to follow.

**Prime factor of $t$:** First observe that

$$s^n + r^n = (a - b) + (a - c) = 2a - (b + c) = 2t\alpha - t^n \equiv 0 \mod t$$

From lemma 4.1.2 we know that $t < s + r$ and $s < r < t$. This gives $t < s + r < 2t$ which implies $s + r \not\equiv 0 \mod t$. Now let $q$ be a prime factor of $t$. Then obviously $s^n + r^n \equiv 0 \mod q$. We want to show that $s + r \not\equiv 0 \mod q$.

Suppose that $q$ is a factor in $s + r$. Then $r \equiv -s \mod q$ and hence $\phi(r, -s) \equiv nr^{n-1} \mod q$. If $r \equiv 0 \mod q$ it would imply that also $s \equiv 0 \mod q$, which is impossible since $r, s$ are relatively prime. So we must have $n = q$. But then $n$ will divide $a$ since $a = t\alpha$. This contradicts our assumption that $n \not| abc$. Hence it is impossible that $q$ divides $r + s$.

So we have $s^n + r^n \equiv 0$ and $s + r \not\equiv 0 \mod q$. Then by lemma 4.1.3 we have $q \equiv 1 \mod n$.

**Prime factors of $r$ and $s$:** Similarly as the previous case, we consider $s$ and $t$.

$$t^n - s^n = (b + c) - (a - b) = 2b + (a - c) = 2r\beta + r^n \equiv 0 \mod r$$

Again, using lemma 4.1.2 we get that $t - s < r$ which implies that $t - s \not\equiv 0 \mod r$. Let $q$ be a prime factor of $r$ and use the exact same argument as the previous case to show that $q \equiv 1 \mod n$. Of course, the same argument also applies to $s$.

**Conclusion** So we can conclude that each number $t, r, s$ contains a prime factor on the form $q = 2mn + 1$. Then by theorem 4.1.1 we get that $q^n \equiv q \mod n^2$. It is also easy to see that $q^n = (2mn + 1)^n \equiv 1 \mod n^2$ and combining these, we get the desired result. ■
The next theorem proves that Abel’s Conjecture is true in case 1.

**Theorem 4.1.6.** Let $a, b, c$ be pairwise relatively prime positive integers where $a^n = b^n + c^n$ and such that $n$ does not divide $abc$. Then each of the numbers $a, b, c$ contains at least two distinct prime factors on the form $2mn^2 + 1$.

**Proof.** Using Abel’s Theorem II again, we can write $a, b, c$ in terms of $t, r, s, \alpha, \beta, \gamma$ the usual way. From theorem 4.1.5 we know that each of $t, r, s$ contains a prime factor of the form $2mn^2 + 1$, and from lemma 4.1.4 we know that $\alpha, \beta, \gamma$ also contains a prime factor of the same form. But each pair $(t, \alpha)$, $(r, \beta)$ and $(s, \gamma)$ is relatively prime, so the prime factors have to be distinct. Hence neither $a, b$ or $c$ can be a power of a prime. ■

What we have done in this section so far, is to show that if $n$ does not divide $abc$, then Abel’s Conjecture holds true. To get to this result, we had to rely on Fürtwangler’s second theorem, which requires non-elementary methods. But as we have already seen in the previous chapter, it is possible to prove the same statement in case I, using only elementary methods.

We will now turn our focus away from case I, and consider the general case of Abel’s conjecture. The proofs of the two following theorems can both be done using elementary methods for case I, but requires non-elementary methods for case II. Even though we are mainly interested in case II of these theorems, we will also include the proof of case I. It is our opinion that it is a good example of what is possible when only using elementary methods.

We will first prove a theorem saying there can be at most finitely many solutions of the equation $a^n = b^n + c^n$ under certain restrictions, and then we will use this to show that the same hold when $a, b$ or $c$ are prime powers.

**Theorem 4.1.7.** There is at most finitely many positive integer solutions to the equation $a^n = b^n + c^n$ such that $a, b, c$ are pairwise relatively prime, and such that at least one of all possible differences between the three integers are less then some upper limit $M$.

**Proof.** First we will look at case I.

**Preliminaries** Without loss of generality we can assume $c < b$. Then $a - b < a - c$. If $a - c < M$, then also $a - b < M$. Hence it will be sufficient to show that the theorem holds if one of the two holds: $b - c < M$ or $a - b < M$.

**The case where $b - c < M$:** Assuming case I we know there exist integers $r, s$ such that $a - c = r^n$ and $a - b = s^n$. Then $r^n - s^n = b - c < M$. From lemma 3.2.3 we know that $s < r$, and therefore we can observe that $r^n - s^n = (r - s)\varphi(r, s) > r^{n-1}$. Hence $r^{n-1} < M$ which implies that $r < M^{1/n}$ and further that $a - c = r^n < M^{n^{1-1}}$. 

We observe that since $c < b$, we have that $c^n + c^n < b^n + c^n = a^n$. Hence $2c^n < a^n$ which implies that $\sqrt[2]{2}c < a$. So $\sqrt[2]{2}c - c < a - c < M \frac{a^n}{\sqrt[2]{2} - 1}$ which implies that $c < \frac{M a^n}{\sqrt[2]{2} - 1}$.

So we have

$$a = (a - c) + c < M \frac{a^n}{\sqrt[2]{2} - 1} + \frac{M a^n}{\sqrt[2]{2} - 1} = \frac{\sqrt[2]{2} M a^n}{\sqrt[2]{2} - 1}$$

which completes the proof in this case.

The case where $a - b < M$: Still assuming case I, we know there exists integers $t, s, r, \beta$ such that $b + c = t^n$, $a - c = r^n$, $a - b = s^n$ and $b = r\beta$. Then

$$s^n - t^n = (a - b) - (b + c) = (a - c) - 2b = r^n - 2r\beta \equiv 0 \pmod{r}$$

So we have

$$s^n \equiv t^n \pmod{r}$$

Obviously $t \equiv t - r \pmod{r}$ so

$$s^n \equiv (t - r)^n \pmod{r} \quad (4.5)$$

Since $t - r < s$ (Lemma 4.1.2), we have that

$$s^n - (t - r)^n < s^n = a - b < M$$

From (4.5) we know that $s^n = mr + (t - r)^n$ for some integer $m$. Hence $mr = s^n - (t - r)^n < M$ which implies $r < \frac{M}{m}$ and further that

$$a - c = r^n < \left( \frac{M}{m} \right)^n < M^n$$

By a similar argument as the previous case, using that $\sqrt[2]{2}c < a$ we get $c < \frac{M a^n}{\sqrt[2]{2} - 1}$ which again gives

$$a = (a - c) + c < M^n + \frac{M a^n}{\sqrt[2]{2} - 1} = \frac{\sqrt[2]{2} M a^n}{\sqrt[2]{2} - 1}$$

The general case using Siegel’s Theorem: We now give a proof of theorem 4.1.7 in general, so we make no assumption about the divisibility of $abc$ and $n$. In this case we have to rely on a theorem due to Siegel\footnote{The proof of Siegel’s Theorem relies on a result due to the Norwegian mathematician Axel Thue (1863-1922). Thue made great and innovative contributions to the field of diophantine approximation. Inspired by Thue’s work, Roth improved one of his results, and today we know this particular result as the Thue-Siegel-Roth-Theorem.} which in [Rib79] is formulated as follows.
4.1. INKERI’S APPROACH

**Proposition 4.1.1** (Siegel). If the curve defined by \( f(x,y) = 0 \) has genus greater than 0, then there exists at most finitely many integer solutions to the equation \( f(x,y) = 0 \).

We prove the case where \( a - b < M \). The other cases are similar. There exists a positive integer \( k \) such that \( a = b + k \). Then we can set \( f(b,c) = b^n + c^n - (b + k)^n \). We want to show that the curve defined by \( f(b,c) = 0 \) has positive genus. We do that by homogenizing the equation so each term is of the same degree. With the variable \( t \) we define

\[
 u = b \quad v = c \quad w = b + kt
\]

We consider the curve defined by \( F(u,v,w) = u^n + v^n + w^n = 0 \). This curve is called the Fermat curve. We see that the first order partial derivatives of \( F \) are all zero only in the point \((0,0,0)\). This point is not on our curve. Hence the curve is nonsingular. Thus the genus of this curve is given by

\[
 g = \frac{(n-1)(n-2)}{2}
\]

so we easily calculate that the genus of \( F(u,v,w) \) is positive. Hence by Siegel’s theorem the equation has finitely many integer solutions. ■

Now we are ready for the last of Inkeri’s theorems.

**Theorem 4.1.8.** Let \( n \) be an odd prime. Then there are at most finitely many solutions to the equation \( a^n = b^n + c^n \) when either of the numbers \( a, b, c \) is a prime power.

**Proof.** We assume that \( c < b < a \). If \( n \) does not divide \( abc \) we know from theorem 4.1.6 that neither of \( a, b, c \) can be prime powers. So we must have that \( n | abc \). Remember from lemma 3.2.3 that \( \phi(b,-c) < \phi(a,c) < \phi(a,b) \). We have also proven in chapter 3 that neither \( a \) nor \( b \) can be prime powers, so we may assume that \( c \) is.

Suppose that \( n | c \). From Theorem II we know that \( c = n^{\alpha} s^n \gamma^n \) and \( \phi(a,b) = n\gamma^n \). Using lemma 3.2.4 we get that

\[
 n < c < \phi(b,-c) < \phi(a,b) = n\gamma^n
\]

Which obviously implies that \( 1 < \gamma \). Hence \( c \) cannot be a prime or a power of a prime as \( n \) and \( \gamma \) are relatively prime integers.

Suppose \( n | a \). Then from Abels Theorem II we know that \( \phi(b,-c) = n\alpha^n \), \( \phi(a,c) = \beta^n \) and \( \phi(a,b) = \gamma^n \). So we have

\[
 n < c < \phi(b,-c) = n\alpha^n < \beta^n < \gamma^n < n\gamma^n
\]

which implies that \( 1 < \gamma \).

Similarly, if \( n | b \) then \( \phi(b,-c) = \alpha^n \), \( \phi(a,c) = n\beta^n \) and \( \phi(a,b) = \gamma^n \). In this case we have

\[
 n < c < \phi(b,-c) = \alpha^n < n\beta^n < \gamma^n < n\gamma^n
\]
which implies that \(1 < \gamma\). Hence \(\gamma\) are always larger than 1, independently of which number \(a\) or \(b\) that is divisible by \(n\).

Since \(c = s\gamma\) is a prime power, we get that \(a - b = s^n = 1\). Then by theorem \([4.1.7]\) we are done.

With the work we have already done in the previous chapter, we could have made this proof significantly shorter. From the proof of proposition \([3.2.1]\) and the comments we made following this proof, we know that if \(c\) is a prime number, then we must have \(a - b = 1\). Hence we could have just applied theorem \([4.1.7]\) directly.

### 4.2 Ribenboim’s Approach

Now we will present yet another proof of Abel’s conjecture in the case where \(n\) does not divide \(abc\). In this approach we will only use elementary methods. We will follow Ribenboim’s collection of this work in [Rib08, Chp. VI.3] and [Rib79, Chp. XI.4]. What we discovered when trying to prove Abel’s conjecture using methods similar to Germain, was that we had to assume \(a - b \neq 1\) to make it work. This approach have the advantage that such an assumption is not necessary, but we will still use only elementary methods.

We will need several lemmas to arrive at the desired conclusion.

**Lemma 4.2.1.** Let \(m \geq 1\) be an odd integer with \(r\) distinct prime factors, and let \(u \geq 0\). Let \(0 < c < b\) be relatively prime integers, \(\alpha = b^{2^u} + c^{2^u}\) and \(\beta = b^{2^u} - c^{2^u}\). Then:

1. \(\alpha\) and \(\beta\) has at least \(r\) distinct prime factors
2. If \(\alpha\) has exactly \(r\) distinct prime factors, then \(\alpha = 2^3 + 1^3\)
3. If \(\beta\) has exactly \(r\) distinct prime factors, then \(b = c + 1\)

*Proof.* [Rib08, Chp. VI, section 3] ■

**Lemma 4.2.2.** Let \(n \geq 3\) be a positive integer having \(r\) distinct odd prime factors. Let \(0 < c < b < a\) be pairwise relatively prime integers such that \(a^n = b^n + c^n\). Then

1. \(a\) and \(b\) have at least \(r + 1\) distinct prime factors
2. If \(c\) has exactly \(r\) distinct prime factors, then \(a = c + 1\)

*Proof.* We know that Fermat’s Last Theorem holds true when \(n\) is a multiple of 3 and a power of 2. So \(n = 2^u m\), where \(u \geq 0\) and \(m \geq 1\) is odd. By assumption, \(m\) has \(r\) distinct prime factors. It follows from lemma \([4.2.1]\) that
a^n, b^n and c^n has at least r distinct prime factors. Obviously a, b and c has exactly as many distinct prime factors as a^n, b^n and c^n respectively.

If b has exactly r distinct prime factors, we get from lemma 4.2.1 that a = c + 1. But this is impossible since c < b < a. Hence b must have at least r + 1 distinct prime factors.

If a has exactly r distinct prime factors, then \( a^n = 2^3 + 1^3 \). Hence n = 3 which is impossible. So a must have at least r + 1 distinct prime factors.

Now consider the integer c. It may very well happen that a - b = 1, so we cannot use lemma 4.2.1 to rule out the possibility that c has r distinct prime factors. But if it does we will have that a - b = 1.

Lemma 4.2.3. Let n > 2 and 0 < c < b < a be relatively prime integers such that \( a^n = b^n + c^n \). If c is a power of a prime, then a - b = 1 and n is an odd prime.

The observant reader may notice that the statement of this lemma is already proved in chapter 3. There we proved that if a - b ≠ 1, the equation has no solution. Hence we must have a - b = 1 if \( a^n = b^n + c^n \). But Ribenboim seems unaware of this fact, and provides the following proof.

Proof. Assume c = \( p^m \) for some prime number p and m > 0. Assume that n has r distinct odd prime factors. From lemma 4.2.2 we know that c will have r or more distinct prime factors. But by assumption c has only one prime factor, hence we must have r = 1. Hence c and n have exactly the same number of distinct prime factors. Then by lemma 4.2.2 we get that a - b = 1.

With these lemmas to help us, the proof of Abel’s conjecture becomes short and easy to follow:

Proposition 4.2.1. If n is an odd prime not dividing abc, and 0 < c < b < a are relatively prime integers such that \( a^n = b^n + c^n \), then c is not a prime power.

Proof. Suppose c is a prime power. Then from lemma 4.2.3 we have that a - b = 1. From theorem 3.1.1 we have that a - b = s^n, hence we must have s = 1. Using lemma 3.1.2 and lemma 3.2.3 we get that r < t < r + 1 which is a contradiction since r, s, t are integers. Hence c cannot be a prime power.

This completes a third proof of case I of Theorem I, when c is a power of a prime. Note that all three proofs are fundamentally different from the proofs for a and b, as we don’t use the factorization of a^n. Also note that lemma 4.2.3 says that if c is a prime power, then we will always have a - b = 1. That means that our proofs in the cases where c is a prime or a prime power, where we also assumed that a - b ≠ 1, is superfluous. It seems odd that Abel did not make any comment on the proof, especially since it uses different methods than the easier cases. We are tempted to believe that Abel was unaware of the fact
that \( a - b = 1 \) whenever \( c \) is a prime power, and that he thought proofs like the ones we made assuming \( a - b \neq 1 \) would be enough to prove his theorem. But of course, this is only speculations, and we will probably never find out exactly what Abel was thinking.

4.3 Cyclotomic integers

In this section we will extend the analysis of Fermat’s equation into the ring of cyclotomic integers \( \mathbb{Z}[\alpha] \), where \( \alpha \) is a primitive root of unity. The concepts of rings and ideals were not yet developed when Abel lived, but some of the techniques we will use here may still have been available to Abel. The hope is that this will shed a new light on Abel’s work on Fermat’s Last Theorem.

We will briefly describe some of the most fundamental concepts needed, but a lot of details are omitted. We follow the example of [Rib79, lecture V] for the theory, and [Was97, chp.1] for the proofs of lemmas and theorems. The aim of this section is to prove the following theorem:

**Theorem 4.3.1.** Let \( a, b, c \) be natural numbers, and let \( n \) be a regular prime such that \( n \nmid abc \). Then the equation \( a^n = b^n + c^n \) has no solutions.

We begin by describing the motivation for extending the analysis into the ring \( \mathbb{Z}[\alpha] \), before defining some of the key concepts in this ring, including the notion of a regular prime. Finally we prove some lemmas leading up to the proof of theorem [4.3.1].

When considering the equation \( a^n = b^n + c^n \) one can factorize the right hand side using the primitive \( n \)th root of unity, which we will denote \( \alpha \). That is, \( n \) is the smallest number such that \( \alpha^n = 1 \), and we also make the additional assumption that \( \alpha \neq 1 \). Then

\[
a^n = \prod_{i=0}^{n-1} (b + \alpha^i c)
\]

Following the example of Abel and Germain, one may wonder if it is possible to deduce that each factor on the right hand side is an \( n \)th power, and carry out similar arguments as in the previous chapters. To do this, we first need to define some fundamental concepts. A general element in \( \mathbb{Z}[\alpha] \) is on the form \( f(\alpha) = a_0 + a_1 \alpha + \ldots + a_{n-1} \alpha^{n-1} \), where \( a_i \in \mathbb{Z} \) for \( 0 \leq i \leq n - 1 \). Observe that in this ring we have that \( \alpha^n = 1 \), \( \alpha^{n+1} = \alpha \), \( \alpha^{n+2} = \alpha^2 \), and so on. Therefore we have the relation

\[
1 + \alpha + \ldots + \alpha^{n-1} = \alpha^n + \alpha + \ldots + \alpha^{n-1} = \alpha(1 + \alpha + \ldots + \alpha^{n-1})
\]

which implies that either \( \alpha = 1 \) or that \( 1 + \alpha + \ldots + \alpha^{n-1} = 0 \). We have assumed that \( \alpha \neq 1 \), hence the latter equality holds. Therefore we can write a general element of \( \mathbb{Z}[\alpha] \) as \( f(\alpha) = a_0 + a_1 \alpha + \ldots + a_{n-2} \alpha^{n-2} \).
We say that $u \in \mathbb{Z}[\alpha]$ is a **unit** if there exist another element $v \in \mathbb{Z}[\alpha]$ such that $uv = 1$. Examples of units in $\mathbb{Z}[\alpha]$ are $1, -1, \alpha, \alpha^{-1}$ and many more. We can also make sense of the notion of divisibility in this ring. If $f(\alpha), g(\alpha) \in \mathbb{Z}[\alpha]$ and there exist an element $h(\alpha) \in \mathbb{Z}[\alpha]$ such that $h(\alpha)f(\alpha) = g(\alpha)$, then we say that $f(\alpha)$ divides $g(\alpha)$, or that $g(\alpha)$ is divisible by $f(\alpha)$. Two elements $f(\alpha), g(\alpha) \in \mathbb{Z}[\alpha]$ are **associated** if $\frac{f(\alpha)}{g(\alpha)}$ is a unit. We call the elements in $\mathbb{Z} \subset \mathbb{Z}[\alpha]$ **rational integers**.

If we were to argue like Germain and Abel with the extended factorization of $a^n$ into the ring $\mathbb{Z}[\alpha]$, we would need unique factorization to hold. However, Kummer showed around the year 1850, that this property turns out to depend on the value of $n$, and that one cannot say in general that unique factorization holds. What is possible, is to show that $\mathbb{Z}[\alpha]$ is the ring of integers of the algebraic number field $\mathbb{Q}(\alpha)$, and thus that the ideals of $\mathbb{Z}[\alpha]$ has unique factorization as a product of prime ideals. So it seems beneficial to consider eq. (4.16) as an equality of ideals:

$$\langle a^n \rangle = \prod_{i=0}^{n-1} \langle b + \alpha^i c \rangle$$

We extend the notion of divisibility to ideals in the obvious way: If $I_1$, $I_2$ and $I_3$ are ideals such that $I_1 = I_2I_3$, then we say that $I_2$ divides $I_1$. Let $f(\alpha), g(\alpha) \in \mathbb{Z}[\alpha]$. Then we say that $f(\alpha) \equiv g(\alpha) \pmod{I_1}$ if $f(\alpha) - g(\alpha) \in I_1$. One may show that the principal ideal $\langle 1 - \alpha \rangle$ in $\mathbb{Z}[\alpha]$ is a prime ideal, and that $\langle n \rangle = \langle 1 - \alpha \rangle^{n-1}$, see for example the first pages of [Was97] for a proof. It is also possible to prove that the only rational integers in $\langle 1 - \alpha \rangle$ are the integer multiples of $n$.

The last thing we need before embarking on the task of proving the theorem, is the notion of a regular prime. The precise definition is that the prime $p$ is regular if it does not divide the class number of $\mathbb{Q}(\alpha_p)$, where $\alpha_p$ is a primitive $p$th root of unity. Computing the class number of an algebraic number field is usually a very difficult task, and we will not go into the theory required to do that. Instead we will think of a regular prime $p$ as a prime with the following property: a prime $p$ is regular if the $p$th power of a non-principal ideal in $\mathbb{Z}[\alpha]$ is never a principal ideal. This property is equivalent to the definition of a regular prime ([Rib79, p.86]), and it is this property that will be important.

**Lemma 4.3.2.** Let $u$ be a unit in the ring $\mathbb{Z}[\alpha]$. Then there exist an element $\epsilon_1 \in \mathbb{Q}(\alpha + \alpha^{-1})$ and $r \in \mathbb{Z}$ such that $u = \alpha^r \epsilon_1$.

**Proof.** See [Was97] p.3-4

**Lemma 4.3.3.** Let $f(\alpha) \in \mathbb{Z}[\alpha]$. Then $f(\alpha)^n$ is congruent to a rational integer modulo $n$. 
Proof. We can write
\[ f(\alpha) = b_0 + b_1 \alpha + \ldots + b_{n-2} \alpha^{n-2} \]
where all the \( b_i \)'s are integers. Then
\[ f(\alpha)^n \equiv b_0^n + (b_1 \alpha)^n + \ldots + (b_{n-2} \alpha^{n-2})^n \equiv b_0^n + b_1^n + \ldots + b_{n-2}^n \pmod{n} \]

Lemma 4.3.4. Let \( f(\alpha) = a_0 + a_1 \alpha + \ldots + a_{n-1} \alpha^{n-1} \). Suppose that \( a_i \in \mathbb{Z} \) and \( a_i = 0 \) for at least one value of \( i \). Then \( m|f(\alpha) \) for some integer \( m \) implies that \( m|a_j \) for all \( j = 0, 1, \ldots, n-1 \).

Proof. We know that \( 1 + \alpha + \ldots + \alpha^{n-1} = 0 \). Consider \( \mathbb{Z} \) as a \( \mathbb{Z} \)-module. Any subset of \( \{1, \alpha, \ldots, \alpha^{n-1}\} \) consisting of \( n-2 \) elements will be a basis for the \( \mathbb{Z} \)-module. By assumption \( a_i = 0 \) for at least one value of \( i \). Hence the other \( a_j \)'s give the coefficients with respect to the basis, hence we are done.

We are now ready to prove theorem 4.3.1.

Proof. We have that
\[ a^n = \prod_{i=0}^{n-1} (b + \alpha^i c), \]
and considering this as an equality of ideals we get
\[ \langle a^n \rangle = \prod_{i=0}^{n-1} \langle b + \alpha^i c \rangle. \]

Coprime ideals: We first prove that the ideals \( \langle b + \alpha^i c \rangle \) are coprime. Suppose that \( p \) is a prime ideal dividing both \( \langle b + \alpha^i c \rangle \) and \( \langle b + \alpha^j c \rangle \) where \( 0 \leq j < i \leq p-1 \). Then we have that
\[ b + \alpha^i c \in p \tag{4.7} \]
\[ b + \alpha^j c \in p \tag{4.8} \]
hence the difference
\[ c(\alpha^i - \alpha^j) = c\alpha^i (1 - \alpha^{i-j}) \in p \]
\( \alpha^j \) is a unit in the ring of cyclotomic integers, so it cannot be an element of \( p \). Also observe that \( 1 - \alpha^{i-j} = \alpha \alpha^{i-j} = (1 - \alpha)(1 + \alpha + \ldots + \alpha^{i-j-1}) \). Hence \( c(1 - \alpha) \in p \), so either \( c \) or \( 1 - \alpha \) has to be an element in \( p \).

Similarly, we observe that the difference
\[ \alpha^i (b + \alpha^i c) - \alpha^i (b + \alpha^j c) \in p \]
This implies that \( \alpha^i b(1 - \alpha^{i-j}) \in p \), hence either \( b \) or \( 1 - \alpha \) is an element of \( p \). If both \( b \) and \( c \) are elements of \( p \), then \( b + c \in p \) which is impossible since \( b, c \) are coprime. So we conclude that \( 1 - \alpha \in p \), and since the ideal generated by \( 1 - \alpha \) is prime, we have \( p = \langle 1 - \alpha \rangle \).
Observe that \( b + c \equiv b + \alpha^i c \pmod{p} \). This is because \( 1 - \alpha^i = (1 - \alpha)(1 + \alpha + \ldots + \alpha^{i-1}) \), hence \( (1 - \alpha^i)c \equiv 0 \pmod{p} \). Using this and our initial assumption we have

\[
b + c \equiv b + \alpha^i c \equiv 0 \pmod{p}
\]

Since \( b + c \in \mathbb{Z} \), we must have \( b + c \equiv 0 \pmod{n} \). But then \( a^n = b^n + c^n \equiv b + c \equiv 0 \pmod{n} \), which is a contradiction.

**Deriving equation:** So since the ideals \( (b + \alpha^i c) \) are pairwise coprime, they must all be the \( n \)th power of an ideal. That is, for all \( i \) we have

\[
(b + \alpha^i c) = a_i^n
\]

for some ideal \( a_i \in \mathbb{Z}[\alpha] \). Since \( n \) is a regular prime, we can conclude that the ideal \( a_i \) is a principal ideal. So for all \( i \), there exist an element \( \delta_i \in \mathbb{Z}[\alpha] \) such that \( a_i = \langle \delta_i \rangle \). In particular we have that

\[
(b + ac) = \langle \delta^n \rangle
\]

for some \( \delta \in \mathbb{Z}[\alpha] \). Hence

\[
b + ac = u\delta^n
\]

where \( u \) is a unit in \( \mathbb{Z}[\alpha] \). From lemma 4.3.2 we get that \( u = \alpha^r \epsilon_1 \), where \( r \in \mathbb{Z} \) and \( \epsilon_1 \in \mathbb{Q}(\alpha + \alpha^{-1}) \). From lemma 4.3.3 there exist an integer \( k \) such that \( \delta^n \equiv k \pmod{n} \). Combining this yields

\[
b + ac \equiv \alpha^r \epsilon_1 k \pmod{n}
\]

First multiplying with \( \alpha^{-r} \), and then taking complex conjugates, gives us the two equations:

\[
\alpha^{-r}(b + ac) \equiv \epsilon_1 k \pmod{n} \quad (4.9)
\]
\[
\alpha^r (b + a^{-1}c) \equiv \epsilon_1 k \pmod{n} \quad (4.10)
\]

Now we subtract one equation from the other:

\[
\alpha^{-r}b + \alpha^{1-r}c - \alpha^r b - \alpha^{r-1}c \equiv 0 \pmod{n}
\]

Finally we multiply by \( \alpha^r \), which gives us the equation:

\[
b + ac - \alpha^{2r}b - \alpha^{2r-1}c \equiv 0 \pmod{n} \quad (4.11)
\]

We know that \( n \neq 3 \). If \( 1, \alpha, \alpha^{2r} \) and \( \alpha^{2r-1} \) are all distinct, then by lemma 4.3.4 we would have that \( n \) divides \( b \) and \( c \). This is impossible since \( b \) and \( c \) are assumed to be relatively prime. Observe that \( 1 \neq \alpha \) and \( \alpha^{2r} \neq \alpha^{2r-1} \). So we are left to check the three remaining cases.
CHAPTER 4. OTHER APPROACHES TO ABEL’S THEOREM I

Case 1: Suppose $1 = \alpha^2 + \alpha r$. Then eq. (4.11) gives $\alpha c - \alpha^2 r - 1 c \equiv 0 \pmod{n}$ which again implies that

$$\alpha c - \alpha^{n-1} c \equiv 0 \pmod{n}$$

Hence by lemma 4.3.4 we see that $n$ divides $c$, which is impossible.

Case 2: Suppose that $\alpha = \alpha^2 r - 1$, i.e. that $\alpha = \alpha^2 r$. Then eq. (4.11) gives

$$b - \alpha^2 b \equiv 0 \pmod{n}$$

By lemma 4.3.4 we must have $n|b$, which is impossible.

Case 3: Finally we consider the case $1 = \alpha^{2r-1}$. Then

$$b + \alpha c - \alpha b - c \equiv 0 \pmod{n}$$

which further gives

$$(b - c) - \alpha (b - c) \equiv 0 \pmod{c}$$

Using lemma 4.3.4 again, we conclude that $n$ must divide $b - c$.

Conclusion: Now, rewriting the initial equation to

$$-b^n = c^n - a^n$$

and going through the proof in a similar way, we will get that $n$ also divides $c + a$. Hence $b \equiv c \equiv -a \pmod{n}$ which implies that $3a \equiv 0 \pmod{n}$. Since $n$ is assumed not to divide $a$ we are forced to conclude that $n = 3$, which is impossible. ■

As mentioned before, the concepts of rings and ideals were not yet developed when Abel lived, so the proof of theorem 4.3.1 are probably beyond the reach of Abel. However, he may have used the factorization using the roots of unity. This method was first described by Gauss in his Disquisitiones Arithmeticae, that was published in 1801, and there is no reason to believe that Abel was not familiar with this. Suppose that Abel used the factorization

$$a^n = \prod_{i=0}^{n-1} (b + \alpha^i c)$$

and suppose that he had some notion of divisibility and unique factorization. Then each factor would be an $n$th power, but of what? Would he be able to deduce somehow, that $n|b - c$?

These remarks may seem like a bit of a far stretch, even for a genius like Abel. But when the elementary methods did not provide us with a proof
of Theorem I, the hope of opening the door into speculation is that it may provide new insight and even new ideas on how to solve it. If Abel could somehow prove that \( n \) divides \( b - c \), the following could perhaps resemble his argument?

**Proposition 4.3.1.** Let \( n \) be a regular prime, and let \( a, b, c \) be positive integers. Suppose that \( b - c \) is a prime number. If \( n \nmid abc \), then the equation \( a^n = b^n + c^n \) has no solutions.

**Proof.** We suppose that there is a solution \( a^n = b^n + c^n \). Since \( n \) is regular we know from the proof of theorem 4.3.1 that \( b - c \equiv 0 \pmod{n} \). From proposition 3.2.4 we know that \( r - s = 1 \), where \( r, s \) are integers as described in Abel’s Theorem II, case 1. Then

\[
\begin{align*}
    b - c &= r^n - s^n \\
    &= (s + 1)^n - s^n \\
    &= \binom{n}{1} s^{n-1} + \binom{n}{2} s^{n-2} + \ldots + \binom{n}{n-1} s + 1 \\
    &\equiv 1 \pmod{n}
\end{align*}
\]

Hence we have a contradiction. ■
Chapter 5

Historical note

In this chapter we give a brief overview of the lives of Niels Henrik Abel and Sophie Germain. As references, we have used [BD12] and [Stu96].

5.1 Niels Henrik Abel

Niels Henrik Abel was born in the southern parts of Norway in the year of 1802. In 1815, when Abel was 13 year old, he was sent to Christiana to attend the Cathedral School. In his first couple of years at this school, there are no records showing that Abel made any special impression, neither good or bad. But in 1818 Abel got a new teacher in mathematics, a man with the name Bent M. Holmboe. Holmboe was a talented mathematician himself, and he soon realised the potential Abel had. He gave Abel books and problems to solve, and he introduced Abel to mathematics way beyond the curriculum. Holmboe would later become a good friend of Abel.

At the end of Abel’s time on the Cathedral School it was clear that he had to go to the university to continue his study and develop his talent. But as his family was not able to support him financially, Abel relied on the support of several university teachers to attend the University of Christiania. It soon became clear that Abel knew more mathematics than any other person in Norway, in which he had to go abroad to continue his studies. In 1823 Søren Rasmussen, a professor in mathematics, gave Abel money to travel to Copenhagen for a few months. The hope was that he could get access to more books at the libraries there, and that he could meet other mathematicians. It was during his stay here that Abel wrote the letter to Holmboe with the four

\[ \sqrt[3]{6064321219}, \text{ include the decimals.} \]

\footnote{Abel dates this particular letter by writing: \textit{year} $\sqrt[3]{6064321219}$, \textit{include the decimals}.}
theorems we have studied in this thesis. It was also here Abel met his future fiancée.

In 1825, Abel was still a student in Norway, and eventually got a grant to travel abroad. The goal was to get to Paris, and make contacts in the mathematical circles including both Legendre and Cauchy. Abel made several stops on his way. In Berlin he met the scientist Geheimrat August Leopold Crelle, and through him he also got the opportunity to meet other peers in the scientific community. Soon after he met Abel, Crelle founded a German mathematical journal, known as Crelle’s Journal. It was in this journal Abel would later publish several articles.

Abel eventually reached Paris, where he worked on his most pioneering mathematical theories. He submitted a paper to the French Academy of Sciences, but it was forgotten and never reviewed before after Abel’s death. In 1827, Abel left Paris, feeling sad and tired. He already had tuberculosis. His stay abroad had been judged a failure, and he was not granted additional funding for his research. He returned to Norway, and was forced to take up a loan to cover his living expenses. He did however get some work at the university in Christiania, but a permanent position seemed out of reach. His submission to the French Academy also seemed to be forever forgotten. Over the next year and a half, Abel’s health got worse, but he still managed to produce many papers that were published in Crelle’s Journal. He traveled home to his fiancée in Froland for Christmas in the year of 1828, but on the way he got very ill. Three months later Abel died, without knowing that not only had Crelle managed to get him a job in Berlin, but the French Academy had also discovered his submitted paper. Words about the talented Norwegian mathematician had started to spread.

Nevertheless, Abel’s contributions to mathematics is impressive for a person who only reached the age of 26. His work has inspired mathematicians for hundreds of years, and even today there are made discoveries that can be connected to his mathematical contributions. The paper he submitted to the French Academy of Science has later become known as the Paris-thesis, and was finally published in 1841, 12 years after Abel’s death.

5.2 Sophie Germain

Sophie Germain was born in 1776 in Paris. She grew up during the French Revolution which undoubtedly affected her upbringing. One day when she was 13 years old, she found her way into her fathers library in an attempt to escape her parents’ conversations about politics. She found a book about Archimedes and his passion for mathematics. The legend is that Archimedes was so consumed by his work that he forgot not just to eat and drink, but he

If we calculate this, we get 1823.59, and we reach 59% of a year around the 3rd og 4th og August
also failed to answer questions from a Roman soldier and was consequently speared to death. Germain thought that if someone could get so consumed by mathematics, it was a field worth studying, and so she began reading mathematics on her own.

In 1794 the university École Polytechnique was established in Paris. As a woman, Germain was not allowed to enrol as a student, but under a male pseudonym she was able to obtain lecture notes and weekly problem sets. Lagrange's lectures in analysis caught her interest in particular, and she submitted her attempted solutions to him every week - always under her male pseudonym. The name she chose to use was one of a former student, Monsieur LeBlanc. It is not for certain how Lagrange found out that LeBlanc was in fact Germain in disguise, but when he did, he continued to mentor Germain and giving her moral support in her mathematical studies.

In 1789 Legendre's Théorie des Nombres was published, and in 1801 followed Gauss' Disquisitiones Arithmeticae. Germain read them both and opened correspondence with both Legendre as well as with Gauss. Still worrying that a woman might not be taken seriously, she signed every letter as LeBlanc. Gauss answered Germain's initial letter complimenting one of her proofs, and giving comments on her work. Inspired by this, Germain sent more letters, which Gauss did not always answer.

Nevertheless, it seems like Gauss was an important mentor to Germain. In 1806 Napoleon was raiding through several German cities. As Gauss was living Göttingen, Germain came to fear for his life. She wrote a family friend in the French Army, asking him to guarantee for Gauss' safety. He did what she asked, but he was also forced to reveal the true identity of Germain. After this, Germain wrote Gauss a letter where she came clean, and explained her use of the name LeBlanc with a fear for "the ridicule attached to a female scientist". Gauss' response was maybe the most engaged he ever wrote Germain, and shows that she never had anything to fear:

How can I describe my astonishment and admiration on seeing my esteemed correspondent M leBlanc metamorphosed into this celebrated person... when a woman, because of her sex, our customs and prejudices, encounters infinitely more obstacles than men in familiarising herself with [number theory’s] knotty problems, yet overcomes these fetters and penetrates that which is most hidden, she doubtless has the most noble courage, extraordinary talent, and superior genius.
Germain sent several letters to Gauss on her progress on Fermat’s Last Theorem. Even though he eventually stopped answering, he must still have been impressed by her work because he was successful in obtaining her an honorary degree at the University of Göttingen. Unfortunately, Germain died of breast cancer in 1831, shortly before being rewarded this degree.

Germain also upheld her correspondence with Legendre. They exchanged ideas and Legendre gave Germain feedback on many of her proofs and ideas. In 1823, in his treatise in number theory, Legendre gives credit to Sophie Germain, and thus also names the theorem that is today known by her name. It is largely due to this footnote we know so much about Germain’s work today.

Germain’s main focus was to develop a proof of Fermat’s Last Theorem. Even though her plan did not work, she made great progress in taking the work away from specific exponents, to looking at more general cases. Germain was undoubtable a natural talent, and had she been given the same access to education as her male peers, she would probably have made even greater progress. As she could not discuss ideas with other mathematicians, her work often suffered from formal mistakes. Using a pseudonym, she apparently was well aware of the limitations she might have had to face due to her gender. Despite of this, her ambitions was sky-high. No one had made any success in proving Fermat’s Last Theorem for more than a few specific exponents, but yet she set out to prove it in full generality. On her death certificate she is recorded as a rentière-anuitant, that is as a single woman with no profession. In my opinion that she rather should be remembered for her important work in mathematics and for leading the way not only in the work of number theory, but also as a female scientist.
Bibliography


