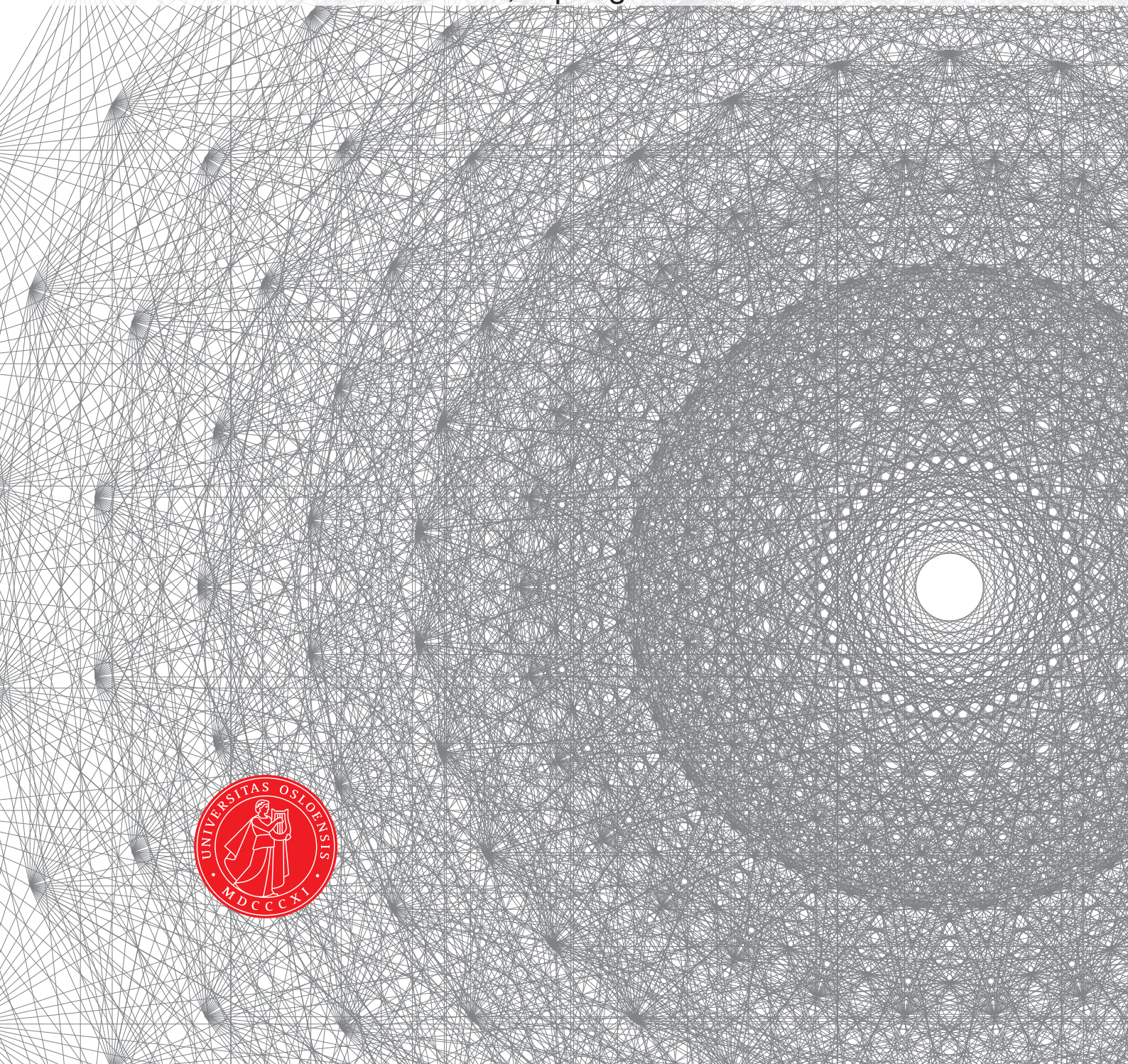
UiO : Department of Mathematics
University of Oslo

A Number Theoretical Approach to Fermat's Last Theorem

MAT5930L

Emilie Fostvedt

Master's Thesis, Spring 2020



This master's thesis is submitted under the master's programme *Lektorprogrammet*, with programme option *Mathematics*, at the Department of Mathematics, University of Oslo. The scope of the thesis is 30 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

The goal of this thesis is to investigate the equation $x^n + y^n = z^n$ from a number theoretical viewpoint. The equation was proven to have no nontrivial solutions for $n > 2$ by Andrew Wiles in the nineties. We will set out to find out when the equation has solutions modulo a prime, and if there exist common solutions. We rely on Fermat's little theorem to help make some calculations easier, as well as the Chinese Remainder Theorem when we look at common solutions. The program Python was used to lessen some of the calculations. We will gain a formula for figuring out how many solutions there are, given an exponent n and a prime p, and a method for finding common solutions given a collection of primes, a set of x, y and an exponent n.

Acknowledgements

I wish to give special thanks to my supervisor on this thesis, Kristian Ranestad, for guiding me, helping me and enduring all my stupid questions. And for helping me understand what I was trying to say. You've helped me become more unambiguous.

I also wish to thank Nasjonalforeningen for Folkehelsen, for the free coffee, the nice lunch breaks and for lending me an office, to enable the writing of this thesis.

My parents for taking care of my son when the kindergartens were closed, so I could work. My father deserves a special thank you for helping me process a lot of data and for being my rubber duck when I struggled with programming. And my grandfather for helping me optimizing my code when the numbers became so big that my compiler crashed.

An awesome collection of friends who helped with their know-how in python and giving me directions when I was stuck. Thank you Mathias, Heidi, Ingrid, Magnus, Alocias and Amund!

And of course my boyfriend, Benhjamin, for enduring my mood swings and for his support.

Last but not least, I wish to thank my son, Eik, for being the sweetheart that he is and brighten my days with all his weird questions, hugs and kisses.

Thank you all!

Oslo, 2020.

Contents

List of Tables

CHAPTER 1

Introduction

In this thesis I wanted to take a closer look at Fermat's last theorem. Ever since I read Simon Singh's book, *Fermat's last theorem*, I have been fascinated by it. Fermat's last Theorem was one of the last enigmas of the mathematical world. Such a simple equation paired with such a simple sentence that even a 10-year old could understand it, yet it took more than three centuries to prove it. The theorem is a widely known theorem in the mathematical world and contains a very simple equation, namely

$$x^n + y^n = z^n, \tag{1.1}$$

where $n \in \mathbb{N}$ and x, y, z are positive integers. The theorem states that Equation (1.1) has no non-trivial solutions when $n > 2$. In 1637 Pierre de Fermat postulated this in the margin of a copy of Arithmetica:

"It is impossible for a cube to be a sum of two cubes, a fourth power to be a sum of two fourth powers, or in general for any number that is a power greater than the second to be the sum of two like powers. I have discovered a truly remarkable proof [of this theorem], but this margin is too small to contain it."[Bri20]

For over 350 years this was only a claim because nobody was able to prove it. It was not until Andrew Wiles gave the revised proof, published in 1995, that this theorem was proven once and for all [Bri20]. In this thesis I will not give the proof or discuss the proof of this theorem, but rather look at the equation from a different perspective. I want to see what happens when we take this equation modulo p, when p is prime. The equation that is the focus in this thesis is therefore

$$x^n + y^n = z^n \pmod{p}, \tag{1.2}$$

for $x, y, z \in \mathbb{Z}_p$, $x, y, z \not\equiv 0 \pmod{p}$, $n \in \mathbb{N}$ and where p is a prime. In this thesis we will give some general results, but mostly restrict n to $n \leq 10$ and p to $2 < p < 50$.

Some questions arise with this approach. When does a solutions exist? Are there many or few solutions? Does there exist a smallest n such that there are no solutions? For a given prime p, there could possibly be many solutions. Does there then exist a set of x, y, z that is a common solution for multiple prime moduli? I hope to have answered all of these questions by the end of this thesis.

CHAPTER 2

Definitions and Theorems

To examine the equation

$$x^n + y^n \equiv z^n \pmod{p}, \tag{2.1}$$

we will need some definitions and theorems, as well as some clarification on notation.

When working in modular arithmetic we work with numbers in $\mathbb{Z}$. The set of integers modulo a prime form a group under addition, and is denoted $\mathbb{Z}_p$. For the set of integers modulo p, where p is prime, with nonzero elements, I will use the notation $\mathbb{Z}_p^*$. This is a group under multiplication and it has some properties. First, the order of the group is $p-1$. The group is also **cyclic**, meaning that there exists an element g in $\mathbb{Z}_p^*$ such that $\langle g \rangle = \mathbb{Z}_p^*$. We then call g a **generator**. 1 is a generator for $\mathbb{Z}_p$, but not for $\mathbb{Z}_p^*$. The generator for $\mathbb{Z}_p^*$ is not necessarily unique.

Primitive root

Another important definition in modular arithmetic is the notion of a primitive root. A **primitive root** of 1 is an integer x such that $x^r \equiv 1 \pmod{p}$, where the smallest integer $r = p-1$. All the elements in $\mathbb{Z}_p^*$ will be solutions, or roots to this equation, but only the elements with order $p-1$ are primitive roots. Since a generator also has order $p-1$, only the generators for the group $\mathbb{Z}_p^*$ are primitive roots of 1.

Example 2.0.1. Let's take a look at $\mathbb{Z}_3^*$ and $\mathbb{Z}_5^*$. There are only two elements in $\mathbb{Z}_3^*$, 1 and 2. 1 is not a generator, so let's look at 2. $2^1 = 2$ and $2^2 = 4 = 1$. So 2 is a generator and also a primitive root, since it satisfies the condition that the smallest exponent r such that 2^r is equivalent to 1 is $r = p-1$, in this case $3-1=2$. So the group $\mathbb{Z}_3^*$ has only one generator.

Now for $\mathbb{Z}_5^*$. We can skip 1, and start with 2. $2^1 = 2$, $2^2 = 4$, $2^3 = 8 = 3$ and $2^4 = 16 = 1$. So $\langle 2 \rangle = \mathbb{Z}_5^*$ and 2 is a generator and also a primitive root. But it is not the only one. Let's look at 3. $3^1 = 3$, $3^2 = 9 = 4$, $3^3 = 27 = 2$ and $3^4 = 81 = 1$. So 3 is also a generator and a primitive root. However 4 is not a generator, because $4^1 = 4$ and $4^2 = 16 = 1$, so we can't get all the elements in $\mathbb{Z}_5^*$ by starting with 4. Clearly $4^4 = 1$, but 4 is not the smallest such exponent where this happens, and it is therefore not a primitive root either. So in $\mathbb{Z}_5^*$ we have two generators, 2 and 3.

Greatest Common Divisor

An important definition in number theory is the greatest common divisor. The **greatest common divisor** of two positive integers is the largest positive integer that divides each of the integers. For the integers m and n it is denoted $\gcd(m, n) = d$. If the greatest common divisor is 1 we say that the integers are **relatively prime**.

Example 2.0.2. What is the greatest common divisor of 40 and 36? A fairly easy approach with smaller numbers, is to write the numbers using their prime components. $40 = 2^3 \cdot 5$ and $36 = 2^2 \cdot 3^2$. 40 and 36 have $2^2 = 4$ in common, and therefore $\gcd(40, 36) = 4$.

Euler's φ-Function

Before we can take a look at some definitions regarding the primitive root of 1, we introduce the Euler's $\varphi(n)$-function. It is a function that is defined for positive integers n and outputs the number of positive integers that are less than or equal to n and relatively prime to n. It is denoted $\varphi(n)$.

Example 2.0.3. Use of $\varphi(n)$ Let's look at $n = 7$.

$$\varphi(7) = 6, \tag{2.2}$$

because there are six numbers less than or equal to 7 that are relatively prime with 7, namely 1, 2, 3, 4, 5 and 6.

When p is a prime, then

$$\varphi(p) = p - 1. \tag{2.3}$$

Indices

We can use the notion of a generator to define what the index of an element in $\mathbb{Z}_p^*$ is. The **index** of a, for $a \in \mathbb{Z}_p^*$, with g as a generating element, is defined as

$$a \equiv g^{\text{ind a}} \pmod{p}, \tag{2.4}$$

or in other words, the index of a is which power of g that equals a. So, the index may vary depending on the choice of generator, since the group $\mathbb{Z}_p^*$ may have more than one generator. The index of $1 \equiv 0 \pmod{\varphi(p)}$. With this definition we get the following rules when taking indices:

$$\text{ind}\,(ab) \equiv \text{ind}\,a + \text{ind}\,b \pmod{\varphi(p)} \tag{2.5}$$

$$\text{ind}\,a^n \equiv n\,\text{ind}\,a \pmod{\varphi(p)}. \tag{2.6}$$

Example 2.0.4. Let's take a look at the group $\mathbb{Z}_5^*$. What is the index of 2 in this case. Now, we must first choose a generator, since the group has two generators. Let $g = 3$. To get 2, we must raise 3 to the third power, so $2 \equiv 3^3 \pmod 5$, and thus the index of 2 is then 3. But if we choose 2 as a generator, the index is 1. So it is important to know if there are more generators, and if so, make a choice of which one to use.

nth-power residues

In Equation (1.2), we raise the x and y and z to the nth power, but to actually check whether or not $x^n + y^n$ is equivalent to a z^n we need to reduce them modulo p. In doing this we use the definition of nth-power residues.

Definition 2.0.5. An integer a is called an **nth-power residue modulo** m if there exist an x such that

$$x^n \equiv a \pmod{m}. \tag{2.7}$$

A special case of nth-power residues is when $n = 2$.

Definition 2.0.6. An integer a is called a **quadratic residue** modulo m if there exists an n such that

$$x^2 \equiv a \pmod{m} \tag{2.8}$$

Another special case is when we let $n = 3$, we then call it a **cubic residue**.

Fermat's little theorem

Some of the work in Chapter 3 uses a theorem often referred to as Fermat's little theorem.

Theorem 2.0.7. ***Fermat's little theorem*** *If p is a prime number, then for any integer a, where p does not divide a, or $a \not\equiv 0 \pmod{p}$ the following holds*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{2.9}$$

Corollary 2.0.8. *If $a \in \mathbb{Z}$, then*

$$a^p \equiv a \pmod{p}, \tag{2.10}$$

for any prime p.

Because this is a widely known theorem that is easily proved, I will not give the proof here. For the avid reader, one proof can be found on page 184 in Fraleigh's book, [Fra03].

Example 2.0.9. Let $a = 2$ and $p = 7$. Then $2^6 = 64$ and $64 - 1 = 63 = 9 \cdot 7$, which indeed is a multiple of 7.

Modular Multiplicative Inverses

We have now looked at some important definitions and theorems that will be used in this thesis, but we still need to define inverses. What does it mean to have a multiplicative inverse in modular arithmetic? A modular multiplicative inverse of an integer $a \pmod{n}$ is an integer x such that

$$ax \equiv 1 \pmod{n} \tag{2.11}$$

for a given natural number n.

Example 2.0.10. In $\mathbb{Z}_5^*$ the inverse of 3 is 2, because $3 \cdot 2 = 6$ which is 1 in $\mathbb{Z}_5^*$.

This means that fractions as inverses can be rewritten as an integer. Let's look at 2^{-1}. It is the inverse of 2, and can also be written as $\frac{1}{2}$ in $\mathbb{Q}$. But we can't write it as a fraction because we are working in $\mathbb{Z}_p^*$. Since $\frac{1}{2}$ has 2 as an inverse, and in e.g. $\mathbb{Z}_5^*$, 3 also has 2 as an inverse, we could argue that in fact $\frac{1}{2} = 3$ when we are working in $\mathbb{Z}_5^*$. Now we have a concise way of thinking about inverses using conventional notation. This means that it is possible to find what x^{-2}, x^{-3}... and so on is in $\mathbb{Z}_p^*$. For example is $2^{-2} = \left(2^{-1}\right)^2 = 3^2 = 9 = 4$ in $\mathbb{Z}_5^*$.

If we now look at x^{p-1} we see that

$$x^{p-1} \equiv x^p \cdot x^{-1} \equiv x^1 \cdot x^{-n} \equiv x^{1-n} \equiv \left(x^{-1}\right)^{n-1} \pmod{p}. \tag{2.12}$$

This result will be useful in the next chapter.

Common Solutions

The equation we are investigating is $x^n + y^n \equiv z^n \pmod{p}$. But what happens when we want to look at common solutions? Here a common solution means a set of x, y, z that solves the equation for multiple primes p at the same time, or finding a solution to a system of congruences,

$$\begin{aligned} x^n + y^n &\equiv z^n \pmod{p_1} \\ x^n + y^n &\equiv z^n \pmod{p_2} \\ &\vdots \\ x^n + y^n &\equiv z^n \pmod{p_i}. \end{aligned}$$

In essence this is finding an intersection for multiple arithmetic progressions, and to do that we need another important result in number theory.

Theorem 2.0.11. ***Chinese Remainder Theorem*** *If gcd* $(m_i, m_j) = 1$ *for* $1 \leq i < j \leq r$*, then the system*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_r \pmod{m_r} \end{aligned}$$

has as its complete solution a single residue class $\pmod{m_1 \cdot \ldots \cdot m_r}$

The proof can be seen on page 60 in LeVeque's book, [LeV77]. Now, how do we use this theorem in our case? First we notice that since we are working with prime moduli, the condition of gcd $(p_i, p_j) = 1$, for $1 \leq i < j \leq s$, is always true in our case. We are also not just looking at x, but at x^n, for $3 \leq n \leq 10$. Let $x^n = x'$. We then get

$$x' \equiv c_1 \pmod{p_1}$$

$$\begin{aligned} x' &\equiv c_2 \pmod{p_2} \\ &\vdots \\ x' &\equiv c_s \pmod{p_s}. \end{aligned}$$

Let's make the same system of congruences, but for y, where $y^n = y'$,

$$\begin{aligned} y' &\equiv d_1 \pmod{p_1} \\ y' &\equiv d_2 \pmod{p_2} \\ &\vdots \\ y' &\equiv d_s \pmod{p_s}. \end{aligned}$$

Now we add each of these linear congruences pairwise based on their moduli,

$$\begin{aligned} x' + y' &\equiv c_1 + d_1 \pmod{p_1} \\ x' + y' &\equiv c_2 + d_2 \pmod{p_2} \\ &\vdots \\ x' + y' &\equiv c_s + d_s \pmod{p_s}. \end{aligned}$$

Our task is to see if $\exists z$ such that

$$\begin{aligned} z' &\equiv c_1 + d_1 \pmod{p_1} \\ z' &\equiv c_2 + d_2 \pmod{p_2} \\ &\vdots \\ z' &\equiv c_s + d_s \pmod{p_s}, \end{aligned}$$

where $z' = z^n$. By using the Chinese remainder theorem on this last system of linear congruences we see that the complete solution must lie in the residue class $\pmod{p_1 \cdot \ldots \cdot p_s}$. So for $p = 3, 5$, the solution must lie in $\pmod{15}$, and for e.g. $p = 3, 5, 7, 11$ the solution lie in $\pmod{1155}$.

Many of these results and definitions will be used throughout the thesis, but Fermat's little theorem is especially important for the next chapter. In the last part of chapter 5 we will rely on the Chinese Remainder Theorem to help us analyse the situation.

CHAPTER 3

Pre-program work

It is obvious that the equation $x^n + y^n \equiv z^n \pmod{p}$ has many trivial solutions. A trivial solution means a solution where x, y, z are all zero, or x, y, z are 0 (mod p). Another fairly trivial solution is when one of them is equal to 0. Then the equation become either $x = z$, $y = z$ or $x = -y$, which all have infinite solutions. Thus, in this chapter, I will focus on solutions where, $x, y, x \neq 0$ and $x, y, z \not\equiv 0 \pmod{p}$.

If an integer is a quadratic residue, as stated in Definition 2.0.6, that would mean that the exponent n in Equation (1.2) is equal to 2. This is the same as finding pythagorean triples, which there are infinitely many of, as proven by Euclid, and is not in the scope of this thesis. This means that whenever we end up with an exponent $n = 2$ or $n = -2$, we already know if there are any solutions or not.

Now I want to take a look at different exponents. Let's take a closer look at $n = p \pm r$ for certain r and see what happens with our equation.

3.1 Exponent *n=p+1*

I wanted to reduce the number of calculations as much as possible before actually having to program them, in order to limit the data output. Therefore I started looking at what happens when the exponent n in Equation (1.2) is greater than the prime p. We know from Equation (2.9) that $a^p \equiv a \pmod{p}$. I first want to look at $n = p + 1$. Equation (1.2) then becomes

$$x^{p+1} + y^{p+1} = z^{p+1} \pmod{p}, \tag{3.1}$$

which can be rewritten as

$$x^p \cdot x + y^p \cdot y = z^p \cdot z \pmod{p}. \tag{3.2}$$

And by Fermat's little theorem we get

$$x \cdot x + y \cdot y = z \cdot z, \tag{3.3}$$

that becomes

$$x^2 + y^2 = z^2 \pmod{p} \tag{3.4}$$

which we know have infinitely many solutions for $x, y, z \in \mathbb{Z}$.
When we increase the exponent by 1, we get

$$x^{p+2} + y^{p+2} = z^{p+2} \pmod{p}, \tag{3.5}$$

which by Fermat's little theorem then becomes

$$x \cdot x^2 + y \cdot y^2 = z \cdot z^2 \pmod{p} \tag{3.6}$$

$$x^3 + y^3 = z^3 \pmod{p} \tag{3.7}$$

By this we see a pattern emerging. Let us rephrase the initial statement that $n > p$, and say that $n = a \cdot (p-1) + r$, for some $r < p-1$, and $r \in \mathbb{N}$. We need only look at $r < p-1$, because whenever $r = p-1$, by Fermat's little theorem we get

$$x^1 + y^1 = z^1 \pmod{p}, \tag{3.8}$$

which we know has infinitely many solutions.

$$x^{(p-1)+r} + y^{(p-1)+r} = z^{(p-1)+r} \pmod{p}, \tag{3.9}$$

we get

$$x^r + y^r = z^r \pmod{p} \tag{3.10}$$

by Fermat's little theorem. And since $r < (p-1)$ we don't need to concern ourselves with an exponent $n > (p-1)$. This only reduce the problem for $p = 3$, $p = 5$, $p = 7$, and $p = 11$ since for all other cases $n < (p-1)$.

3.2 Exponent *n=p-1*

When the set the exponent $n = p - 1$ we get

$$x^{p-1} + y^{p-1} = z^{p-1} \pmod{p}, \tag{3.11}$$

which by Fermat's little theorem becomes

$$x \cdot x^{-1} + y \cdot y^{-1} = z \cdot z^{-1} \pmod{p}, \tag{3.12}$$

and we get

$$1 + 1 = 1 \pmod{p}, \tag{3.13}$$

which obviously has no solutions.

3.3 Exponent *n=p-2*

When we set the exponent $n = p - 2$ we get

$$x^{p-2} + y^{p-2} = z^{p-2} \pmod{p}, \tag{3.14}$$

which by Fermat's little theorem becomes

$$x^1 \cdot x^{-2} + y^1 \cdot y^{-2} = z^1 \cdot z^{-2} \pmod{p}, \tag{3.15}$$

which in turn is

$$x^{-1} + y^{-1} = z^{-1} \pmod{p}. \tag{3.16}$$

This is equivalent to the equation

$$x + y \equiv z \pmod{p}, \tag{3.17}$$

and it has a solution in $\mathbb{Z}_p^*$ for every x, $y \in \mathbb{Z}_p^*$ such that $x, y \not\equiv 0$.

3.4 Exponent *n=p-r*

As we continue with this pattern we will get -2, -3,... as the value of the exponent and eventually come back to an exponent we have already investigated, only with a negative value.

In modular arithmetic this turns out to be the same as the positive exponent, and we get an upper constraint on the exponent, namely $\frac{p-1}{2}$.

Let's replace n with $\frac{p-1}{2}$. We then get

$$x^{\frac{p-1}{2}} + y^{\frac{p-1}{2}} = z^{\frac{p-1}{2}} \pmod{p}. \tag{3.18}$$

When restating this we get

$$(x^{p-1})^{\frac{1}{2}} + (y^{p-1})^{\frac{1}{2}} = (z^{p-1})^{\frac{1}{2}} \pmod{p}. \tag{3.19}$$

By Fermat's little theorem we then get

$$1^{\frac{1}{2}} + 1^{\frac{1}{2}} = 1^{\frac{1}{2}}, \tag{3.20}$$

which of course is

$$\pm 1 \pm 1 = \pm 1. \tag{3.21}$$

These are only solutions in $\mathbb{Z}_3^*$, for $1 + 1 = -1$ and $-1 + -1 = 1$. For all other $\mathbb{Z}_p^*$ with $p > 3$ these 4 possibilities will not yield a valid solution, and we get a restriction for the exponent.

Lemma 3.4.1. ***Exponent restriction*** *Let $p > 3$ and $x, y, z \not\equiv 0$. When the exponent n in the equation $x^n + y^n \equiv z^n \pmod{p}$ is equal to $\frac{p-1}{2}$ there is no solution.*

All of the results stated in this chapter will help reduce the output and calculation time for the codes presented in the next chapter.

CHAPTER 4

Programming

To calculate all possible solutions to $x^n + y^n \equiv z^n \pmod{p}$ by hand is extremely tedious and takes way too long. I therefore made some small codes to help me with the workload.

4.1 Code for finding nth-power residues

To be able to look at solutions for the equation in question, I first looked at nth-power residues. To make it easier to calculate the residues from the different powers modulo a prime, I wrote a code to do it for me. The code can be seen below.

```
import numpy as np
primes=[3,5,7,11,13,17,19,23,29,31,37,41,43,47]

expo=[3,4,5,6,7,8,9,10]


n=6

for p in primes:
    pnew=p-1
    a= [None]*pnew
    for i in range(pnew):
        a[i]=i+1
    b=[None]*pnew
    for i in range (pnew):
        b[i]=a[i]**n %p
    print(b)
```

The residues that this code calculates can be seen in Appendix A, when the exponent n goes from 3 to 10.

4.2 Code for finding solutions to $x^n + y^n \equiv z^n \pmod{p}$

There are many many solutions to $x^n + y^n \equiv z^n \pmod{p}$. I wrote the following code to get the different solutions to this equation, for $3 \leq p < 50$ and the exponent n ranging from 3 to 10.

```
primes=[3,5,7,11,13,17,19,23,29,31,37,41,43,47]

expo=[3,4,5,6,7,8,9,10]


n=8


def unique(array):
  return list(dict.fromkeys(array))


for p in primes:
    pnew=p-1
    a= [None]*pnew
    for i in range(pnew):
        a[i]=i+1
    b=[None]*pnew
    for i in range (pnew):
        b[i]=a[i]**n %p
    final_list=unique(b)
    array_list = []
    for x in final_list:
        for y in final_list:
            for z in final_list:
                if (x+y)%p==z:
                    array_list.append([x,y,z])
                    print(x,y,z)

    frame = pd.DataFrame(array_list, columns=['','',''])
    print(frame.to_latex(index=False,column_format='ccc',
    caption='Solutions to Fermat in $\Z_%d^*$' % p,label='sol-n-z%d' % p))
```

This code uses the nth-power residues and checks whether or not an x^n, y^n and z^n satisfies Equation (1.2). If so, the code outputs $x^n, y^n, z^n \pmod{p}$ as an array, and then gives that array as a row in a table with LaTeX syntax. The results from this program can be seen in Appendix B. In this Appendix a few complete tables of solutions are listed, and the number of solutions are listed for the rest.

4.3 Common solutions

To check common solutions manually was fairly easy with very small p. But when I wanted to check for more p and larger p, like common solutions for $p = 3$, $p = 5$, $p = 7$ and $p = 11$, it was too many solutions to check by hand. In stead I wrote a code that outputs all the sets of x, y, z that is a solution for a given n and all primes $3 \leq p < 50$. The code doesn't check if any of the sets are common for the different p, but rather outputs all of them as a .txt file. The code can be seen below.

```
import functools
import operator

primes=[3,5,7,11]
n=3

f=open('Common_sol_n=3_p=11.txt', 'w')
tot_mod=functools.reduce(operator.mul,primes)

for p in primes:
    f.write('Modulus:'+str(p)+'\n')
    for x in range(1,tot_mod+1):
        xmod=x%p
        a=pow(xmod,n,p)
        for y in range(1,tot_mod+1):
            ymod=y%p
            b=pow(ymod,n,p)
            d=(a+b)%p
            for z in range(1,tot_mod+1):
                zmod=z%p
                c=(zmod,n,p)
                if d==c:
                    sol=[x,y,z]
                    sol_str= ",".join(str(i) for i in sol)
                    f.write(sol_str + '\n')

f.close()
```

The data from this program is then imported into Excel, and then I used Excel's IF function to check if any of the sets of x, y, z were common for the different primes. The result of the Excel-processed data can be seen in Table 5.2.

CHAPTER 5

Analyzing results

The codes in Chapter 4 yields many tables seen in Appendix A and Appendix B. By analyzing them and looking closer I wanted to see if I could find a pattern that may lead to a result.

5.1 Number of residues

When looking at the tables in Appendix A, we see that when the gcd $(p-1, n) = 1$ there are $p-1$ number of unique nth-power residues. When $\gcd(p-1, n) > 1$ there are $\frac{p-1}{\gcd\,(p-1,n)}$ number of nth-power residues. These results are generalized in the following theorem.

Theorem 5.1.1. *Let p be a prime and $d = gcd(n, \varphi(p))$. The equation*

$$x^n \equiv a \pmod{p} \tag{5.1}$$

then has a solution for a fixed $a \in \mathbb{Z}_p^*$ if and only if

$$a^{\varphi(p)/d} \equiv 1 \pmod{p}. \tag{5.2}$$

Furthermore the number of unique nth-power residues in $\mathbb{Z}_p^*$ is $\frac{\varphi(p)}{d}$.

Proof. First, since d divides n, let $n = k \cdot d$ for some $k \in \mathbb{Z}$. Suppose that there is a a solution to Equation (5.1), namely $x^n = a$. Then

$$a^{\varphi(p)/d} \equiv (x^n)^{\varphi(p)/d} \equiv x^{k\cdot\varphi(p)} \equiv x^{(p-1)\cdot k} \equiv \left(x^{(p-1)}\right)^k \equiv 1^k \equiv 1 \pmod{p}, \tag{5.3}$$

by Fermat's little theorem and the results from Section 3.2.
Now assume that

$$a^{\varphi(p)/d} \equiv 1 \pmod{p}. \tag{5.4}$$

Taking indices yields

$$\frac{\varphi(p)}{d}\text{ind } a \equiv \text{ind } 1 \pmod{\varphi(p)}. \tag{5.5}$$

The index of 1 is by definition 0 $\pmod{\varphi(p)}$. For simplicity, call ind $x = \alpha$ and ind $a = \beta$. We then get

$$\frac{p-1}{d}\beta \equiv 0 \pmod{p-1}, \tag{5.6}$$

which is equivalent to

$$\beta \equiv 0 \pmod{d}. \tag{5.7}$$

This in turn is equivalent to $d \mid \beta$. And with $d = \gcd(n, \varphi(p))$, this means that the equation

$$n\alpha \equiv \beta \pmod{\varphi(p)} \tag{5.8}$$

is solvable, and that the equation

$$x^n \equiv a \pmod{p} \tag{5.9}$$

has a solution.

Now for number of solutions. If g is a primitive root, meaning in this case that $\langle g \rangle = \mathbb{Z}_p^*$, then the $\varphi(p)/d$ numbers $g^d, g^{2d}, \ldots, ^{(\varphi(p)/d)d}$ are distinct (mod p) and satisfy Equation (5.2), and there must be $\varphi(p)/d$ of them. ■

Corollary 5.1.2. *If $(p-1, n) = 1$, there are $p-1$ nth-power residues in $\mathbb{Z}_p^*$.*

With this Corollary we can stipulate that when $\gcd(p-1, n) = 1$ we have many nth-power residues to check for a solution, and there are probably many. We will come back to this in the next section.

5.2 Solutions

Many tables in Appendix B list the possible solutions to Equation (1.2). The first 2 tables show the solutions, and Table B.4 show how many soutions there are for a given prime p and a given exponent n. To see if there was a certain pattern for when there was a solution or not, I made a table that shows exactly that. Table 5.1 is a truth table of whether or not there exist a solution to Equation (1.2) for a prime p, and an exponent n, where $3 \leq p < 50$ and $n = 3, 4, \ldots, 10$.

From Table 5.1 we can see that $\nexists\, n$ such that Equation (1.2) is solvable $\forall$ p. However, $\exists\, p$ such that Equation (1.2) is solvable $\forall\, n$. These p are $p = 23$ and $p = 47$. By checking the gcd $(n, \varphi(p))$ and the number of solutions for given n and p, I noticed that there is a pattern to the solutions whenever gcd $(n, \varphi(p)) = 1$. This is generalized in the following theorem.

Theorem 5.2.1. *If the gcd $(n, \varphi(p) = 1)$, then the number of solutions to Equation (1.2) is $(p-1) \cdot (p-2)$, if we let $x^n + y^n \equiv z^n$ be a different solution from $y^n + x^n \equiv z^n$.*

Proof. When the gcd $(n, \varphi(p)) = 1$ we know from Corollary 5.1.2 that the number of nth-power residues is $p-1$. This means that we have $p-1$ choices for x^n. When this is chosen we cannot choose a y^n that is equivalent to $p - x^n$ (mod p) because that would yield 0 which we do not allow as a solution. Thus we are left with $p-2$ choices for y^n. We can permute these choices in $(p-1) \cdot (p-2)$ different ways. The number of solutions to Equation (1.2) for a given n and p such that gcd $(n, \varphi(p)) = 1$ is then $(p-1) \cdot (p-2)$. ■

p \ n	3	4	5	6	7	8	9	10
3	1	-	-	-	-	-	-	-
5	1	-	-	-	-	-	-	-
7	0	-	-	-	-	-	-	-
11	1	1	0	-	-	-	-	-
13	0	0	1	0	-	-	-	-
17	1	0	1	1	1	0	-	-
19	1	1	1	0	1	1	0	-
23	1	1	1	1	1	1	1	1
29	1	1	1	1	0	1	1	1
31	1	1	1	1	1	1	1	0
37	1	1	1	1	1	1	0	1
41	1	0	0	1	1	0	1	0
43	1	1	1	0	1	1	1	1
47	1	1	1	1	1	1	1	1

Table 5.1: Truth table for whether there exists a solution to Equation (1.2) for certain p and n when $x, y, z \neq 0$.

Example 5.2.2. Let $p = 5$ and $n = 3$. gcd $(3, 4) = 1$. Then the number of solutions is $4 \cdot 3 = 12$. This is also easy to count. We start with $1 + 1 = 2$, $1 + 2 = 3$, $1 + 3 = 4$. Here we have 3 solutions. For the next set we start with $2 + 1 = 3$, then $2 + 2 = 4$, we skip $2 + 3 = 5 = 0$ since $0 \notin \mathbb{Z}_p^*$ and go straight to $2 + 4$. We now also have 3 solutions. We will get 3 new solutions when starting with 3 as our x^n, and as well as for 4, and we get the total of $4 \cdot 3 = 12$ number of solutions.

If we now take in to consideration that the operation $+$ is commutative in the group $\mathbb{Z}_p^*$ and let $x^n + y^n \equiv z^n$ be the same solution as $y^n + x^n \equiv z^n$, we get a smaller number of purely unique solutions.

Theorem 5.2.3. *If the gcd* $(n, \varphi(p)) = 1$*, then the number of unique solutions to Equation* (1.2) *is*

$$\frac{(p-1)^2}{2}.$$

Proof. I will prove this by counting. First we must have that gcd $(n, \varphi(p)) = 1$, since that gives us $p - 1$ number of nth-power residues to make solutions from. I split the possible solutions in to distinct sets, based on the first term of the solution. So set no. 1, S_1 will be comprised of all solutions of the form $1 + a$, for any $a \in \mathbb{Z}_p^*$. Now S_1 will consist of the following solutions

$$\begin{aligned} &1 + 1 \\ &1 + 2 \\ &\vdots \\ &1 + (p-1) \end{aligned}$$

These are all the permutations of the nth-power residues with 1 as the first term, and there are $(p - 1)$ of them. However, we must discard one of them,

the last one. This is because it yields 0 in $\mathbb{Z}_p^*$, and $0 \notin \mathbb{Z}_p^*$. This leaves us with $(p-2)$ solutions for the first set. For the second set, S_2, we list all the possible solutions first, and then see if we need to discard any of them.

$$\begin{aligned} &2+1 \\ &2+2 \\ &\vdots \\ &2+(p-2) \\ &2+(p-1). \end{aligned}$$

For S_2 we see that we must discard two solutions. $2+1$ since it has already been counted as $1+2$ in S_1, as well as $2+(p-2)$ since this yields 0 in $\mathbb{Z}_p^*$. That leaves us with $(p-3)$ solutions. One could imagine that we could just follow this pattern until we reach the last set, which must contain 1. But since S_1 consist of $(p-2)$ solutions, S_2 of $(p-3)$ and so on, the set containing one solution, $(p-1)+(p-1)$ is the second to last set, S_{p-2} and not S_{p-1}. So what went wrong?

Let's take closer look at the group $\mathbb{Z}_p^* = \{1, 2, \ldots, a, b, \ldots, p-2, p-1\}$. where $a = \frac{p-1}{2}$ and $b = a+1$. We follow out initial pattern all the way to the set S_a which consist of the following possible solutions

$$\begin{aligned} &a+1 \\ &a+2 \\ &\vdots \\ &a+a \\ &a+b \\ &\vdots \\ &a+(p-1). \end{aligned}$$

We end up discarding all the possible solutions before the solution $a+a$, which there are $\frac{p-1}{2}-1$ of, as well as the solution $a+(p-a)$, meaning we discard a total of $\frac{p-1}{2}$ solutions, and we are left with $\frac{p-1}{2}$ solutions, since there were $(p-1)$ possibilities to begin with.

Now the problem arises when we get to the set S_b. We list the possible solutions,

$$\begin{aligned} &b+1 \\ &b+2 \\ &\vdots \\ &b+a \end{aligned}$$

$$\begin{aligned} &b+b \\ &\vdots \\ &b+(p-1). \end{aligned}$$

Note that we automatically discard all solutions before $b+b$, since these have been counted in the previous sets. And then we usually discard an extra solution, $b+(p-b)$. But in this case, the extra solution we discard, because it yields 0, is in fact $b+a$, since $b+(p-b) = p = 1+(p-1) = 1+\frac{p-1}{2}+\frac{p-1}{2} = 1+a+a = b+a$. We have already discarded this solution, and we can't discard it twice, so we get one more solution than expected. Thus the number of solutions in S_b we count is also $\frac{p-1}{2}$. Now the next set S_{b+1} will have the same issue. We have already discarded the solution that yields 0, so we are left with $\frac{p-1}{2}-1$ solutions. This new pattern leads us all the way down to S_{p-1} which now correctly gives us one solution to count.

For the total number of unique solutions we count the valid solutions in all the sets and get the following sum

$$(p-2)+(p-3)+\ldots+\frac{p-1}{2}+\frac{p-1}{2}+\left(\frac{p-1}{2}-1\right)+\ldots+2+1.$$

By adding these together in a clever way, we get

$$[1+(p-2)]+[2+(p-3)]+\ldots+[\frac{p-1}{2}+\frac{p-1}{2}].$$

Each of these part sums yield $p-1$ and there are $\frac{p-1}{2}$ of them. That gives us

$$\frac{p-1}{2}\cdot(p-1) = \frac{(p-1)^2}{2}$$

■

Example 5.2.4. Let $p = 5$ and $n = 3$. gcd $(3,4) = 1$, so we can use the formula in Theorem 5.2.3. Then the number of unique solutions is $\frac{(5-1)^2}{2} = \frac{16}{2} = 8$. This is also easy to count. For the first set, we have the solutions comprised of nth-power residues: $1+1 = 2$, $1+2 = 3$ and $1+3 = 4$. Same as the previous example. For the next set, we have the valid solutions $2+2 = 4$ and $2+4 = 1$. For the third set, we get $3+3 = 1$ and $3+4 = 2$ and for the last set we have $4+4 = 3$. In total this is 8 unique solutions, as expected.

5.3 Common solutions

I also wanted to take a look at common solutions, meaning a set of x, y, z that yields a solution for several moduli. There does not exist a common solution (x, y, z), to Equation (1.2) for all primes under 20 because $n = 3$ is the only exponent worth investigating for the smaller primes 3, 5 and 7, and for $n = 3$ there are no solutions with $p = 7$ or $p = 13$, with $x, y, z \not\equiv 0 \pmod{p}$. But to properly check for common solutions we must lift the restriction $x, y, z \not\equiv 0 \pmod{p}$ since we are looking at different moduli. Therefore we cannot use

Table 5.1 as a basis for our investigation, but rather look at a larger set of values for x, y, z. Now, since we are looking for solutions in multiple moduli the allowed values for x, y and z will range from 1 to the product of all the moduli, as stated in Chapter 2, as a result of the Chinese Remainder Theorem. Let's see if we can find a common solution for small p and n.

Example 5.3.1. Let $n = 3$ and $p = 3$ and $p = 5$. Does there exist common solutions when we allow $x, y, z \equiv 0 \pmod{p}$? The answer is yes. Look at e.g. the set $(x, y, z) = (1, 4, 5)$. In $\mathbb{Z}_3$ these x, y, z to the third power yield $1 + 1 = 2$ which is a solution. In $\mathbb{Z}_5$ we get $1^3 + 4^3 \equiv 1 + 4 = 0$, which is also a solution. In fact for these two primes with $n = 3$ we have a set of 225 common solutions. We get a total of 225 solutions for $n = 3$ and $p = 3, 5$, because we let $x, y, z \in \{1, \ldots, 15\}$, since $3 \cdot 5 = 15$.

Example 5.3.2. If we now take a look at the primes $3, 5$ and 7, and the exponent $n = 3$, the set of $\{x, y, z\} = \{1, 3, 7\}$ yields a solution for all the moduli. This is fairly easy to calculate. In $\mathbb{Z}_3$ $1^3 + 3^3 = 1 + 0 = 1$ and $7^3 = 1$ so it is a solution. In $\mathbb{Z}_5$ we get $1^3 + 3^3 = 1 + 2 = 3 = 7^3$, and is also a solution. In $\mathbb{Z}_7$ $1^3 + 3^3 = 1 + 6 = 0 = 7^3$.

If we look at a set of larger primes, and thus a larger set of moduli, we get an increasing number of allowed values for our set of $\{x, y, z\}$. For example for all primes up to 47, the allowed values ranges from 1 to $307,444,891,294,245,705$. So naturally one can expect that the numbers of common solutions will increase, when we increase the number of moduli. This can be seen for primes up to 11 in Table 5.2.

p_i \ n	3	4	5	6	7	8	9	10
5	225	297	225	225	225	297	225	225
7	12375	14553	11025	16425	11025	14553	12375	11025
11	1497375	1760913	1664775	1987425	1334025	1760193	1497375	2216025

Table 5.2: Number of common solutions for all primes less than or equal to p_i, n from 3 to 10, and x, y, z between 1 and P, where $P = \prod_{i=1}^{s} p_i$.

As we can see from Table 5.2, when we increase the number of primes we look for common solutions for, the number of solutions increase quite a lot. I wanted to see if I could get to common solutions for all primes up to 47, but I was limited by my program. When trying to generate this much data, not only did my program not terminate, and I had to manually terminate it, but the txt file that was generated was too big for many of my text editors. I managed to open one of the txt files, only to discover that it consisted of over a million lines of solutions and after about a minute the editor crashed. Thus, the table is somewhat limited compared to what I wanted. But, we might be able to get some results from the limited data.

First, there will always be at least one solution for all moduli, namely $P + P = P$, where $P = \prod_{i=1}^{s} p_i$. This will yield $0 + 0 = 0$ inn all moduli, since the product of all the primes will be a multiple of the given prime modulus. I denote this solution the trivial common solution. E.g for primes $3, 5$ this trivial

common solution will be $15^n + 15^n = 15^n$, since this yields $0 + 0 = 0$ in both $\mathbb{Z}_3$ and $\mathbb{Z}_5$, regardless of the value of n.

We can also find a common solution x, y, z when we have a pair of $\{x, y\}$. Our task then, if possible, is to find the z as stated in Chapter 2. Let $x = 10$ and $y = 23$. Let's try and find a common solution for the prime moduli $3, 5, 7$ and $n = 3$. First we find what x^n and y^n is modulus the primes.

$$\begin{aligned} 10^3 &\equiv 1 \pmod 3 \quad \text{and} \quad 23^3 \equiv 2 \pmod 3, \\ 10^3 &\equiv 0 \pmod 5 \quad \text{and} \quad 23^3 \equiv 2 \pmod 5, \\ 10^3 &\equiv 6 \pmod 7 \quad \text{and} \quad 23^3 \equiv 1 \pmod 7. \end{aligned}$$

Now we sum,

$$\begin{aligned} 1 + 2 &\equiv 0 \pmod 3 \\ 0 + 2 &\equiv 2 \pmod 5 \\ 6 + 1 &\equiv 0 \pmod 7. \end{aligned}$$

Now we make use of the fact that the moduli are pairwise relatively prime, and create the system

$$\frac{P}{p_i} z_i \equiv 1 \pmod{p_i}.$$

In our case that yields the congruences

$$\begin{aligned} 35 \cdot z_1 &\equiv 1 \pmod 3, \\ 21 \cdot z_2 &\equiv 1 \pmod 5, \\ 15 \cdot z_3 &\equiv 1 \pmod 7, \end{aligned}$$

and they have solutions $z_1 = 2$, $z_2 = 1$ and $z_3 = 1$. We then get that

$$\begin{aligned} z^3 &\equiv 35 \cdot 2 \cdot 0 + 21 \cdot 1 \cdot 2 + 15 \cdot 1 \cdot 0 \\ &\equiv 42 \pmod{105}. \end{aligned}$$

We get that our $z = 63$, since $63^3 \equiv 42 \pmod{105}$. Our set of $\{x, y, z\}$ is then $\{10, 23, 63\}$. However if we were to choose $\{x, y\} = \{1, 2\}$ we would by following the same method end up with the equation $z^3 \equiv 9 \pmod{105}$, which has no solution. So these values for x and y yield no solution.

5.4 Conclusion

As the previous sections shows, there are indeed solutions to $x^n + y^n \equiv z^n \pmod p$ when we are working in the cyclic group $\mathbb{Z}_p^*$. By Theorem 5.2.1 we now know that if $\gcd(n, p-1) = 1$ there are $(p-1) \cdot (p-2)$ solutions. As Table 5.1 shows, not all combinations of n and p yields a solution, but many do. For the primes $p = 23$ and $p = 47$ there are at least one solution $\forall n$, when $n = 3, \ldots 10$. The results from Section 3.4 is clearly visible in Table 5.1. For example for $n = 3$ and $p = 7$, we see that there is no solution, because $\frac{7-1}{2} = 3$, and our

lemma then states that there can be no solutions. The same is the case for the pairs $(n, p) = \{(5, 11), (6, 13), (8, 17), (9, 19)\}$. So there will never be solutions when the exponent $n = \frac{p-1}{2}$.

When we then look at common solutions, we see that we must make use of the Chinese Remainder Theorem. First we see that we must increase our allowed values for x, y, z, from $p - 1$ to the multiple of the prime moduli. This action lifts the restriction $x, y, z \not\equiv 0 \pmod{p_i}$ for any prime modulus p_i. Second, there are many common solutions, for at least the primes up to $p = 11$. Third, if we choose a set of x and y and an n, we can find a common a solution for several prime moduli by using the method showed in Section 5.3. If no such solution exist, we end up with an insolvable modulus equation of the form, $z^n \equiv d \pmod{P}$, where P is the product of all the prime moduli.

We can also use Table 5.1 to tell us something about the composition of our x, y, z in a common solution. E.g a common solution for $n = 3$ and $p = 3, 5, 7$ must have that $7 \mid xyz$. This is because we know from the table that there are no solutions to $x^3 + y^3 \equiv z^3 \pmod 7$ when $x, y, z \not\equiv 0 \pmod 7$. So to have a solution when we are in $\pmod 7$, at least one the x, y, z must be a multiple of seven. The same happens for common solutions when $n = 4$. If we then look at common solutions up to $p = 47$, we get that the product of x, y, z must be a multiple of 13, 17 and 41, or $13 \cdot 17 \cdot 41 \mid xyz$. So whenever we look at common solutions with a collection of primes, we now know that if for a given n and p, the equation has no nontrivial solutions, a common solution must then have that the prime $p \mid xyz$.

Appendices

APPENDIX A

nth-power residues in $\mathbb{Z}_p^*$

A.1 Cubic Residues

The cubic residues in $\mathbb{Z}_p^*$ for a prime p and with $3 \leq p < 50$ are listed in the following tables

$\mathbb{Z}_3^*$	$\gcd(2,3) = 1$
1	$1^3 \equiv 1 \pmod 3$
2	$2^3 \equiv 2 \pmod 3$

Table A.1: Cubic residues in $\mathbb{Z}_3^*$

$\mathbb{Z}_5^*$	$\gcd(4,3) = 1$
1	$1^3 \equiv 1 \pmod 5$
2	$2^3 \equiv 3 \pmod 5$
3	$3^3 \equiv 2 \pmod 5$
4	$4^3 \equiv 4 \pmod 5$

Table A.2: Cubic residues in $\mathbb{Z}_5^*$

$\mathbb{Z}_7^*$	$\gcd(6,3) = 3$
1	$1^3 \equiv 1 \pmod 7$
2	$2^3 \equiv 1 \pmod 7$
3	$3^3 \equiv 6 \pmod 7$
4	$4^3 \equiv 1 \pmod 7$
5	$5^3 \equiv 6 \pmod 7$
6	$6^3 \equiv 6 \pmod 7$

Table A.3: Cubic residues in $\mathbb{Z}_7$

Group	Cubic residues
$\mathbb{Z}_{11}*$	All elementens in $\mathbb{Z}_{11}*$
$\mathbb{Z}_{13}*$	$\{1, 5, 8, 12\}$
$\mathbb{Z}_{17}*$	All elements in $\mathbb{Z}_{17}^*$
$\mathbb{Z}_{19}*$	$\{1, 7, 8, 11, 12, 18\}$
$\mathbb{Z}_{23}*$	All elements in $\mathbb{Z}_{23}$
$\mathbb{Z}_{29}*$	All elements in $\mathbb{Z}_{29}$
$\mathbb{Z}_{31}*$	$\{1, 2, 4, 8, 15, 16, 23, 27, 29, 30\}$
$\mathbb{Z}_{37}*$	$\{1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36\}$
$\mathbb{Z}_{41}*$	All elements in $\mathbb{Z}_{41}$
$\mathbb{Z}_{43}*$	$\{1, 2, 4, 8, 11, 16, 21, 22, 27, 32, 35, 39, 41, 42\}$
$\mathbb{Z}_{47}*$	All elements in $\mathbb{Z}_{47}$

Table A.4: Cubic residues for $\mathbb{Z}_{11}^*$ to $\mathbb{Z}_{47}^*$

A.2 4th-Power Residues

The 4th power residues in $\mathbb{Z}_p^*$ for a prime p and with $9 \leq p < 50$ are listed in the following table

Group	4th-power residues
$\mathbb{Z}_{11}*$	$\{1, 3, 4, 5, 9\}$
$\mathbb{Z}_{13}*$	$\{1, 3, 9\}$
$\mathbb{Z}_{17}*$	$\{1, 4, 13, 16\}$
$\mathbb{Z}_{19}*$	$\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$
$\mathbb{Z}_{23}*$	$\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$
$\mathbb{Z}_{29}*$	$\{1, 7, 16, 20, 23, 24, 25\}$
$\mathbb{Z}_{31}*$	$\{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\}$
$\mathbb{Z}_{37}*$	$\{1, 7, 9, 10, 12, 16, 26, 33, 34\}$
$\mathbb{Z}_{41}*$	$\{1, 4, 10, 16, 18, 23, 25, 31, 37, 40\}$
$\mathbb{Z}_{43}*$	$\{1, 4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23, 24, 25, 31, 35, 36, 38, 40, 41\}$
$\mathbb{Z}_{47}*$	$\{1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42\}$

Table A.5: 4th-power residues for $\mathbb{Z}_{11}^*$ to $\mathbb{Z}_{47}^*$

A.3 5th Power Residues

The 5th power residues in $\mathbb{Z}_p^*$ for a prime p and with $11 \leq p < 50$ are listed in the following table

Group	5th-power residues
$\mathbb{Z}_{11}*$	$\{1, 10\}$
$\mathbb{Z}_{13}*$	All elements in $\mathbb{Z}_{13}^*$
$\mathbb{Z}_{17}*$	All elements in $\mathbb{Z}_{17}^*$
$\mathbb{Z}_{19}*$	All elements in $\mathbb{Z}_{19}^*$
$\mathbb{Z}_{23}*$	All elements in $\mathbb{Z}_{23}^*$
$\mathbb{Z}_{29}*$	All elements in $\mathbb{Z}_{29}^*$
$\mathbb{Z}_{31}*$	$\{1, 5, 6, 25, 26, 30\}$
$\mathbb{Z}_{37}*$	All elements in $\mathbb{Z}_{37}^*$
$\mathbb{Z}_{41}*$	$\{1, 3, 9, 14, 27, 32, 38, 40\}$
$\mathbb{Z}_{43}*$	All elements in $\mathbb{Z}_{43}^*$
$\mathbb{Z}_{47}*$	All elements in $\mathbb{Z}_{47}^*$

Table A.6: 5th-power residues for $\mathbb{Z}_{11}^*$ to $\mathbb{Z}_{47}^*$

A.4 6th-Power Residues

The 6th power residues in $\mathbb{Z}_p^*$ for a prime p and with $13 \leq p < 50$ are listed in the following table

Group	6th-power residues
$\mathbb{Z}_{13}*$	$\{1, 12\}$
$\mathbb{Z}_{17}*$	$\{1, 2, 4, 8, 9, 13, 15, 16\}$
$\mathbb{Z}_{19}*$	$\{1, 7, 11\}$
$\mathbb{Z}_{23}*$	$\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$
$\mathbb{Z}_{29}*$	$\{1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28\}$
$\mathbb{Z}_{31}*$	$\{1, 2, 4, 8, 16\}$
$\mathbb{Z}_{37}*$	$\{1, 10, 11, 26, 27, 36\}$
$\mathbb{Z}_{41}*$	$\{1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40\}$
$\mathbb{Z}_{43}*$	$\{1, 4, 11, 16, 21, 35, 41\}$
$\mathbb{Z}_{47}*$	$\{1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42\}$

Table A.7: 6th-power residues for $\mathbb{Z}_{13}^*$ to $\mathbb{Z}_{47}^*$

A.5 7th Power Residues

The 7th power residues in $\mathbb{Z}_p^*$ for a prime p and with $15 \leq p < 50$ are listed in the following tables

Group	7th-power residues
$\mathbb{Z}_{17}*$	All elements in $\mathbb{Z}_{17}^*$
$\mathbb{Z}_{19}*$	All elements in $\mathbb{Z}_{19}^*$
$\mathbb{Z}_{23}*$	All elements in $\mathbb{Z}_{23}^*$
$\mathbb{Z}_{29}*$	$\{1, 12, 17, 28\}$
$\mathbb{Z}_{31}*$	All elements in $\mathbb{Z}_{31}^*$
$\mathbb{Z}_{37}*$	All elements in $\mathbb{Z}_{37}^*$
$\mathbb{Z}_{41}*$	All elements in $\mathbb{Z}_{41}^*$
$\mathbb{Z}_{43}*$	$\{1, 6, 7, 36, 37, 42\}$
$\mathbb{Z}_{47}*$	All elements in $\mathbb{Z}_{47}^*$

Table A.8: 7th-power residues for $\mathbb{Z}_{17}^*$ to $\mathbb{Z}_{47}^*$

A.6 8th Power Residues

The 8th power residues in $\mathbb{Z}_p^*$ for a prime p and with $17 \leq p < 50$ are listed in the following table.

Group	8th-power residues
$\mathbb{Z}_{17}*$	$\{1, 16\}$
$\mathbb{Z}_{19}*$	$\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$
$\mathbb{Z}_{23}*$	$\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$
$\mathbb{Z}_{29}*$	$\{1, 7, 16, 20, 23, 24, 25\}$
$\mathbb{Z}_{31}*$	$\{1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28\}$
$\mathbb{Z}_{37}*$	$\{1, 7, 9, 10, 12, 16, 26, 33, 34\}$
$\mathbb{Z}_{41}*$	$\{1, 10, 16, 18, 37\}$
$\mathbb{Z}_{43}*$	$\{1, 4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23, 24, 25, 31, 35, 36, 38, 40, 41\}$
$\mathbb{Z}_{47}*$	$\{1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42\}$

Table A.9: 8th-power residues for $\mathbb{Z}_{17}^*$ to $\mathbb{Z}_{47}^*$

A.7 9th Power Residues

The 9th power residues in $\mathbb{Z}_p^*$ for a prime p and with $19 \leq p < 50$ are listed in the following table.

Group	9th-power residues
$\mathbb{Z}_{19}*$	$\{1, 18\}$
$\mathbb{Z}_{23}*$	All elements in $\mathbb{Z}_{23}^*$
$\mathbb{Z}_{29}*$	All elements in $\mathbb{Z}_{29}$
$\mathbb{Z}_{31}*$	$\{1, 2, 4, 8, 15, 16, 23, 27, 29, 30\}$
$\mathbb{Z}_{37}*$	$\{1, 6, 31, 36\}$
$\mathbb{Z}_{41}*$	All elements in $\mathbb{Z}_{41}^*$
$\mathbb{Z}_{43}*$	$\{1, 2, 4, 8, 11, 16, 21, 22, 27, 32, 35, 39, 41, 42\}$
$\mathbb{Z}_{47}*$	All elements in $\mathbb{Z}_{47}^*$

Table A.10: 9th-power residues for $\mathbb{Z}_{19}^*$ to $\mathbb{Z}_{47}^*$

A.8 10th power residues

The 10th power residues in $\mathbb{Z}_p^*$ for a prime p and with $21 \leq p < 50$ are listed in the following table.

Group	10th-power residues
$\mathbb{Z}_{19}*$	$\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$
$\mathbb{Z}_{29}*$	$\{1, 4, 5, 6, 7, 9, 16, 20, 22, 23, 24, 25, 28\}$
$\mathbb{Z}_{31}*$	$\{1, 5, 25\}$
$\mathbb{Z}_{37}*$	$\{1, 3, 4, 7, 9, 10, 11, 12, 25, 26, 27, 28, 30, 33, 34, 36\}$
$\mathbb{Z}_{41}*$	$\{1, 9, 32, 40\}$
$\mathbb{Z}_{43}*$	$\{1, 4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23, 24, 25, 31, 35, 36, 38, 40, 41\}$
$\mathbb{Z}_{47}*$	$\{1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42\}$

Table A.11: 10th-power residues for $\mathbb{Z}_{19}^*$ to $\mathbb{Z}_{47}^*$

APPENDIX B

Solutions to $x^n + y^n \equiv z^n \pmod{p}$

B.1 Examples of solutions when $n = 3$

Table B.1: Solutions to Equation (1.2) in $\mathbb{Z}_3^*$

x^3+	$y^3 \equiv$	$z^3 \pmod 3$
1	1	2
2	2	1

Table B.2: Solutions to Equation (1.2) in $\mathbb{Z}_5^*$

x^3+	$y^3 \equiv$	$z^3 \pmod 5$
1	1	2
1	3	4
1	2	3
3	1	4
3	3	1
3	4	2
2	1	3
2	2	4
2	4	1
4	3	2
4	2	1
4	4	3

Table B.3: Solutions to Equation (1.2) in $\mathbb{Z}_7^*$

No solutions

B.2 Number of solutions to $x^n + y^n \equiv z^n \pmod{p}$

p \ n	3	4	5	6	7	8	9	10
3	2	-	-	-	-	-	-	-
5	12	-	-	-	-	-	-	-
7	0	-	-	-	-	-	-	-
11	90	10	0	-	-	-	-	-
13	0	0	132	0	-	-	-	-
17	240	0	240	24	240	0	-	-
19	12	36	306	0	306	36	0	-
23	462	55	462	55	462	55	462	55
29	756	14	756	84	0	14	756	84
31	30	105	12	5	870	105	30	0
37	24	18	1260	12	1260	18	0	144
41	1560	0	0	182	1560	0	1560	0
43	42	210	1722	0	12	210	42	210
47	2070	253	2070	253	2070	253	2070	253

Table B.4: Number of solutions to Equation (1.2) for certain p and n when $x, y, z \neq 0$.

References

[Bri20] Britannica. 'Fermat's last theorem'. In: *Encyclopædia Britannica* (2020).

[Fra03] Fraleigh, J. B. *A First Course In Abstract Algebra*. Pearson Education, 2003.

[LeV77] LeVeque, W. J. *Fundamentals of Number Theory*. Dover Publications, 1977.