Utrecht University

Bachelor Thesis

Flat cyclotomic polynomials

Victor de Vries

supervised by

Dr. Lola Thompson

Abstract

In this thesis we study cyclotomic polynomial polynomials with only -1, 0 and 1 as its coefficients, which are called 'flat cyclotomic polynomials'. We prove that every cyclotomic polynomial of order two is flat. We also give an infinite family of flat cyclotomic polynomials of order three and we give a criterion for the height of cyclotomic polynomials of order three. Lastly, we prove that there exist infinitely many flat cyclotomic polynomials of order four and give a weaker criterion for the heights of general cyclotomic polynomials.

Aknowledgements

I would like to thank my supervisor Dr. Lola Thompsons for introducing me to this topic and for giving me constructive feedback and ideas during our meetings. I also very much appreciated that she engouraged me to investigate some things by myself rather than looking them up. I would also like to thank my family and Eeke Hoogenboom for supporting me in my studies.

Contents

Introduction

The n^{th} cyclotomic polynomial, $\Phi_n(x)$, is the monic polynomial whose roots are the primitive n^{th} roots of unity. An equivalent definition for the n^{th} cyclotomic polynomial is: The n^{th} cyclotomic polynomial is the irreducible and monic divisor of x^n-1 in $\mathbb{Q}[X]$, that has degree $\varphi(n)$. Cyclotomic polynomials are important in Galois theory since they are the minimal polynomials of cyclotomic extensions. These are given by adjoining a primitive n^{th} root of unity to $\mathbb{Q}$.

Cyclotomic polynomials have been subject of study at least as far back as 1798. In that year Carl Friedrich Gauss wrote his 'Disquisitiones Arithmeticae', in which the last chapter is about cyclotomic polynomials. A cyclotomic polynomial is called flat if all of its coefficients are from the set $\{-1, 0, 1\}$. As it turns out, not all cyclotomic polynomials are flat. In fact, for any $m \in \mathbb{Z}$ there exists $n \in \mathbb{N}$ such that $\Phi_n(x)$ has m as one of its coefficients which was proved by Suzuki [9]. The amount of odd prime divisors of n is of such importance when studying $\Phi_n(x)$, that it has become convention to say: If n has k odd prime divisors, $\Phi_n(x)$ is of order k. A lot of papers have been written about the growth of the 'height' of cyclotomic polynomials as n increases. The 'height' of $\Phi_n(x)$ is the largest absolute value of the coefficients of $\Phi_n(x)$, denoted $A(n)$. Bateman, Pomerance and Vaughn [2] proved in 1984 that $A(n) \leq n^{\frac{2^{k-1}}{k}-1}$ where k is the order of $\Phi_n(x)$. Maier [8] showed that given any functions from the natural numbers $\psi(n) > 0$ and $\epsilon(n) > 0$ satisfying $\lim_{n\to\infty} \psi(n) = \infty$ and $\lim_{n\to\infty} \epsilon(n) = 0$, the bounds $n^{\epsilon(n)} \leq A(n) \leq n^{\psi(n)}$ hold for almost all n.

In this thesis we study flat cyclotomic polynomials. In 1883 Migotti proved that all cyclotomic polynomials of order two are flat. Gennady Bachman [1] proved in 2006 that an infinite family of cyclotomic poylnomials of order three exist. He proved that for a prime $5 < p$, there exist infinitely many pairs of primes (q, r) such that $\Phi_{pqr}(x)$ is flat. Kaplan [5] later improved this by proving that for any primes p and q, there exist infinitely many primes r such that $\Phi_{pqr}(x)$ is flat. Kaplan was also the first one to prove that there are infinitely many cyclotomic polynomials of order four [6]. Flat cyclotomic polynomials seem to get sparser as their order increases. As an example, computations of Arnold and Monagan showed that there only exist 1389 square-free integers n with four odd prime divisors that generate flat $\Phi_n(x)$ for $n < 3 \cdot 10^8$. No flat cyclotomic polynomials of order five have been found yet and it is conjectured that none exist.

In Chapter 1 we define introduce the n^{th} cyclotomic polynomial in more detail and we give some of the properties that $\Phi_n(x)$ has for general n. In Chapter 2 we define the 'height' and 'order' of a cyclotomic polynomial. We show that the height of $\Phi_n(x)$ only depends on

the odd prime factors of n and we prove that all cyclotomic polynomials of order two are flat. Our proof for this is based on the proof given by Lam and Lueng [7]. In Chapter 3 we look at cyclotomic polynomials of order three. In this chapter we prove that if $r \equiv \pm 1 \pmod{pq}$ for odd primes $p < q < r$, $\Phi_{pqr}(x)$ is flat. We also show that if $r \equiv \pm s \pmod{pq}$ for odd primes $p < q < r, s$, we have $A(pqr) = A(qps)$. For proving both these results, we follow the approach taken by Kaplan [5]. In the final Chapter we prove that the set of coefficients of $\Phi_{ns}(x)$ and $\Phi_{nt}(x)$ are the same if s and t are primes that satisfy some relation. We will use this result to show that there exist infinitely many flat cyclotomic polynomials of order four. Again we follow the approach first taken by Kaplan [6].

Notation

Some of the sets that are used in this thesis are:

- $\mathbb{N}$, the natural numbers $\{1, 2, ...\}$
- $\mathbb{N}_0$, the natural numbers and 0, $\{0, 1, 2, ...\}$
- $\mathbb{Z}$, the whole numbers $\{..., -1, 0, 1, ...\}$
- $\mathbb{Z}_n$, the residue classes of division by n, $\{[0], [1], ..., [n-1]\}$
- $\mathbb{C}$, the complex numbers $\{a + bi \,|\, a, b \in \mathbb{R}\}$
- $\mathbb{Z}[X]$, the polynomials with coefficients in $\mathbb{Z}$, $\{\sum_{k=0}^{N} a_k x^k \,|\, a_k \in \mathbb{Z},\ N \in \mathbb{N}_0\}$

$a|b$, 'There exists $k \in \mathbb{Z}$ such that $ak = b$'
$a \nmid b$, 'There does not exist $k \in \mathbb{Z}$ such that $ak = b$'
$\gcd(a, b)$ 'the largest number in $\mathbb{N}$ that divides both a and b'
In this document the set $\{d|n\}$ is sometimes used, where n is a natural number, to denote the set of all **positive** divisors of n.

As '|' is used for 'divides', we use '#' for the cardinality of sets e.g. $\#\{p\} = 1$.

With φ we denote the Euler totient function.
$\varphi : \mathbb{N} \to \mathbb{N} \quad n \mapsto \#\{1 \leq k \leq n \,|\, \gcd(k, n) = 1\}$
With τ, we denote the 'tau function'.
$\tau : \mathbb{N} \to \mathbb{N} \quad n \mapsto \#\{d|n\}$

For two whole numbers $a < b$ we denote $[a, b] = \{k \in \mathbb{Z} \,|\, a \leq k \leq b\}$ and
$]a, b[= \{k \in \mathbb{Z} \,|\, a < k < b\}$. There should not be any confusion about this having the same notation as the interval of real numbers, as it is not mentioned in this thesis.

Generally we use p to denote a prime number. If no further context is given, one can assume that p is meant to represent a prime.

Chapter 1

Background on cyclotomic polynomials

In section 1.1 we define cyclotomic polynomials by looking at their roots. In section 1.2 we look at some general properties of cyclotomic polynomials.

1.1 Roots of unity

In this section we introduce the n^{th} roots of unity, which we use to define the n^{th} cyclotomic polynomial.

Definition 1.1.1. *Given $n \in \mathbb{N}$. A complex number z is called an **n^{th} root of unity** if and only if it satisfies $z^n = 1$.*

As the polynomial $z^n - 1$ has exactly n roots in $\mathbb{C}$, by the Fundamental Theorem of Algebra, there are exactly n distinct n^{th} roots of unity. All the elements of $\{e^{\frac{2\pi ik}{n}} | 1 \leq k \leq n\}$ satisfy $z^n = 1$, therefore the n^{th} roots of unity are exactly the set $\{e^{\frac{2\pi ik}{n}} \,|\, 1 \leq k \leq n\}$.

Proposition 1.1.2. *The n^{th} roots of unity form a group under multiplication.*

Proof. For any z, z', which are roots of unity we have $(z \cdot z')^n = z^n \cdot z'^n = 1$, so the n^{th} roots of unity are closed under multiplication. The unique identity in $\mathbb{C} \setminus \{0\}$ with multiplication is 1. Since 1 is an n^{th} root of unity it is the unique identity of the n^{th} roots of unity. Since multiplication in $\mathbb{C}$ is associative, the multiplication of the n^{th} roots of unity is also associative. Each element in $\mathbb{C} \setminus \{0\}$ with multiplication has a unique inverse z^{-1}. For an n^{th} root of unity z we have $(z^{-1})^n = (z^n)^{-1} = 1$, so every element has an inverse. We conclude that the n^{th} roots of unity form a group under multiplication. □

The group formed by the n^{th} roots of unity is isomorphic to a familiar group.

Proposition 1.1.3. *The group of n^{th} roots of unity is isomorphic to $(\mathbb{Z}_n, +)$.*

Proof. Consider the map $\psi : \mathbb{Z}_n \to \{e^{\frac{k}{n}2\pi i} | \, 1 \leq k \leq n\}$ $\psi([k]) = e^{\frac{k}{n}2\pi i}$. Suppose that $k, k' \in [k]$, then $k' = k + tn$ with $t \in \mathbb{Z}$, therefore $\psi([k']) = e^{\frac{k+tn}{n}2\pi i} = e^{\frac{k}{n}2\pi i} = \psi([k])$. This means that ψ is well-defined since $\psi([k])$ does not depend on the representative of $[k]$.
We have $\psi([k+k']) = e^{\frac{k+k'}{n}2\pi i} = e^{\frac{k}{n}2\pi i} \cdot e^{\frac{k'}{n}2\pi i} = \psi([k]) \cdot \psi([k'])$, therefore ψ is a homomorphism.
For $\zeta = e^{\frac{k}{n}2\pi i}$ we have $\psi([k]) = \zeta$ therefore ψ is surjective.
For $[k] \neq [k']$ we get $\psi([k]) = e^{\frac{k}{n}2\pi i} \neq e^{\frac{k'}{n}2\pi i} = \psi([k'])$ therefore ψ is injective.
Since ψ is a bijective homomorphism it is an isomorphism between $(\mathbb{Z}_n, +)$ and the group of n^{th} roots of unity. □

Definition 1.1.4. *An n^{th} root of unity ζ_n is called a **primitive n^{th} root of unity** or shorthand **primitive** if the order of ζ_n is n.*

Since the elements in $\mathbb{Z}_n$ with order n are the elements $\{[k] \in \mathbb{Z}_n | \gcd(k, n) = 1\}$, the primitive n^{th} roots of unity are the set $\{e^{\frac{k2\pi i}{n}} | 1 \leq k \leq n \quad \gcd(k, n) = 1\}$.

Proposition 1.1.5. *For a primitive n^{th} root of unity ζ_n we have $x^n - 1 = \prod_{k=1}^{n}(x - \zeta_n^k)$.*

Proof. Since the order of ζ_n is n, the set $\{\zeta_n^k | \, 1 \leq k \leq n\}$ is exactly the set of n^{th} roots of unity. The n^{th} roots of unity are exactly the set of zeros of $x^n - 1$. Therefore by the Fundamental Theorem of Algebra we can write $x^n - 1 = C \cdot \prod_{k=1}^{n}(x - \zeta_n^k)$. The highest order term of the right hand side is x^n, therefore $C = 1$. □

Using the primitive n^{th} roots of unity we define the n^{th} cyclotomic polynomial.

Definition 1.1.6. *The **n^{th} cyclotomic polynomial** is the monic polynomial whose roots are the primitive n^{th} roots of unity.*
It is denoted by $\Phi_n(x) := \prod_{\substack{1 \leq k \leq n \\ gcd(k,n)=1}} (x - \zeta_n^k)$, where $\zeta_n = e^{\frac{2\pi i}{n}}$.

It follows that the degree of $\Phi_n(x)$ is easy to compute.

Corollary 1.1.7. *The degree of $\Phi_n(x)$ is $\varphi(n)$.*

Proof. The degree of $(x - \zeta_n^k)$ is 1 for all k.
Therefore we get $\deg(\Phi_n) = \sum_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} 1 = \#\{1 \leq k \leq n | \gcd(k, n) = 1\} = \varphi(n)$. □

Now that we have defined the n^{th} cyclotomic polynomial and we know its degree, we are going to prove a theorem which relates some of them.

Theorem 1.1.8. *Let $\Phi_d(x)$ denote the d^{th} cyclotomic polynomial. It holds that* $\prod_{d|n} \Phi_d(x) = x^n - 1$.

Proof. By definition 1.1.6 we have $\prod_{d|n} \Phi_d(x) = \prod_{d|n}(\prod_{\substack{1\leq k\leq d \\ \gcd(k,d)=1}} (x - e^{\frac{k2\pi i}{d}}))$.

Consider the set $S := \{\frac{k}{d} |\, d|n \quad k \in [1,d] \quad \gcd(k,d) = 1\}$.

If we have $\frac{k}{d} = \frac{k'}{d'}$, then $kd' = k'd$. Since $\gcd(k',d') = 1$ we get $k'|k$ by the fundamental lemma and we get $k|k'$, as $\gcd(k,d) = 1$. This implies $k = k'$ and therefore we get $(k,d) = (k',d')$. Now consider the set $T := \{(k,d) |\, d|n \quad k \in [1,d] \quad \gcd(k,d) = 1\}$. By the previous reasoning S corresponds one-to-one with T via the map $(k,d) \mapsto \frac{k}{d}$. The cardinality of T is $\sum_{d|n} \varphi(d)$. A well known theorem in number theory is $\sum_{d|n} \varphi(d) = n$, therefore $\#T = n$. Since all elements of S can be written in the form $\frac{a}{n}$ with $1 \leq a \leq n$ and S has exactly n elements, we conclude that $S = \{\frac{a}{n} |\, 1 \leq a \leq n\}$.

Using the previous observations we get $\prod_{d|n} \Phi_d(x) = \prod_{\substack{d|n \\ 1\leq k\leq d \\ \gcd(k,d)=1}} (x - e^{\frac{2\pi ik}{d}}) = \prod_{\frac{k}{d}\in S} (x - e^{\frac{k}{d}2\pi i}) = \prod_{1\leq a\leq n} (x - e^{\frac{a}{n}2\pi i})$, which equals $x^n - 1$ by the Fundamental Theorem of Algebra. □

This theorem is quite handy, as it yields $\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\, d\neq n} \Phi_d(x)}$, which allows us to compute $\Phi_n(x)$ for a positive integer n. Computing $\Phi_n(x)$ is quite easy now for small n.

Example 1.1.9. The first twelve cyclotomic polynomials are:

$\Phi_1(x) = x - e^{2\pi i} = x - 1$

$\Phi_2(x) = \frac{x^2 - 1}{x - 1} = x + 1$

$\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1$

$\Phi_4(x) = \frac{x^4 - 1}{(x-1)(x+1)} = x^2 + 1$

$\Phi_5(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1$

$\Phi_6(x) = \frac{x^6 - 1}{(x^2+x+1)(x-1)(x+1)} = \frac{x^4 + x^2 + 1}{x^2 + x + 1} = x^2 - x + 1$

$\Phi_7(x) = \frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

$$\Phi_8(x) = \frac{x^8-1}{(x^2+1)(x+1)(x-1)} = \frac{x^8-1}{x^4-1} = x^4+1$$
$$\Phi_9(x) = \frac{x^9-1}{(x^2+x+1)(x-1)} = \frac{x^9-1}{x^3-1} = x^6+x^3+1$$
$$\Phi_{10}(x) = \frac{x^{10}-1}{(x^4+x^3+x^2+x+1)(x+1)(x-1)} = \frac{x^5+1}{x+1} = x^4-x^3+x^2-x+1$$
$$\Phi_{11}(x) = \frac{x^{11}-1}{x-1} = x^{10}+x^9+x^9+x^7+x^6+x^5+x^4+x^3+x^2+x+1$$
$$\Phi_{12}(x) = \frac{x^{12}-1}{(x^2-x+1)(x^2+1)(x^2+x+1)(x+1)(x-1)} = \frac{x^8+x^4+1}{x^4+x^2+1} = x^4-x^2+1$$

When we look at the degrees of these, we see that we have for instance $\deg(\Phi_{10}(x)) = 4$, $\deg(\Phi_{11}(x)) = 10$ and $\deg(\Phi_6(x)) = 2$. This is consistent with $\varphi(10) = \varphi(5)\varphi(2) = 4$, $\varphi(11) = 10$, $\varphi(6) = \varphi(3)\varphi(2) = 2$.

These give rise to some interesting questions. One of them is: Is $\Phi_n(x) \in \mathbb{Z}[X]$ for all n? One could ask if an even stronger condition is true namely: Are -1, 0 and 1 the only possible coefficients for $\Phi_n(x)$. The reader is advised to look at these examples and see if they can come up with other conjectures about how $\Phi_n(x)$ behaves. We will leave the question about the coefficients only being -1, 0 or 1 for the next chapter. In the next section we prove some general properties of cyclotomic polynomials.

1.2 General properties of cyclotomic polynomials

Now that we have defined what the n^{th} cyclotomic polynomial is, we are going to study some of its properties. In particular, Theorem 1.1.8 will be useful for deriving some of the upcoming results. Another tool that is used frequently for proving the upcoming theorems is the well-ordering principle, which is equivalent to mathematical induction.

For any prime p and $k \in \mathbb{N}$, we can give an explicit formula for $\Phi_{p^k}(x)$.

Proposition 1.2.1. *If p is a prime and $k \in \mathbb{N}$, then $\Phi_{p^k}(x) = \sum_{m=0}^{p-1} x^{p^{k-1}m}$.*

Proof. The set $\{d|n\}$ for $n = p^k$ is $\{p^a | \, 0 \le a \le k\}$.
By using Theorem 1.1.8 we get $\Phi_{p^k}(x) = \dfrac{x^{p^k}-1}{\prod_{a=0}^{k-1}\Phi_{p^a}(x)} = \dfrac{x^{p^k}-1}{x^{p^{k-1}}-1} = \sum_{m=0}^{p-1} x^{p^{k-1}m}$. □

So if n only has one prime divisor, $\Phi_n(x)$ behaves quite nicely. In the next two theorems we look at the constant term of $\Phi_n(x)$ and the sum of coefficients of $\Phi_n(x)$.

Theorem 1.2.2. *The constant term of $\Phi_n(x)$ is given by* $\Phi_n(0) = \begin{cases} -1 \text{ if } n = 1, \\ 1 \text{ if } n > 1. \end{cases}$

Proof. Notice that the $n = 1$ case is correct.
Let $S = \{n > 1 |\, \Phi_n(0) \neq 1\}$. Suppose that S is nonempty. Note that $2 \notin S$. By the well ordering principle S has a least element l. All $d|l$ with $d \neq l, 1$ are not in S and are greater then 1, therefore $\Phi_d(0) = 1$ for those d.

By Theorem 1.1.8 we have $\Phi_l(0) = \dfrac{0^l - 1}{\prod_{d|l,\, d\neq l,1} \Phi_d(0) \cdot \Phi_1(0)} = \dfrac{-1}{-1} = 1$. Therefore we have $l \notin S$. Since S does not have a least element, S must be empty. This means that we get $\Phi_n(0) = \begin{cases} -1 \text{ if } n = 1, \\ 1 \text{ if } n > 1. \end{cases}$ □

Now we are going to give a formula for the sum of the coefficients, $\Phi_n(1)$.

Theorem 1.2.3. *The sum of coefficients of $\Phi_n(x)$, $\Phi_n(1)$, is given by*
$\Phi_n(1) = \begin{cases} 0 \text{ if } n = 1 \\ p \text{ if } n = p^k \text{ with } k \in \mathbb{N} \text{ and } p \text{ prime }, \\ 1 \text{ if } p_1|n \text{ and } p_2|n \text{ with } p_1 \neq p_2 \text{ primes.} \end{cases}$

Proof. Note that the $n = 1$ case is correct and by Proposition 1.2.1, the $n = p^k$ case is correct. We are now going to prove that for all n with multiple distinct prime divisors $\Phi_n(1) = 1$.
We define $S = \{n \in \mathbb{N} |\ p_1|n, p_2|n$ with $p_1 \neq p_2$ primes and $\Phi_n(1) \neq 1\}$. Since it is true that $\Phi_6(x) = x^2 - x + 1$, we have $6 \notin S$. Suppose that S is nonempty, then there is a least element $l \in S$. We can write l in its canonical prime factorization: $l = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$.

Because we have $\prod_{d|l} \Phi_d(x) = x^l - 1$, we also have $\Phi_l(x) \cdot \prod_{d|l,\, d\neq 1,l} \Phi_d(x) = \sum_{i=1}^{l} x^{l-i}$. Splitting up the divisors of l in those of the form p^k, where p is a prime and those not of this form yields $\Phi_l(x) \cdot \prod_{p^k|l} \Phi_{p^k}(x) \cdot \prod_{d|l,\, d\neq 1,l,p^k} \Phi_d(x) = \sum_{i=1}^{l} x^{l-i}$. For all $d \in \{d|l \quad d \neq 1, l, p^k\}$ we have $d \in \{n \in \mathbb{N} |\quad p_1, p_2|n$ with $p_1 \neq p_2$ primes$\}$; however we have $d \notin S$ since $d < l$. Therefore we have $\Phi_d(1) = 1$ for all such d. As earlier mentioned we have $\Phi_d(1) = p$ for $d = p^k$.

We get $\Phi_l(1) \cdot \prod_{p^k|l} \Phi_{p^k}(1) \cdot \prod_{d|l,\, d\neq 1,l,p^k} \Phi_d(1) = \sum_{i=1}^{l} 1^{l-i}$, which implies $\Phi_l(1) \cdot \prod_{p^k|l} p = l$. Therefore we get $\Phi_l(1) \cdot p_1^{e_1} \cdot \ldots \cdot p_n^{e_n} = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$. This mean that $\Phi_l(1) = 1$ and therefore $l \notin S$.

Since $l \notin S$, S does not contain its least element, which contradicts the well orderings principle, therefore S must be empty. This means that for all n that have distinct prime

divisors, we have $\Phi_n(1) = 1$. We conclude that $\Phi_n(1) = \begin{cases} 0 \text{ for } n = 1 \\ p \text{ for } n = p^k, \\ 1 \text{ for } p_1, p_2 | n. \end{cases}$ □

Now that we have studied how the constant term and the sum of the coefficients behave, we are going to prove that $\Phi_n(x)$ only has integer coefficients. For proving this we are going to use the formula for the constant term.

Theorem 1.2.4. *For all $n \in \mathbb{N}$ we have $\Phi_n(x) \in \mathbb{Z}[X]$.*

Proof. We define $S = \{n \in \mathbb{N} | \, \Phi_n(x) \notin \mathbb{Z}[X]\}$. Suppose that S is nonempty. Then S must have some least element l. Note that $1 \notin S$ since $\Phi_1(x) = x - 1$. We have a cyclotomic polynomial $\Phi_l(x) = \sum_{k=0}^{\varphi(l)} a_k x^k \notin \mathbb{Z}[X]$. Now we define $T := \{k \in \mathbb{N}_0 | \, a_k \notin \mathbb{Z}\}$. Since we have $T \subset \mathbb{N}_0$ and T is nonempty by assumption, T has a least element j. This is not 0, as the constant term a_0 is an integer by Theorem 1.2.2.

Note that all the divisors d of l except l are not in S. This means that $\Phi_d(x) \in \mathbb{Z}[X]$ for $d|l$ with $d \neq l$. Therefore the product $\prod_{d|l,\, d\neq l} \Phi_d(x)$ is also in $\mathbb{Z}[X]$. Since $\Phi_l(x)$ is a polynomial of degree $\varphi(l)$ and since $\Phi_l(x) \cdot \prod_{d|l,\, d\neq l} \Phi_d(x) = x^l - 1$, $\prod_{d|l,\, d\neq l} \Phi_d(x)$ is a polynomial of degree $l - \varphi(l)$. Therefore we can write $\prod_{d|l,\, d\neq l} \Phi_d(x) = \sum_{k=0}^{l-\varphi(l)} b_k x^k$ with $b_k \in \mathbb{Z}$ for all k.

Since $x^l - 1 \in \mathbb{Z}[X]$, we can write $x^l - 1 = \sum_{k=0}^{l} c_k x^k$ with $c_k \in \mathbb{Z}$. Note that c_j is given by $c_j = \sum_{k+i=j} a_i b_k$ and therefore we get $-a_j b_0 = \sum_{\substack{k+i=j \\ k<j}} a_i b_k - c_j$. Since b_0 is the constant term of $\prod_{d|l,\, d\neq l} \Phi_d(x)$, b_0 must be -1 by Theorem 1.2.2. Therefore we get $a_j = \sum_{\substack{k+i=j \\ k<j}} a_i b_k - c_j \in \mathbb{Z}$. This is because for all $k < j$, we have $b_k \in \mathbb{Z}$ by construction of j and T. We get $j \notin T$, so T does not contain its least element, therefore it must be empty. But this means that $\Phi_l(x) \in \mathbb{Z}[X]$ and therefore $l \notin S$, so S does not contain its least element. We conclude that S must be empty and therefore $\Phi_n(x) \in \mathbb{Z}[X]$ for all $n \in \mathbb{N}$. □

Now that we have proven that $\Phi_n(x)$ has integer coefficients for all n, we would like to prove that $\Phi_n(x)$ is symmetric for all $n \geq 2$. A polynomial $\sum_{k=0}^{N} a_k x^k$ with degree N is called symmetric if $a_k = a_{N-k}$ for all k. We first prove a lemma for general symmetric polynomials.

Lemma 1.2.5. *Let $f(x)$ be a symmetric polynomial and let $g(x)$ and $h(x)$ be polynomials such that $f(x) \cdot g(x) = h(x)$. Then $h(x)$ is symmetric if and only if $g(x)$ is symmetric.*

Proof. We write $f(x) = \sum_{m=0}^{M} a_m x^m$, $g(x) = \sum_{n=0}^{N} b_n x^n$ and $h(x) = \sum_{k=0}^{M+N} c_k x^k$.
Suppose $g(x)$ is symmetric. Then for any k we have $c_k = \sum_{m+n=k} a_m b_n = \sum_{m+n=k} a_{M-m} b_{N-n} = \sum_{i+j=(M+N)-k} a_i b_j = c_{(M+N)-k}$. This means that $h(x)$ is symmetric.

Now suppose that $h(x)$ is symmetric. We are going to prove that $g(x)$ is symmetric by induction on its coefficients. For b_0 of $g(x)$ we have $a_0 \cdot b_0 = c_0 = c_{M+N} = a_M \cdot b_N$ and since $f(x)$ is symmetric we get $a_0 \cdot b_0 = a_0 \cdot b_N$, which means that $b_0 = b_N$.

Suppose that for n up to $k < \frac{N}{2}$ we have $b_n = b_{N-n}$. We have $\sum_{m+n=k+1} a_m b_n = c_{k+1} = c_{(M+N-(k+1))} = \sum_{i+j=M+N-(k+1)} a_i b_j = \sum_{m+n=k+1} a_{M-m} b_{N-n}$. Now we use that $f(x)$ is symmetric and that for $n \leq k$, $b_{N-n} = b_n$ holds to get $\sum_{m+n=k+1} a_{M-m} b_{N-n} = a_0 b_{N-(k+1)} + \sum_{\substack{m+n=k+1 \\ n<k+1}} a_m b_n$. This is equal to $\sum_{m+n=k+1} a_m b_n$ by the beginning of the paragraph. Cancelling terms yields $b_{N-(k+1)} = b_{k+1}$.

This completes our proof by induction of $g(x)$ being a symmetric polynomial. We conclude that if $f(x)$ is a symmetric polynomial with $f(x) \cdot g(x) = h(x)$, then $h(x)$ is symmetric if and only if $g(x)$ is. □

With the help of this lemma, we prove that $\Phi_n(x)$ is symmetric for all $n \geq 2$.

Proposition 1.2.6. *For all $n \geq 2$, $\Phi_n(x)$ is a symmetric polynomial.*

Proof. We define $S = \{n \geq 2 |\, \Phi_n(x) \text{ is not symmetric}\}$. Suppose that S is nonempty, then it has a least element l. Note that $2 \notin S$ since $\Phi_2(x) = x + 1$. By assumption $\Phi_l(x)$ is non-symmetric.

We have $\prod_{d|l,\, d\neq 1,l} \Phi_d(x) \cdot \Phi_l(x) \cdot \Phi_1(x) = x^l - 1$ and therefore $\prod_{d|l,\, d\neq 1,l} \Phi_d(x) \cdot \Phi_l(x) = \sum_{k=0}^{l-1} x^k$. Since for all $d|l$ with $d \neq 1, l$ we have $1 < d < l$ and therefore $d \in \{n \geq 2\} \setminus S$, which means that $\Phi_d(x)$ is symmetric for those d. By applying Lemma 1.2.5 repeatedly, we see that the product $\prod_{d|l,\, d\neq 1,l} \Phi_d(x)$ is symmetric as well. Since $\sum_{k=0}^{l-1} x^k$ is symmetric, the lemma yields that $\Phi_l(x)$ is symmetric.

This means that $l \notin S$, therefore S must be empty. We conclude that for all $n \geq 2$, $\Phi_n(x)$ is symmetric. □

In the following two theorems we are going to relate $\Phi_{pn}(x)$ to $\Phi_n(x)$ for a prime p. The two important cases are $p|n$ and $p \nmid n$. In the next theorem we look at the case $p \nmid n$ and in the theorem thereafter we look at the case $p|n$.

Theorem 1.2.7. *For any integer n and any prime p, if $p \nmid n$ then $\Phi_n(x) \cdot \Phi_{pn}(x) = \Phi_n(x^p)$.*

Proof. We define $S = \{n \in \mathbb{N} | \exists p \text{ prime s.t. } p \nmid n \text{ and } \Phi_n(x) \cdot \Phi_{pn}(x) \neq \Phi_n(x)\}$. Suppose that S is nonempty, then it has a least element l. Note that $1 \notin S$, as for any prime p we have $\Phi_1(x) \cdot \Phi_p(x) = x^p - 1 = \Phi_1(x^p)$. There exists a prime p such that $p \nmid l$ and $\Phi_l(x) \cdot \Phi_{pl}(x) \neq \Phi_l(x^p)$.

Since $p \nmid l$, we have $\gcd(p, l) = 1$, which, because the τ function is multiplicative, implies that the set of divisors of pl is $p\{d|l\} \sqcup \{d|l\}$. Using Theorem 1.1.8 we get $\prod_{d|pl} \Phi_d(x) = x^{pl} - 1 = (x^p)^l - 1 = \prod_{d|l} \Phi_d(x^p)$. Now using that $\{d|pl\} = \{d|l\} \sqcup p\{d|l\}$ yields $\prod_{d|l} \Phi_d(x) \cdot \Phi_{pd}(x) = \prod_{d|l} \Phi_d(x^p)$. Since for all $d|l$ with $d \neq l$ we have $p \nmid d$ and $d < l$, which implies $d \notin S$, we get $\Phi_d(x) \cdot \Phi_{pd}(x) = \Phi_d(x^p)$ for $d|l$ with $d \neq l$. Therefore we get $\prod_{d|l,\, d\neq l} \Phi_d(x^p) \cdot \Phi_l(x) \cdot \Phi_{pl}(x) = \prod_{d|l} \Phi_d(x^p)$. Cancelling terms yields $\Phi_l(x) \cdot \Phi_{pl}(x) = \Phi_l(x^p)$.

Since p was chosen arbitrarily, we have $\Phi_l(x) \cdot \Phi_{pl}(x) = \Phi_l(x^p)$ for any prime p with $p \nmid l$. Therefore we get $l \notin S$, and thus S does not have a least element, so S must be empty, which means that if $p \nmid n$ we have $\Phi_n(x) \cdot \Phi_{pn}(x) = \Phi_n(x^p)$. □

Now we look at the case where we have a prime p such that $p|n$.

Theorem 1.2.8. *For any integer n and any prime p, if $p|n$ then $\Phi_{pn}(x) = \Phi_n(x^p)$.*

Proof. Let $S = \{n \in \mathbb{N} | \exists p \text{ prime s.t. } p|n,\ \Phi_{pn}(x) \neq \Phi_n(x^p)\}$. Suppose that S is nonempty, then S has has a least element l. Note that $2 \notin S$ since $\Phi_4(x) = \Phi_2(x^2)$. There exists a prime p such that $p|l$ and $\Phi_{pl}(x) \neq \Phi_l(x^p)$.

Since $p|l$, the set of divisors of pl is given by $p\{d|l\} \sqcup \{d|l \text{ s.t. } p \nmid d\}$. We can write this as $p\{d|l \text{ s.t. } p|d\} \sqcup p\{d|l \text{ s.t. } p \nmid d\} \sqcup \{d|l \text{ s.t. } p \nmid d\}$. By Theorem 1.1.8 we have $\prod_{d|pl} \Phi_d(x) = x^{pl} - 1 = \prod_{d|l} \Phi_d(x^p)$. Using the formula for the set $\{d|pl\}$ we obtained, we can write $\prod_{d|pl} \Phi_d(x) = \prod_{d|l,\, p|d} \Phi_{pd}(x) \cdot \prod_{d|l,\, p\nmid d} \Phi_{pd}(x) \cdot \Phi_d(x)$. We can use Theorem 1.2.7 on the right product to get $\prod_{d|pl} \Phi_d(x) = \prod_{d|l,\, p|d} \Phi_d(x) \cdot \prod_{d|l,\, p\nmid d} \Phi_d(x^p)$. Since for all $d|l$ with $p|d$ and $d \neq l$ we have $d \in \{n \in \mathbb{N} \,|\, \exists p \text{ prime s.t. } p|n\} \setminus S$, we get that $\Phi_{pd}(x) = \Phi_d(x^p)$ for those d. Filling this in yields $\prod_{d|pl} \Phi_d(x) = \Phi_{pl}(x) \cdot \prod_{d|l,\, d\neq l,\, p|d} \Phi_d(x^p) \cdot \prod_{d|l,\, p\nmid d} \Phi_d(x^p)$. Therefore we have $\prod_{d|l} \Phi_d(x^p) = \Phi_{pl}(x) \cdot \prod_{d|l,\, d\neq l} \Phi_d(x^p)$. Cancelling terms yields $\Phi_{pl}(x) = \Phi_l(x^p)$.

Since the prime p with $p|l$ was chosen arbitrarily, we get that for any prime p with $p|l$,

we have $\Phi_{pl}(x) = \Phi_l(x^p)$. Therefore we have $l \notin S$, which means that S does not contain its least element, therefore S is empty. We conclude that if $p|n$ then $\Phi_{pn}(x) = \Phi_n(x^p)$. □

One use of this theorem is demonstrated by the following corollary.

Corollary 1.2.9. *Given any integer n written in its canonical form $n = p_1^{e_1} \cdot ... \cdot p_m^{e_m}$. We define $n_0 := p_1 \cdot ... \cdot p_m$ to be the largest square-free factor of n. By applying Theorem 1.2.8 multiple times, we get $\Phi_n(x) = \Phi_{n_0}(x^{\frac{n}{n_0}})$.*

In the next theorem we relate $\Phi_{2n}(x)$ to $\Phi_n(x)$ for odd n, which is a special case of $p \nmid n$. It turns out that if $p = 2$, we get some extra information about $\Phi_{pn}(x)$.

Theorem 1.2.10. *Given an integer n. If $2 \nmid n$, then* $\Phi_{2n}(x) = \begin{cases} -\Phi_n(-x) \text{ if } n = 1, \\ \Phi_n(-x) \text{ if } n > 1. \end{cases}$

Proof. The $n = 1$ case is true, as $\Phi_2(x) = x + 1 = -(-x - 1) = -\Phi_1(-x)$.
Let $S = \{n > 1 \quad 2 \nmid n,\ \Phi_{2n}(x) \neq \Phi_n(-x)\}$. Suppose that S is nonempty, then S has a least element l. For $n = 3$ we have $\Phi_6(x) = x^2 - x + 1 = \Phi_3(-x)$, therefore $3 \notin S$. Because we have $2 \nmid l$, we have $\gcd(2, l) = 1$, which means that the set of divisors of $2l$ is $2\{d|l\} \sqcup \{d|l\}$. Therefore we can write $\prod_{d|l} \Phi_d(x) \cdot \Phi_{2d}(x) = \prod_{d|2l} \Phi_d(x) = x^{2l} - 1 = (x^l + 1)(x^l - 1)$. Since it holds that $\prod_{d|l} \Phi_d(x) = x^l - 1$, we must have $\prod_{d|l} \Phi_{2d}(x) = x^l + 1$. Since l is odd, this implies that $\prod_{d|l} \Phi_{2d}(x) = -((-x)^l - 1)) = -\prod_{d|l} \Phi_d(-x)$.

For all $d|l$ with $d \neq l, 1$ we have $d \in \{n \text{ odd}\} \backslash S$, therefore $\Phi_{2d}(x) = \begin{cases} -\Phi_d(-x) \text{ if } d = 1, \\ \Phi_d(-x) \text{ if } d > 1 \end{cases}$
for all $d|l$ with $d \neq l$. Plugging this in yields that $\Phi_{2l}(x) \cdot -\prod_{d|l,\, d \neq l} \Phi_d(-x) = -\prod_{d|l} \Phi_d(-x)$.
Cancelling terms yields $\Phi_{2l}(x) = \Phi_l(-x)$. Therefore $l \notin S$, so S must be empty, as it contains no least element. We conclude that $\Phi_{2n}(x) = \Phi_n(-x)$ if $2 \nmid n$. □

This concludes the section about general properties of cyclotomic polynomials. The one question that has remained unanswered throughout this section is: Do all cyclotomic polynomials only have coefficients from the set $\{-1, 0, 1\}$? Or one could ask: Which cyclotomic polynomials only have coefficients from this set? Looking at such polynomials will be the main focus of the rest of the thesis.

Chapter 2

Cyclotomic polynomials of order two

In this section, we further explore the coefficients of cyclotomic polynomials. We will pay special attention to the cyclotomic polynomials $\Phi_n(x)$, where n has two distinct odd prime factors.

Definition 2.0.1. *Given a cyclotomic polynomial* $\Phi_n(x) = \sum_{k=0}^{\varphi(n)} a_k x^k$
We define the ***height*** *of* $\Phi_n(x)$ *to be the largest absolute value of its coefficients.*
We denote the height of $\Phi_n(x)$ *by* $A(n) := \max_{0 \leq k \leq \varphi(n)} \{|a_k|\}$

Since the maximal absolute value of the coefficients of $\Phi_n(x)$ is called its height, it makes a lot of sense to call a cyclotomic polynomial with coefficients in $\{-1, 0, 1\}$ 'flat'.

Definition 2.0.2. *A cyclotomic poylnomial is called a* ***flat cyclotomic polynomial*** *or is shorthand called* ***flat*** *if its height is* 1*.*

As mentioned in the introduction, not every cyclotomic polynomial is flat. The first example of a cyclotomic polynomial that has height not equal to 1 is $\Phi_{105}(x)$. We will prove that this is the smallest n for which $\Phi_n(x)$ is not flat in section 2.1.

Proposition 2.0.3. *Not all cyclotomic polynomials are flat.*

Proof. A counterexample is $\Phi_{105}(x) = x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^5 + x^2 + x + 1$, which has height 2. □

As we will see, only for larger n such as 105 can we get non-flat $\Phi_n(x)$. So we might think that for all large n, we get large $A(n)$. This is not true, as for example $A(900) = 1$. We see that only for large n, but not all large n, we get large $A(n)$. This is largely because the height of $\Phi_n(x)$ depends only on the distinct odd prime divisors of n.

Proposition 2.0.4. *The height of a cyclotomic polynomial $\Phi_n(x)$ depends only on the distinct odd prime divisors of n.*

Proof. Let $n = 2^{e_0} \cdot p_1^{e_1} \cdot ... \cdot p_m^{e_m}$ where $p_1, .., p_m$ are the odd prime factors of n and $e_0 \geq 0$, $e_1, .., e_m \geq 1$. If $e_0 = 0$ we define $n_0 = p_1 \cdot ... p_m$. By Corollary 1.2.9 we have $\Phi_n(x) = \Phi_{n_0}(x^{\frac{n}{n_0}})$, so $A(n) = A(n_0) = A(p_1 \cdot ... \cdot p_m)$. If $e_0 \neq 0$ we define $n_0 = 2 \cdot p_1 \cdot ... \cdot p_m$. By Corollary 1.2.9 we have $\Phi_n(x) = \Phi_{n_0}(x^{\frac{n}{n_0}})$. By Theorem 1.2.10 we have $\Phi_{n_0}(x) = \Phi_{p_1 \cdot ... \cdot p_m}(-x)$ and therefore $\Phi_n(x) = \Phi_{p_1 \cdot ... \cdot p_m}(-x^{\frac{n}{n_0}})$. We get $A(n) = A(p_1 \cdot ... \cdot p_m)$ in both cases. □

Since the height of a cyclotomic polynomial $\Phi_n(x)$ depends only on the distinct odd primes that divide n, it makes sense to classify $\Phi_n(x)$ by the amount of odd primes that divide n.

Definition 2.0.5. *Given a cyclotomic polynomial $\Phi_n(x)$, where n has exactly k odd distinct prime factors. We then say that $\Phi_n(x)$ is a* ***cyclotomic polynomial of order k****.*

Example 2.0.6. $\Phi_8(x)$ is a cyclotomic polynomial of order 0.
$\Phi_{105}(x)$ is a cyclotomic polynomial of order 3 since $105 = 3 \cdot 5 \cdot 7$.
$\Phi_{324}(x)$ is a cyclotomic polynomial of order 1 since $324 = 2^2 \cdot 3^4$.

We can use some observations made in the first Chapter to prove something about the height of cyclotomic polynomials of order 0 and 1.

Proposition 2.0.7. *Any cyclotomic polynomial of order 0 or order 1 is flat.*

Proof. We have that $\Phi_1(x)$ is flat and for any prime p, $\Phi_p(x)$ is flat by Theorem 1.2.1. Proposition 2.0.4 therefore implies that any cyclotomic polynomial of order 1 or order 0 is flat. □

In the next section we are going to prove that any cyclotomic polynomial of order two is flat as well.

2.1 Cyclotomic polynomials of order two

In the first part of this section we are going to give an explicit formula for $\Phi_{pq}(x)$ for odd primes p and q. As we saw in the proof of Proposition 2.0.4, we then have an explicit formula for any cyclotomic polynomial of order two. This explicit formula for $\Phi_{pq}(x)$ was first proved by Lam and Lueng [7]. We will follow their proof while adding some detail, such as the upcoming lemma, which was assumed in the original proof. The second part of this section is dedicated to proving that the non-zero coefficients of $\Phi_{pq}(x)$ alternate between 1 and -1.

Lemma 2.1.1. *Given any distinct primes p and q, there exists unique $r \in [0, q-2]$ and $s \in [0, p-2]$ such that $(p-1)(q-1) = pr + qs$.*

Proof. First we prove the uniqueness of r and s. Suppose $pr+qs = (p-1)(q-1) = pr'+qs'$ with $r, r' \in [0, q-2]$ and $s, s' \in [0, p-2]$. Then we have $p(r-r') = q(s'-s)$. Since we have $\gcd(p,q) = 1$, we get $p|(s'-s)$ and $q|(r-r')$ by the fundamental lemma. Because we have $-p < s'-s < p$ and $-q < r-r' < q$, we must have $r-r' = s'-s = 0$ and therefore $(r,s) = (r',s')$.

Now we prove the existence of such r and s. Because we have $\gcd(p,q) = 1$, the Diophantine equation $px+qy = 1$ has a solution (x_0, y_0). The set of all solutions of this equation is given by $\{(x_0+qt, y_0-pt) | \, t \in \mathbb{Z}\}$. Suppose that $(0,y)$ is a solution, then $yq = 1$, which is not possible. We can write $x_0 = dq + x_1$ with $d \in \mathbb{Z}$ and $0 \leq x_1 < q$. Note that $(x_0 - dq, y_0 + dp)$ is also a solution. Because we have $x_0 - dq = x_1$, it holds that $0 < x_1 < q$. We define $y_1 = y_0 + dp$, which gives us $y_1 = \dfrac{1-px_1}{q}$, therefore y_1 is negative. Since we have $x_1 \leq q-1$, we get $y_1 \geq \dfrac{1-p(q-1)}{q} > \dfrac{-pq}{q} = -p$. So (x_1, y_1) is a solution of $px+qy = 1$ with $0 < x_1 < q$ and $-p < y_1 < 0$.

We have $(p-1)(q-1) = pq-p-q+1 = pq-p-q+(px_1+qy_1) = p(x_1-1)+q(p+y_1-1)$. Now we set $r = x_1 - 1$ and $s = p - y_1 - 1$ to get $r \in [0, q-2]$ and $s \in [0, p-2]$ with $(p-1)(q-1) = pr+qs$. □

Although at first sight this lemma seems very unrelated to cyclotomic polynomials, it is useful for getting a nice formula for $\Phi_{pq}(x)$. Our strategy to give the explicit formula for $\Phi_{pq}(x)$ will be to find a monic polynomial $p(x)$ that has the same degree as $\Phi_{pq}(x)$ and the same roots. The following theorem was proven by Lam and Lueng ([7]).

Theorem 2.1.2. *Let $(r,s) \in [0, q-2] \times [0, p-2]$ such that $(p-1)(q-1) = pr+qs$. Then we have* $\Phi_{pq}(x) = (\sum_{i=0}^{s} x^{qi}) \cdot (\sum_{k=0}^{r} x^{pk}) - x \cdot (\sum_{j=0}^{p-2-s} x^{qj}) \cdot (\sum_{l=0}^{q-2-r} x^{pl})$.

Proof. Since we have $p \nmid q$ and $q \nmid p$, we get from Theorem 1.2.7 that $\Phi_{pq}(x) \cdot \Phi_p(x) = \Phi_p(x^q)$ and $\Phi_{pq}(x) \cdot \Phi_q(x) = \Phi_q(x^p)$. Therefore any root ζ of $\Phi_{pq}(x)$ is a zero of $\Phi_p(x^q)$ and $\Phi_q(x^p)$. Of course any root ζ of $\Phi_{pq}(x)$ is also a root of $x^{pq}-1$.

Let ζ be any root of $\Phi_{pq}(x)$. Since ζ is a root of $\Phi_p(x^q)$ and $\Phi_q(x^p)$, we get $\sum_{i=0}^{p-1}(\zeta^q)^i = \sum_{j=0}^{q-1}(\zeta^p)^j = 0$. By Lemma 2.1.1 we can write $(p-1)(q-1)$, as $pr+qs$ with unique $r \in [0, q-2]$ and unique $s \in [0, p-2]$. We can use s and r to write $\sum_{i=0}^{s}(\zeta^q)^i = -\sum_{j=s+1}^{p-1}(\zeta^q)^j$ and $\sum_{k=0}^{r}(\zeta^p)^k = -\sum_{l=r+1}^{q-1}(\zeta^p)^l$. Multiplying both left sides and both right sides leads to

$$(\sum_{i=0}^{s} \zeta^{qi}) \cdot (\sum_{k=0}^{r} \zeta^{pk}) - (\sum_{j=s+1}^{p-1} \zeta^{qj}) \cdot (\sum_{l=r+1}^{q-1} \zeta^{pl}) = 0. \tag{2.1}$$

We are now going to do manipulations to the term $(\sum_{j=s+1}^{p-1} \zeta^{qj}) \cdot (\sum_{l=r+1}^{q-1} \zeta^{pl})$. We can write $(\sum_{j=s+1}^{p-1} \zeta^{qj}) \cdot (\sum_{l=r+1}^{q-1} \zeta^{pl}) = (\sum_{j=0}^{p-2-s} \zeta^{qj} \cdot \zeta^{q(r+1)}) \cdot (\sum_{l=0}^{q-2-r} \zeta^{pl} \cdot \zeta^{p(s+1)})$
$= \zeta^{q(r+1)+p(s+1)} \cdot (\sum_{j=0}^{p-2-s} \zeta^{qj}) \cdot (\sum_{l=0}^{q-2-r} \zeta^{pl}) = \zeta^{pq+1} \cdot (\sum_{j=0}^{p-2-s} \zeta^{qj}) \cdot (\sum_{l=0}^{q-2-r} \zeta^{pl})$.

Since ζ is a zero of $\Phi_{pq}(x)$, it is also a zero of $x^{pq}-1$, so $\zeta^{pq}=1$. Therefore we get $(\sum_{j=s+1}^{p-1} \zeta^{qj}) \cdot (\sum_{l=r+1}^{q-1} \zeta^{pl}) = \zeta \cdot (\sum_{j=0}^{p-2-s} \zeta^{qj}) \cdot (\sum_{l=0}^{q-2-r} \zeta^{pl})$. Note that these sums are well-defined, as we had $s \leq p-2$ and $r \leq q-2$.

Substituting this into (2.1) yields $(\sum_{i=0}^{s} \zeta^{qi}) \cdot (\sum_{k=0}^{r} \zeta^{pk}) - \zeta \cdot (\sum_{j=0}^{p-2-s} \zeta^{qj}) \cdot (\sum_{l=0}^{q-2-r} \zeta^{pl}) = 0$. So ζ is a zero of the polynomial $p(x) := (\sum_{i=0}^{s} x^{qi}) \cdot (\sum_{k=0}^{r} x^{pk}) - x \cdot (\sum_{j=0}^{p-2-s} x^{qj}) \cdot (\sum_{l=0}^{q-2-r} x^{pl})$.

As ζ was an arbitrary zero of Φ_{pq}, all the zeros of Φ_{pq} will be zeros of $p(x)$. The left side of the polynomial has highest order term $qs+pr=(p-1)(q-1)$. The right side has highest order term $1+q(p-2-s)+p(q-2-r)=1+2pq-(p-1)(q-1)-2p-2q=(p-1)(q-1)-1$. So this polynomial has degree $(p-1)(q-1)=\varphi(pq)=\deg(\Phi_{pq}(x))$. The coefficient of the highest order term is 1, so this polynomial is monic.

Since $p(x)$ and $\Phi_{pq}(x)$ have the same roots and the same degree and all the roots of $\Phi_{pq}(x)$ have multiplicity 1, we can use the Fundamental Theorem of Algebra which gives us $\Phi_{pq}(x) = C \cdot p(x)$ for some constant C. Since $p(x)$ and $\Phi_{pq}(x)$ are both monic we get $p(x) = \Phi_{pq}(x)$. Therefore we get

$$\Phi_{pq}(x) = (\sum_{i=0}^{s} x^{qi}) \cdot (\sum_{k=0}^{r} x^{pk}) - x \cdot (\sum_{j=0}^{p-(s+2)} x^{qj}) \cdot (\sum_{l=0}^{q-(r+2)} x^{pl}). \tag{2.2}$$

□

Now we can compute $\Phi_{pq}(x)$ for any distinct odd primes p and q. We will compute $\Phi_{55}(x)$ in the following example.

Example 2.1.3. We have $55 = 5 \cdot 11$ with $(5-1)(11-1) = 40$. We can write $40 = 8 \cdot 5 + 0 \cdot 11$. Therefore we get $\Phi_{55}(x) = \sum_{k=0}^{8} x^{5k} - x \cdot (\sum_{j=0}^{3} x^{11j}) \cdot (\sum_{l=0}^{1} x^{5l}) = x^{40} - x^{39} + x^{35} - x^{34} + x^{30} - x^{28} + x^{25} - x^{23} + x^{20} - x^{17} + x^{15} - x^{12} + x^{10} - x^{6} + x^{5} - x + 1$.

The idea was to apply this theorem to find $\Phi_{pq}(x)$ when p and q are distinct odd primes. However we did not use that p and q are odd primes anywhere in the proof of the theorem or the proof of the lemma, so what happens when $p = 2$ and q is an odd prime? In this case we have $(p-1)(q-1) = (q-1) = r \cdot 2$ for some $0 \leq r \leq q-2$ since q is odd. We

therefore have $s = 0$. Now Theorem 2.1.2 yields that $\Phi_{2q}(x) = \sum_{k=0}^{\frac{q-1}{2}} x^{2k} - x \cdot \sum_{l=0}^{\frac{q-1}{2}-1} x^{2l} = \sum_{\substack{k \text{ even} \\ k\in[0,q-1]}} x^k - \sum_{\substack{k \text{ odd} \\ k\in[0,q-1]}} x^k = \Phi_q(-x)$. This is consistent with Theorem 1.2.10.

Having this explicit formula for $\Phi_{pq}(x)$ allows us to show that all cyclotomic polynomials of order two are flat.

Corollary 2.1.4. *All cyclotomic polynomials of order two are flat.*

Proof. First we show that $\Phi_{pq}(x)$ is flat for all odd primes p and q. If we look at the formula for $\Phi_{pq}(x)$ in (2.2), the only thing we need to check to show that this holds is that we can not get multiple terms with the same exponent in the left or right sum.

Suppose that we have this in the left sum $(\sum_{i=0}^{s} x^{qi}) \cdot (\sum_{k=0}^{r} x^{pk})$. Then we have $qi + pk = qi' + pk'$, and thus $q(i - i') = p(k' - k)$. As $\gcd(p, q) = 1$, we get $q|k - k'$ and $p|i - i'$. Since we have $-p < i - i' < p$ and $-q < k' - k < q$, we must have $i = i'$ and $k' = k$, which implies that no two terms in the left sum have the same exponent.

Since $p - s - 2 < p$ and $q - r - 2 < q$, one can do similar steps to show that there is no double term in the negative part of $\Phi_{pq}(x)$. Because all terms in the left sum and all terms in the right sum have distinct exponents, we know that any term $a_k x^k$ of $\Phi_{pq}(x)$ either has 1, -1 or 0 as a_k. Therefore we conclude that $\Phi_{pq}(x)$ is flat for any distinct primes p and q.

By Proposition 2.0.4, the height of any cyclotomic polynomial of order two $\Phi_n(x)$ is the same as the height of $\Phi_{pq}(x)$, where p and q are the odd divisors of n. We showed that $A(pq) = 1$, therefore $A(n) = 1$ for any order two $\Phi_n(x)$. □

From this it follows that for $n < 105$ all cyclotomic polynomials are flat and therefore $\Phi_{105}(x)$ is the first possible non-flat cyclotomic polynomial.

Corollary 2.1.5. *All cyclotomic polynomials $\Phi_n(x)$ with $n < 105$ are flat.*

Proof. We have $105 = 3 \cdot 5 \cdot 7$, which is the lowest product of three distinct odd primes. Therefore for all $n < 105$, n has less then three distinct odd prime divisors. Thus $\Phi_n(x)$ is of order 0, 1 or 2 for $n < 105$. Since any cyclotomic polynomial of order 0, 1 or 2 is flat, $\Phi_n(x)$ is flat for $n < 105$. □

In the remaining part of this section we will work towards proving that for distinct primes p and q, $\Phi_{pq}(x)$ has alternating nonzero coefficients. To prove this we first prove the next theorem, which gives an alternative formula for any coefficient a_n of $\Phi_{pq}(x)$.

Theorem 2.1.6. *The n^{th} coefficient a_n of $\Phi_{pq}(x)$ is given by*

$$a_n = \begin{cases} 1 \text{ if } \exists\, c_1, t_1 \geq 0 \text{ s.t. } n = c_1p + t_1q \text{ and } \nexists\, c_2, t_2 \geq 0 \text{ s.t. } n-1 = c_2p + t_2q, \\ \\ -1 \text{ if } \nexists\, c_1, t_1 \geq 0 \text{ s.t. } n = c_1p + t_1q \text{ and } \exists\, c_2, t_2 \geq 0 \text{ s.t. } n-1 = c_2p + t_2q, \\ \\ 0 \text{ if } \exists\, c_1, t_1 \geq 0 \text{ s.t. } n = c_1p + t_1q \text{ and } \exists\, c_2, t_2 \geq 0 \text{ s.t. } n-1 = c_2p + t_2q \\ \text{ or if } \nexists\, c_1, t_1 \geq 0 \text{ s.t. } n = c_1p + t_1q \text{ and } \nexists\, c_2, t_2 \geq 0 \text{ s.t. } n-1 = c_2p + t_2q. \end{cases}$$

Proof. As we have $p \nmid q$, Theorem 1.2.7 gives us that $\Phi_q(x) \cdot \Phi_{pq}(x) = \Phi_q(x^p)$. This gives us

$$(1-x^q)\Phi_{pq}(x) = (1-x)(1+x^p+...+x^{p(q-1)}). \tag{2.3}$$

We write $\Phi_{pq}(x)$ as $\sum_{k=0}^{\varphi(pq)} a_k x^k$ and $(1-x)(1+x^p+...+x^{p(q-1)})$ as $\sum_{m=0}^{p(q-1)+1} \chi_m x^m$ where χ_m is given by $\chi_m = \begin{cases} 1 \text{ if } m \equiv 0 \,(\text{mod } p), \\ -1 \text{ if } m \equiv 1 \,(\text{mod } p), \\ 0 \text{ else.} \end{cases}$

For any $0 \leq n \leq \varphi(pq)$ we can write $n = qs + r$ with $0 \leq r < q$ and $s \geq 0$. For $0 \leq t \leq s$ we define $n_t := tq + r$. Since $n_0 = r < q$, we have $a_{n_0} = \chi_{n_0}$ by (2.3). For $t \geq 1$ we get $a_{n_t} - a_{n_{t-1}} = \chi_{n_t}$. Summing over all χ_{n_t} yields $\sum_{t=0}^{s} \chi_{n_t} = a_{n_0} + \sum_{t=1}^{s} (a_{n_t} - a_{n_{t-1}}) = a_{n_s} = a_n$

This implies that the coefficient a_n is given by $a_n = \sum_{k \in S} \chi_k$, where $S = \{n - tq |\, 0 \leq t \leq s\}$.

Let $k_1, k_2 \in S$, then we have $k_1 = n - t_1q$, $k_2 = n - t_2q$. Suppose that $\chi_{k_1} = \chi_{k_2} = 1$. Then $n - t_1q \equiv n - t_2q \equiv 0 \,(\text{mod } p)$ and therefore $(t_1 - t_2)q \equiv 0 (\text{mod } p)$. We have chosen n such that $0 \leq n \leq \varphi(pq) = (p-1)(q-1)$ and $n = r + sq$, so we have $s < p$. Because we have $\gcd(p, q) = 1$, it follows that $p|(t_1 - t_2)$. As we have $0 \leq t_1, t_2 \leq s < p$, we have $-p < t_1 - t_2 < p$ implying $t_1 - t_2 = 0$, which means that $t_1 = t_2$, and thus $k_1 = k_2$. Similar reasoning yields that $\chi_{k_1} = \chi_{k_2} = -1$ implies that $k_1 = k_2$.

So there can be at most one $k \in S$ with $\chi_k = 1$ and at most one $k \in S$ with $\chi_k = -1$. Suppose that there exists k with $\chi_k = 1$. Then $k = n - tq = c \cdot p$ with $0 \leq t \leq s$ and $0 \leq c \leq (q-1)$. Therefore we get $n = tq + cp$ with $0 \leq t \leq s$ and $0 \leq c \leq (q-1)$. Suppose that $t > s$, then we get $tq > n$, therefore $cp < 0$, which is impossible. Suppose that $c > (q-1)$, then $n \geq p(q-1) > \varphi(pq)$, which is impossible. Therefore we see that we have $\chi_k = 1$ if and only if we can write $n = tq + cp$ with $t, c \geq 0$.

By doing similar steps we can see that there exists a $k \in S$ with $\chi_k = -1$ if and only if there exist $c, t \geq 0$ such that $n - 1 = cp + tq$. Since we have $a_n = \sum_{k \in S} \chi_k$, a_n will be 1 if there is a $\chi_k = 1$ and not a $\chi_k = -1$. It will be -1 if there is a $\chi_k = -1$ and no $\chi_k = 1$. It will be 0 if both or neither exist. Putting this together with the previous paragraph yields the desired formula

$$a_n = \begin{cases} 1 \text{ if } \exists\, c_1, t_1 \geq 0 \text{ s.t. } n = c_1p + t_1q \text{ and } \nexists\, c_2, t_2 \geq 0 \text{ s.t. } n-1 = c_2p + t_2q, \\ -1 \text{ if } \nexists\, c_1, t_1 \geq 0 \text{ s.t. } n = c_1p + t_1q \text{ and } \exists\, c_2, t_2 \geq 0 \text{ s.t. } n-1 = c_2p + t_2q, \\ 0 \text{ if } \exists\, c_1, t_1 \geq 0 \text{ s.t. } n = c_1p + t_1q \text{ and } \exists\, c_2, t_2 \geq 0 \text{ s.t. } n-1 = c_2p + t_2q \\ \text{ or if } \nexists\, c_1, t_1 \geq 0 \text{ s.t. } n = c_1p + t_1q \text{ and } \nexists\, c_2, t_2 \geq 0 \text{ s.t. } n-1 = c_2p + t_2q. \end{cases} \quad . \quad \square$$

As an example we will use this theorem to compute some of the coefficients of $\Phi_{77}(x)$.

Example 2.1.7. Given $\Phi_{77}(x) = \sum_{k=0}^{60} a_k x^k$.
We can write $40 = 3 \cdot 11 + 7$, and we can write 39 as $11 + 4 \cdot 7$, so $a_{40} = 0$. We can not write 38 as $c \cdot 11 + t \cdot 7$, so we get $a_{39} = 1$. We also can not write 37 in this form, so $a_{38} = 0$. We have $36 = 2 \cdot 7 + 2 \cdot 11$, so $a_{37} = -1$.

Though computing $\Phi_{pq}(x)$ with this formula is much slower than with Theorem 2.1.2, it is useful for proving the next theorem.

Theorem 2.1.8. *The nonzero coefficients of $\Phi_{pq}(x)$ alternate between 1 and -1.*

Proof. First of all note that 1 and -1 are the only possible nonzero coefficients of $\Phi_{pq}(x)$, as $\Phi_{pq}(x)$ is flat. Suppose we have $n_1 < n_2$ with $a_{n_1} = a_{n_2} = 1$. We want to show that there exists $n_1 < n < n_2$ with $a_n = -1$.
By Theorem 2.1.6 there exist $c_1, t_1, c_2, t_2 \geq 0$ such that $n_1 = c_1p + t_1q$, $n_2 = c_2p + t_2q$ and there do not exist $c, t \geq 0$, such that $n_1 - 1 = cp + tq$ or $n_2 - 1 = cp + tq$.

Now define $S = \{n \in]n_1, n_2[\,|\, \exists c, t \geq 0 \text{ s.t. } n = cp + tq\}$. If S is empty, then no element in $]n_1, n_2[$ can be written as $cp + tq$ with $c, t \geq 0$. This means that $n_1 + 1$ can not be written in this form, however n_1 can by assumption, so $a_{n_1+1} = -1$.

If our set S is nonempty, it is bounded, therefore it has a largest element $m \in S$ for which $m + 1 \notin S$. Note that we can not have $m + 1 = n_2$, as $n_2 - 1$ can not be written as $cp + tq$ with $c, t \geq 0$. By construction of S we have $m + 1 \neq cp + tq$ for all $c, t \geq 0$, however $(m + 1) - 1 = m = cp + tq$ for some $c, t \geq 0$. This means that $a_{m+1} = -1$, so we have found n satisfying $n_1 < n < n_2$ with $a_n = -1$ in the case of S being empty and nonempty.

Now suppose $n_1 < n_2$ with $a_{n_1} = a_{n_2} = -1$. Now we want to find $n_1 < n < n_2$ with $a_n = 1$. By Theorem 2.1.6 there exist $c_1, c_2, t_1, t_2 \geq 0$ such that $n_1 - 1 = c_1p + t_1q$, $n_2 - 1 = c_2p + t_2q$, and there do not exist $c, t \geq 0$ such that $n_1 = cp + tq$ or $n_2 = cp + tq$.

We define $S = \{n \in]n_1, n_2 - 1[\,|\, \exists c, p \geq 0 \text{ s.t. } n = cp + tq\}$. If S is empty, then for all $n \in]n_1, n_2 - 1[$ no such c, p exist. Therefore $n_2 - 2$ can not be written in the form $cp + tq$ with $c, t \geq 0$, however $n_2 - 1$ can by assumption. So in this case we have $a_{n_2-1} = 1$.

Suppose that S is nonempty. Then S has a least element l, such that $l \in S$ and $l - 1 \notin S$. If $l = n_1 + 1$, then $l - 1 = n_1$, which does not have these c, t. If $l > n_1 + 1$, then $l - 1$ does

not have these c, t by construction of S. Therefore we will have $a_l = 1$. In all cases we can find some $n_1 < n < n_2$ such that $a_n = 1$.

This means that between any two -1 coefficients we have a 1 and conversely between any two 1's we have a -1, which means that the coefficients of $\Phi_{pq}(x)$ alternate between 1 and -1. □

This result in itself is quite nice, as it helps us understand the cyclotomic polynomial $\Phi_{pq}(x)$ better. It has further use in the next chapter where we study the coefficients of cyclotomic polynomials of order three.

Remark 2.1.9. Though all cyclotomic polynomials $\Phi_{pq}(x)$ have non-zero coefficients that alternate between 1 and -1, not all cyclotomic polynomials of order two have this. This is because for distinct odd primes p and q, $\Phi_{2pq}(x)$ is a cyclotomic polynomial of order two, which equals $\Phi_{pq}(-x)$. Having $-x$ as input instead of x breaks the property of alternating non-zero coefficients. An example of a cyclotomic polynomial of order two that does not have alternating non-zero coefficients is $\Phi_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$.

Note that by Corollary 1.2.9 for any $e_1, e_2 > 0$, the nonzero coefficients of $\Phi_{p^{e_1}q^{e_2}}(x)$ also alternate between -1 and 1 for distinct primes p, q.

Chapter 3

Cyclotomic polynomials of order three

In this chapter we study the coefficients of cyclotomic polynomials of order three. As we have already seen, the height of cyclotomic polynomials of order three behaves less 'nicely' than those of lower order, since cyclotomic polynomials of order three are not always flat. Since the height of a cyclotomic polynomial of order three $\Phi_n(x)$ is only determined by the three distinct odd prime divisors of n, we are going to study $\Phi_{pqr}(x)$ for primes $2 < p < q < r$ just like we studied $\Phi_{pq}(x)$ in the previous chapter. In the first section we build towards proving that, for any distinct odd primes p and q, there exists an infinite set of primes $\{r\}$, such that $\Phi_{pqr}(x)$ is flat. The second section is dedicated to proving that, given primes $2 < p < q < r$, the height of $\Phi_{pqr}(x)$ only depends on the class of r in $\mathbb{Z}_{pq}$. In both the sections we follow the approach taken by Kaplan [5] while filling in additional details.

3.1 Flat cyclotomic polynomials of order three

As mentioned above, in this section we intend to give an infinite family of primes $\{r\}$ for given primes $2 < p < q$ such that $\Phi_{pqr}(x)$ is flat. This family of primes $\{r\}$ will be those satisfying $r \equiv 1 \pmod{pq}$. This is an infinite family by the following theorem.

Proposition 3.1.1. ***Dirichlet's Theorem on arithmetic progressions:*** *Given any natural numbers n and k such that $gcd(k, n) = 1$ holds. Then there exist infinitely many primes p that satisfy $p \equiv k \,(mod\ n)$.*

In order to prove that each of these primes r generates a flat $\Phi_{pqr}(x)$, we are going to prove three lemmas in this section. These lemmas are all quite technical. Before proving these lemmas, we introduce some notation that is used throughout this section.

Notation 3.1.2. *Let p, q and r be some given odd primes. We define $f_n(m)$ as the unique value satisfying $0 \leq f_n(m) < pq$ and $f_n(m) \equiv r^{-1}(n - m) \,(mod\ pq)$. If we are working with a fixed n, we will write $f_n(m)$ as $f(m)$ in order to improve readability.*

Notation 3.1.3. *Throughout this chapter we denote the following polynomials as follows:* $\Phi_{pqr}(x) = \sum_{n=0}^{\varphi(pqr)} c_n x^n, \quad \Phi_{pq}(x) = \sum_{k=0}^{\varphi(pq)} a_k x^k.$

Notation 3.1.4. *Given a fixed n and a coefficient a_k of Φ_{pq}, we define* $a'_k := \begin{cases} a_k \text{ if } rk \leq n, \\ 0 \text{ else.} \end{cases}$

The first of the three lemmas that we are going to prove is a formula that expresses any coefficient of $\Phi_{pqr}(x)$ in terms of coefficients of $\Phi_{pq}(x)$. There are some similarities between the proof of this lemma and the proof of Theorem 2.1.6.

Proposition 3.1.5. *Let c_n be a coefficient of $\Phi_{pqr}(x)$, then* $c_n = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{q+p-1} a'_{f(m)}$. *Because n is fixed we don't bother writing $a'_{f_n(m)}$ instead of $a'_{f(m)}$.*

Proof. As we have $r \nmid pq$ we get from Theorem 1.2.7 that $\Phi_{pqr}(x) \cdot \Phi_{pq}(x) = \Phi_{pq}(x^r)$. Since we have $\Phi_{pq}(x) = \dfrac{x^{pq}-1}{\Phi_p(x)\Phi_q(x)\Phi_1(x)}$, we can write $\Phi_{pqr}(x)(1-x^{pq}) = -\Phi_p(x)\Phi_q(x)\Phi_1(x)\Phi_{pq}(x^r)$. This yields that $\Phi_{pqr}(x)(1-x^{pq}) = (1+x+...+x^{p-1})(1-x^q)\Phi_{pq}(x^r)$. Because we have $q > p$ by assumption, we get

$$\Phi_{pqr}(x)(1-x^{pq}) = (1+x+...+x^{p-1}-x^q-...-x^{p+q-1})\Phi_{pq}(x^r). \tag{3.1}$$

We will denote $(1+x+...+x^{p-1}-x^q-...-x^{p+q-1})$ as $\sum_{m=0}^{p+q-1} \chi_m x^m$, where χ_m is given by

$$\chi_m = \begin{cases} 1 \text{ if } m \in [0, p-1], \\ -1 \text{ if } m \in [q, q+p-1], \\ 0 \text{ else.} \end{cases}$$

We can write n as $n = t + s \cdot pq$ with $0 \leq t < pq$. For $0 \leq k \leq s$ we define $n_k := t + k \cdot pq$ with $n_s = n$. The term with degree n_k on the right side of (3.1) is $(\sum_{m+ri=n_k} \chi_m a_i)x^{n_k}$. The term on the left side of (3.1) with degree n_k is $(c_{n_k} - c_{n_{k-1}})x^{n_k}$ if $k \geq 1$ and $c_{n_0}x^{n_0}$ if $k = 0$. Since terms with the same degree must be equal, we get the equations $c_{n_0} = \sum_{m+ri=n_0} \chi_m a_i$ and $c_{n_k} - c_{n_{k-1}} = \sum_{m+ri=n_k} \chi_m a_i$ for $k \geq 1$. Summing all these equations for $0 \leq k \leq s$ yields $c_{n_0} - c_{n_0} + c_{n_1} - c_{n_1} + c_{n_2} ... - c_{n_{s-1}} + c_{n_s} = \sum_{0 \leq k \leq s} (\sum_{m+ri=n_k} \chi_m a_i)$. Therefore we end up with $c_n = c_{n_s} = \sum_{\substack{m+ri=n_k \\ 0 \leq k \leq s}} \chi_m a_i$. Since the set $\{n_k \,|\, 0 \leq k \leq s\}$ is exactly the set $\{m \,|\, m \equiv n \,(\text{mod } pq) \text{ with } 0 \leq m \leq n\}$, we get $\sum_{\substack{m+ri=n_k \\ 0 \leq k \leq s}} \chi_m a_i = \sum_{(m,i) \in S} \chi_m a_i$, where we have

$S = \{(m,i)| \quad 0 \leq m, i \quad m + ri \equiv n \,(\mathrm{mod}\, pq) \text{ and } m + ri \leq n\}$.

Suppose that $m + ri \equiv n \,(\mathrm{mod}\, pq)$, then $i \equiv r^{-1}(n-m) \,(\mathrm{mod}\, pq)$. Since we consider i for a coefficient a_i of $\Phi_{pq}(x)$, which has degree is $(p-1)(q-1) < pq$, we get $0 \leq i < pq$. Combining this with the previous line yields $i = f(m)$.

Let $rf(m) \leq n$ and suppose that $m + rf(m) > n$. As we consider m for a coefficient χ_m, we have $0 \leq m \leq p-1+q$. Thus $m < pq$ and therefore we can write $m + rf(m) = n + \delta$ with $0 < \delta < pq$. Since we have $m + rf(m) \equiv m + (n-m) \equiv n \,(\mathrm{mod}\, pq)$, we get $pq | n + \delta - n = \delta$, which is a contradiction since $0 < \delta < pq$. Therefore $m + rf(m) \leq n$ is a condition that is equivalent to $rf(m) \leq n$ for $0 \leq m \leq q + p - 1$. Using these observations, we can write

$$c_n = \sum_{(m,i)\in S} \chi_m a_i = \sum_{\substack{m\geq 0 \\ rf(m)\leq n}} \chi_m a_{f(m)} = \sum_{m\geq 0} \chi_m a'_{f(m)} = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{p+q-1} a'_{f(m)}. \qquad \square$$

Now that we know how any coefficient of $\Phi_{pqr}(x)$ looks like in terms those of $\Phi_{pq}(x)$, we will prove another lemma, which will be needed to prove that $\Phi_{pqr}(x)$ is flat if $r \equiv 1 \,(\mathrm{mod}\ pq)$.

Lemma 3.1.6. *Given $0 \leq n \leq \varphi(pqr)$ which is fixed. Then we have* $\sum_{m=0}^{p-1} a_{f(m)} = \sum_{m=q}^{p+q-1} a_{f(m)}$.

Proof. From Lemma 3.1.5 we get that any coefficient c_n of $\Phi_{pqr}(x)$ can be written as $c_n = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{p+q-1} a'_{f(m)} = \sum_{m=0}^{p+q-1} \chi_m a'_{f(m)}$. For $n > \deg(\Phi_{pqr}(x)) = (p-1)(q-1)(r-1)$ we must have $c_n = 0$. If n is chosen such that for all $m \in [0, p+q-1]$, $rf(m) \leq n$, then we would have $a'_{f(m)} = a_{f(m)}$ for all $m \in [0, p+q-1]$, so we would get $\sum_{m=0}^{p+q-1} \chi_m a'_{f(m)} = \sum_{m=0}^{p+q-1} \chi_m a_{f(m)}$.

As we have $\deg(\Phi_{pq}(x)) = (p-1)(q-1)$, $f(m) > (p-1)(q-1)$ implies that $a_{f(m)} = 0$. Choose $n \geq r(p-1)(q-1)$. Then we also have $n > (p-1)(q-1)(r-1)$. Thus we get $c_n = 0$. Therefore we get $\sum_{m=0}^{p+q-1} \chi_m a'_{f(m)} = 0$. As for all nonzero $a_{f(m)}$ we have $f(m) \in [0, (p-1)(q-1)]$ and we have chosen $n \geq r(p-1)(q-1)$, we have $rf(m) \leq n$ for all non-zero $a_{f(m)}$. This yields $0 = \sum_{m=0}^{p+q-1} \chi_m a'_{f(m)} = \sum_{m=0}^{p+q-1} \chi_m a_{f(m)}$ and therefore $\sum_{m=0}^{p-1} a_{f(m)} = \sum_{m=q}^{p+q-1} a_{f(m)}$.

Now suppose that we have $0 \leq n \leq \varphi(pqr)$. Then we can find $t > r(p-1)(q-1)$ such that $t \equiv n \,(\mathrm{mod}\ pq)$. We get $f_n(m) \equiv r^{-1}(n-m) \,(\mathrm{mod}\ pq) \equiv r^{-1}(t-m) \,(\mathrm{mod}\ pq) \equiv f_t(m)$ and therefore $f_n(m) = f_t(m)$ for all m.

Therefore the equality $\sum_{m=0}^{p-1} a_{f_n(m)} = \sum_{m=q}^{p+q-1} a_{f_n(m)}$ holds for n, as it holds for t. $\square$

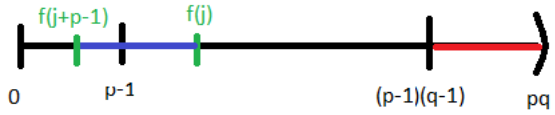
The previous two lemmas that we proved hold for general cyclotomic polynomials $\Phi_{pqr}(x)$. For the next lemma we demand that $r \equiv 1 \,(\mathrm{mod}\ pq)$. The general idea for the next lemma

is the following: Given $r \equiv 1 \pmod{pq}$ and given a fixed n as well as $m \in [j, j+p-1]$. Then the $f(m)$ values that give $a_{f(m)} \neq 0$ are contained in some interval I and the $f(m)$ values that give $a'_{f(m)} \neq 0$ are contained in some interval J, which is equal to I minus some high values in I.

Lemma 3.1.7. *Suppose that $r \equiv 1 \,(mod\ pq)$ and given a fixed $0 \leq n \leq \varphi(pqr)$. For any interval $[j, j+p-1] \subset [0, pq[$, there exists an interval $I = [a, b]$ and $J = [a, c]$ with $c \leq b$, such that $\sum_{m=j}^{j+p-1} a_{f(m)} = \sum_{k \in I} a_k$ and $\sum_{m=j}^{j+p-1} a'_{f(m)} = \sum_{k \in J} a_k$.*

Proof. As $r \equiv 1 \pmod{pq}$ we now get that $f(m) \equiv (n-m) \pmod{pq}$. For any integer b we get $f(m+b) \equiv (n-(m+b)) \pmod{pq} \equiv f(m)-b \pmod{pq}$. Therefore for all $m \in [j, j+p-1]$ we get that $f(m) = f(j+(m-j)) \equiv f(j) - (m-j) \pmod{pq}$. Now we split the problem in two cases, which are $f(j) \geq p-1$ and $f(j) < p-1$.

First we look at the case $f(j) \geq p-1$. Since for all $m \in [j, j+p-1]$ we have $(m-j) \leq p-1$, we get $0 \leq f(j) - (m-j) < pq$, therefore $f(m) = f(j) - (m-j)$ for all $m \in [j, j+p-1]$. Choosing $I = [f(j)-p-1, f(j)]$ yields $I = \{f(m) | \, m \in [j, j+p-1]\}$ and therefore I contains all $f(m)$ such that $a_{f(m)} \neq 0$. An example of this case is shown in the following illustration, where the blue values are all the $f(m)$'s and the red values are the integers higher than the degree of $\Phi_{pq}(x)$. We choose I to be the blue interval.

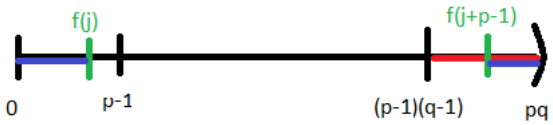


Now we look at the case $f(j) < p-1$. For all $m \in [j, j+f(j)] \subsetneq [j, j+p-1]$ we get that $0 \leq f(j) - (m-j) < pq$, therefore $f(m) = f(j) - (m-j)$ for $m \in [j, j+f(j)]$.

For all $m \in [j+f(j)+1, j+p-1]$ we have $-(p-1) < f(j) - (m-j) < 0$. Therefore we get $-(p-1) + pq < f(j) - (m-j) + pq < pq$. Since $f(m) \equiv f(j) - (m-j) + pq \pmod{pq}$, we get $f(m) = f(j) - (m-j) + pq$ for all $m \in [j+f(j)+1, j+p-1]$. The degree of $\Phi_{pq}(x)$ is $(p-1)(q-1)$, so for all $k > (p-1)(q-1)$ we get that $a_k = 0$. We have $(p-1)(q-1) = pq - (p-1) - q < pq - (p-1) < f(m)$ for all $m \in [j+f(j)+1, j+p-1]$. Therefore for all $m \in [j+f(j)+1, j+p-1]$ we have $a_{f(m)} = 0$!

Now we choose $I = [0, f(j)]$, which is exactly the set of $f(m)$ for $m \in [j, j+f(j)]$. This interval contains all $f(m)$ with $a_{f(m)} \neq 0$, as for $m \in [j+f(j)+1, j+p-1]$ we have $a_{f(m)} = 0$.

An example of this case is shown in the following illustration where the colours have the same meaning as in the previous illustration. We choose I to be the blue part on the left side.



As in both cases we can find I that contains all the $f(m) \in \{f(m)|\, m \in [j, j+p-1]\}$ with $a_{f(m)} \neq 0$ and $I \subset \{f(m)|\, m \in [j, j+p-1]\}$, we get that $\sum_{m=j}^{j+p-1} a_{f(m)} = \sum_{k \in I} a_k$.

Having found I, we now define J as $J := \{k \in I|\, rk \leq n\}$. Only the high values $k \in I$ for which $rk > n$ are removed from I, so if $I = [a, b]$ then $J = [a, c]$ with some $c \leq b$. We get $\sum_{m=j}^{j+p-1} a'_{f(m)} = \sum_{\substack{j \leq m \leq j+p-1 \\ rf(m) \leq n}} a_{f(m)} = \sum_{\substack{k \in I \\ rk \leq n}} a_k = \sum_{k \in J} a_k$.

We have thereby proven the existence of the intervals I and J of the desired form. □

Now that we have collected our three ingredients it is time to cook up the main theorem of this section. For the largest part of this proof, we will look at two cases, which we will divide into two cases again. We prove that in all these cases we have $|c_n| \leq 1$ for an arbitrary coefficient c_n of $\Phi_{pqr}(x)$. The following theorem was one of the main results in [5] by Kaplan.

Theorem 3.1.8. *Let r be a prime satisfying $r \equiv 1 \,(mod\ pq)$ for distinct odd primes p and q. Then $\Phi_{pqr}(x)$ is a flat cyclotomic polynomial.*

Proof. Lemma 3.1.5 gives us, that $c_n = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{q+p-1} a'_{f(m)}$. We will call the first sum $S := \sum_{m=0}^{p-1} a'_{f(m)}$ and the second sum $T := \sum_{m=q}^{q+p-1} a'_{f(m)}$. By Lemma 3.1.7 there exist intervals J_0 and J_q such that $\sum_{m=0}^{p-1} a'_{f(m)} = \sum_{j \in J_0} a_j$ and $\sum_{m=q}^{q+p-1} a'_{f(m)} = \sum_{j \in J_q} a_j$. Because J_0 and J_q are intervals and by Theorem 2.1.8, the coefficients of $\Phi_{pq}(x)$ alternate, the sum of the coefficients a_k with k in these intervals has absolute value at most 1. Therefore we have $|S|, |T| \leq 1$. Now we need to prove that we can not have $S = T = 1$ or $S = T = -1$. We divide the problem into the case $T = 1$ and $T = -1$.

First we look at the case $T = 1$. Again we will divide the problem in two cases: Either there is some $k \in [q, q+p-1]$ with $a_{f(k)} \neq a'_{f(k)}$ (so $a'_{f(k)} = 0$) or this k does not exist.

Suppose this k exists. If $f(k) > (p-1)(q-1)$ then we get $a_{f(k)} = 0$ and $a'_{f(k)} = 0$, so we must have $f(k) \leq (p-1)(q-1)$.

Now we are going to rule out the case $f(k) = (p-1)(q-1)$ with $k = p+q-1$. For all $j \in [q, q+p-1]$ we have $f(j) = f(k + (j-k)) \equiv f(k) + (k-j) \,(\text{mod } pq)$. For any of these j we have $f(k) + (k-j) \leq (p-1)(q-1) + p - 1 = pq - q < pq$, therefore we get $f(j) = f(k) + (k-j) \geq f(k)$ for all $j \in [q, q+p-1]$. As we have $rf(k) > n$, we get $rf(j) > n$ for all $j \in [q, q+p-1]$. So $a'_{f(j)} = 0$ for all $j \in [q, q+p-1]$, which yields $T = 0$, which is a contradiction, as we assumed $T = 1$.

Now that we have ruled out the case $f(k) = (p-1)(q-1)$ with $k = p+q-1$, we go back to the case $k \in [q, q+p-1]$ with $a_{f(k)} \neq a'_{f(k)}$. For all $m \in [0, p-1]$ we have $f(m) = f(k + (m-k)) \equiv f(k) + (k-m) \,(\text{mod } pq)$. We know that $f(k) \leq (p-1)(q-1)$,

$k \leq p+q-1$ and we can not have both these inequalities being an equality. Therefore we get $f(k)+(k-m) < (p-1)(q-1)+(p+q-1-0) = pq$. This yields that for all $m \in [0, p-1]$ we get $f(m) = f(k) + (k-m) > f(k)$. Since we have $rf(k) > n$, it holds that $rf(m) > n$ for all $m \in [0, p-1]$. So for all $m \in [0, p-1]$, we get $a'_{f(m)} = 0$, which means that $S = 0$. Thus we get $c_n = S - T = -1$.

Now suppose that no $k \in [q, q+p-1]$ exists such that $a_{f(k)} \neq a'_{f(k)}$. Using lemma 3.1.6 we get $1 = T = \sum_{j=q}^{q+p-1} a'_{f(j)} = \sum_{j=q}^{q+p-1} a_{f(j)} = \sum_{i=0}^{p-1} a_{f(i)}$. From Lemma 3.1.7 we get that there is an interval $I_0 = [a, b]$, such that $\sum_{i=0}^{p-1} a_{f(i)} = \sum_{l \in I_0} a_l = 1$. As the coefficients of $\Phi_{pq}(x)$ alternate, we get that the nonzero a_k with highest l and the nonzero a_l with lowest l are both 1. From Lemma 3.1.7 we get that there exists an interval J_0 with $\sum_{j \in J_0} a_j = \sum_{i=0}^{p-1} a'_{f(i)}$, where $J_0 = [a, c]$ with $c \leq b$. The sum $\sum_{j \in J_0} a_j$ will be 0 or 1, since the lowest nonzero a_j is equal to 1 if a nonzero a_j exists, because $I_0 = [a, b]$ and $J_0 = [a, c]$ with $c \leq b$. We have $c_n = S - T = \sum_{i=0}^{p-1} a'_{f(i)} - 1 = \sum_{j \in J_0} a_j - 1 = -1$ or 0, depending on whether $S = 1$ or $S = 0$.

Now suppose that $T = -1$. Again we have two cases which are determined by the existence of a $k \in [q, q+p-1]$ with $a_{f(k)} \neq a'_{f(k)}$. If this k exists we can do exactly the same steps as in the case of $T = 1$ to conclude that $S = 0$, which gives us $c_n = S - T = 1$.

In the case that no such k exists we can again use Lemma 3.1.6 to get $-1 = T = \sum_{j=q}^{p+q-1} a'_{f(j)} = \sum_{j=q}^{p+q-1} a_{f(j)} = \sum_{i=0}^{p-1} a_{f(i)}$. By Lemma 3.1.7, we can find an interval $I_0 = [a, b]$ such that $-1 = \sum_{i=0}^{p-1} a_{f(i)} = \sum_{i \in I_0} a_i$. As the coefficients of $\Phi_{pq}(x)$ alternate, both the nonzero a_i with highest i and the nonzero a_i with lowest i must be -1. We can again find an interval J_0 such that $J_0 = [a, c]$ with $c \leq b$ for which we have $\sum_{j \in J_0} a_j = \sum_{i=0}^{p-1} a'_{f(i)}$. The sum $\sum_{j \in J_0} a_j$ will be -1 or 0 depending on whether the nonzero a_j with highest j is 1 or -1 if such a nonzero a_j exists. We get $c_n = S - T = \sum_{j \in J_0} a_j + 1$, which is 1 or 0 depending on whether $\sum_{j \in J_0} a_j = -1$ or 0.

This concludes the final case, which means that in all the cases we have $|c_n| \leq 1$ for arbitrary n, therefore we conclude that if $r \equiv 1 \pmod{pq}$, $\Phi_{pqr}(x)$ is flat. □

Now we have proven that for any two primes $2 < p < q$, any prime r satisfying $r \equiv 1 \pmod{pq}$ yields flat $\Phi_{pqr}(x)$. We are going to improve this to $\Phi_{pqr}(x)$ is flat if $r \equiv \pm 1 \pmod{pq}$ in the next section. The theorem implies the following immediate corollary.

Corollary 3.1.9. *Any cyclotomic polynomial $\Phi_n(x)$ of order three such that n has odd prime divisors $p < q < r$ with $r \equiv 1 \,(mod\ pq)$ is flat.*

Proof. This is follows immediately from the last theorem combined with Proposition 2.0.4. □

Now we can find many flat cyclotomic polynomials of order three.

Example 3.1.10. In this example we will compute $A(5418)$. We can write $5418 = 2{\cdot}3^2{\cdot}7{\cdot}43$. So the odd prime divisors of 5418 are $3 < 7 < 43$. We have $43 \equiv 1 \,(\text{mod } 21)$, which implies that $A(5418) = 1$.

3.2 The height of cyclotomic polynomials of order three

In this section we are going to prove a relationship between the height of cyclotomic polynomials of order three. This relationship states that for any odd primes $p < q < r, s$, if we have $r \equiv \pm s \,(\text{mod } pq)$, then we have $A(pqr) = A(pqs)$. In order to prove this, we will first prove the two main lemmas. Kaplan [5] was the first person who came up with this relationship and as in the previous section, we will follow his approach while filling in additional detail. First we introduce some notation that is used in this section.

Notation 3.2.1. *In this section we use the following notation:*

$$\Phi_{pqr}(x) = \sum_{n=0}^{\varphi(pqr)} c_n x^n, \quad \Phi_{pqs}(x) = \sum_{l=0}^{\varphi(pqs)} d_l x^l, \quad \Phi_{pq}(x) = \sum_{k=0}^{\varphi(pq)} a_k x^k,$$

$$1 + x + ... + x^{p-1} - x^q - ... - x^{p+q-1} = \sum_{m=0}^{p+q-1} \chi_m x^m.$$

Given a fixed n, then for any coefficient a_k of $\Phi_{pq}(x)$, we write $a_k^{(n)} = \begin{cases} a_k \text{ if } rk \le n, \\ 0 \text{ else.} \end{cases}$

For this fixed n, we write $0 \le f_n(m) < pq$ with $f_n(m) \equiv r^{-1}(n-m) \,(mod\ pq)$.

Given a fixed l, then for any coefficient a_k of $\Phi_{pq}(x)$, we write $a_k^{(l)} = \begin{cases} a_k \text{ if } sk \le l, \\ 0 \text{ else.} \end{cases}$

For this fixed l, we write $0 \le g_l(m) < pq$ with $g_l(m) \equiv s^{-1}(l-m) \,(mod\ pq)$.
If we are only working with one n or l, we may write $a'_k = a_k^{(n)}$, $a_k^* = a_k^{(l)}$, $f_n(m) = f(m)$ or $g_l(m) = g(m)$ in order to make the document easier to read.

We are going to prove the first of the two main lemmas needed for proving that if $r \equiv s \,(\text{mod } pq)$ then $A(pqr) = A(pqs)$.

Lemma 3.2.2. *Given a fixed $0 \le n \le \varphi(pqr)$. If for any m we have that $\chi_m a_{f(m)}$ and $\chi_{m+r} a_{f(m+r)}$ are both nonzero, then they must be equal.*

Proof. Suppose that $\chi_m a_{f(m)}$ and $\chi_{m+r} a_{f(m+r)}$ are nonzero.
Since χ_m is nonzero, we must have $0 \leq m \leq p-1$ or $q \leq m \leq q+p-1$. Because we have $m+r > m+q$ if both χ_m and χ_{m+r} are nonzero, we must have $0 \leq m \leq p-1$ and $q \leq m+r \leq q+p-1$. Therefore $\chi_m = -\chi_{m+r}$ if they are both nonzero.

Now we look at $a_{f(m)}$ and $a_{f(m+r)}$, which are nonzero. Suppose that $f(m) = 0$, then we have $f(m+r) \equiv r^{-1}(n-(m+r)) \equiv f(m) - 1 \,(\mathrm{mod}\ pq)$. This implies $f(m+r) = pq - 1 > \varphi(pq) = \deg(\Phi_{pq}(x))$, which implies that $a_{f(m+r)} = 0$, which is not possible.

Therefore we get $f(m) > 0$ and since we have $f(m+r) \equiv f(m) - 1 \,(\mathrm{mod}\ pq)$, we get $f(m+r) = f(m) - 1$. This implies that $a_{f(m+r)} = a_{f(m)-1}$. Since $a_{f(m)}$ and $a_{f(m)-1}$ are nonzero, one must be 1 and the other must be -1 since the nonzero coefficients of $\Phi_{pq}(x)$ alternate between 1 and -1. This yields that $a_{f(m+r)} = -a_{f(m)}$. Putting this together with $\chi_m = -\chi_{m+r}$ yields that $\chi_m a_{f(m)} = \chi_{m+r} a_{f(m+r)}$ if they are both nonzero. □

Now we introduce notation, which we will use until Theorem 3.2.7.

Notation 3.2.3. *Given a fixed $0 \leq l \leq \varphi(pqs)$ such that $d_l \neq 0$. Then we write $U = \{m \,|\, \chi_m a^*_{g(m)} \neq 0\}$ and $V = \{m \,|\, \chi_m a_{g(m)} \neq 0\,,\ a^*_{g(m)} = 0\}$.*
We define $g(j) := \max\limits_{m \in U}\{g(m)\}$ and $g(k) := \min\limits_{m \in V}\{g(m)\}$.

Note that we specified $d_l \neq 0$. This is needed to guarantee the existence of the after mentioned maximum and minimum.

Lemma 3.2.4. *This minimum $g(k)$ and this maximum $g(j)$ both exist if $d_l \neq 0$. Furthermore we have $g(j) < g(k)$.*

Proof. We have $d_l \neq 0$, therefore we get $\sum\limits_{m=0}^{p+q-1} \chi_m a^*_{g(m)} \neq 0$. Therefore there must be some $m \in [0, p+q-1]$ such that $\chi_m a^*_{g(m)} \neq 0$, so our maximum $g(j)$ is well-defined. By Lemma 3.1.6 we have $\sum\limits_{m=0}^{p+q-1} \chi_m a_{g(m)} = 0 \neq \sum\limits_{m=0}^{p+q-1} \chi_m a^*_{g(m)}$. This means that there is some $\chi_m a^*_{g(m)} \neq \chi_m a_{g(m)}$, which only happens when $\chi_m a_{g(m)} \neq 0$ and $a^*_{g(m)} = 0$. Therefore our maximum $g(k)$ is well-defined.

For $g(k)$ we have $a^*_{g(k)} = 0$ with $a_{g(k)} \neq 0$ and for $g(j)$ we have $a^*_{g(j)} \neq 0$, which means that we have $sg(k) > l$ and $sg(j) \leq l$, therefore $g(j) < g(k)$. □

The next lemma will be used as an auxiliary lemma to prove Lemma 3.2.6, which is the second main lemma needed for proving that if $r \equiv s \,(\mathrm{mod}\ pq)$ then $A(pqr) = A(pqs)$.

Lemma 3.2.5. *Suppose that $s > pq$ and d_l is a coefficient of $\Phi_{pqs}(x)$ with $d_l \neq 0$ then we have $d_l = d_{sg(j)+j}$.*

Proof. Since $d_l \neq 0$, $g(j)$ is well-defined. For simplicity we denote $z = sg(j) + j$.
We can write $d_l = \sum\limits_{m=0}^{p+q-1} \chi_m a^*_{g(m)} = \sum\limits_{\substack{m \in [0, p+q-1] \\ g(m) \leq g(j)}} \chi_m a_{g(m)}$ since $g(j) < g(k)$.

We have $z \equiv s \cdot s^{-1}(l-j)+j \equiv l \pmod{pq}$. Therefore we have $g_z(m) = g(m)$ for all m. This means that we can write $d_z = \sum_{\substack{m\in[0,p+q-1] \\ sg(m)\leq sg(j)+j}} \chi_m a_{g(m)}$. Since we have $j \leq p+q-1$, we have $j \leq pq < s$, which implies that $sg(m) \leq sg(j)+j$ is equivalent to $g(m) \leq g(j)$. This yields $d_z = \sum_{\substack{m\in[0,p+q-1] \\ g(m)\leq g(j)}} \chi_m a_{g(m)} = d_l$. □

Now we are ready to prove the second main lemma.

Lemma 3.2.6. *Suppose that $s > pq$ and d_l is a coefficient of $\Phi_{pqs}(x)$ with $|d_l| = A(pqs)$, then we have $\chi_k a_{g(k)} = -\chi_j a_{g(j)}$.*

Proof. Since $|d_l| = A(pqs) > 0$, $g(j)$ and $g(k)$ are well-defined. As in the previous lemma we write $z = sg(j)+j$. Since we have $d_l \neq 0$ and $s > pq$, we can use the previous lemma we to get $d_l = d_z$. Therefore we have $|d_z| = A(pqs)$.

We have $d_{z-pq} = \sum_{m=0}^{p+q-1} \chi_m a_{g(m)}^{(z-pq)} = \sum_{\substack{m\in[0,p+q-1] \\ sg(m)\leq z-pq}} \chi_m a_{g(m)} = \sum_{\substack{m\in[0,p+q-1] \\ sg(m)\leq sg(j)+(j-pq)}} \chi_m a_{g(m)}$.
Since $0 \leq j \leq p+q-1 \leq pq < s$, we get that $-s < j-pq < 0$, which means that $sg(m) \leq sg(j)+(j-pq)$ happens if and only if $g(m) < g(j)$.
Therefore we get $d_{z-pq} = \sum_{\substack{m\in[0,p+q-1] \\ g(m)<g(j)}} \chi_m a_{g(m)} = d_z - \chi_j a_{g(j)}$.

Now we are going to look at $d_{k+sg(k)}$. We are going to write $y = k+sg(k)$. We have $d_y = \sum_{m=0}^{p+q-1} \chi_m a_{g_y(m)}^{(y)} = \sum_{\substack{m\in[0,p+q-1] \\ sg_y(m)\leq y}} \chi_m a_{g_y(m)}$. Similarly to how we showed that $g_z(m) = g(m)$ for all m in the previous lemma, we can show that it also holds that $g_y(m) = g(m)$ for all m. Thus we have $d_y = \sum_{\substack{m\in[0,p+q-1] \\ sg(m)\leq y}} \chi_m a_{g(m)}$. Since we have $0 \leq k \leq p+q-1 \leq pq < s$, we have $sg(m) \leq y$ if and only if $g(m) \leq g(k)$. Therefore we have $d_y = \sum_{\substack{m\in[0,p+q-1] \\ g(m)\leq g(k)}} \chi_m a_{g(m)}$. Since we have $g(j) < g(k)$, we can write this sum as $\sum_{\substack{m\in[0,p+q-1] \\ g(m)\leq g(j)}} \chi_m a_{g(m)} + \sum_{\substack{m\in[0,p+q-1] \\ g(j)<g(m)<g(k)}} \chi_m a_{g(m)} + \chi_k a_{g(k)}$.
Note that the left sum is equal to d_z. For any $m \in [0, p+q-1]$ with $g(j) < g(m) < g(k)$, we have $m \notin U$ and $m \notin V$ by construction of $g(j)$ and $g(k)$. Since $U = \{m \,|\, \chi_m a_{g(m)}^* \neq 0\}$ and $V = \{m \,|\, \chi_m a_{g(m)} \neq 0\,,\, a_{g(m)}^* = 0\}$, we have $\chi_m a_{g(m)} = 0$ for $m \in [0, p+q-1]$ with $g(j) < g(m) < g(k)$. This means that we can write $d_y = d_z + \chi_k a_{g(k)}$ and $d_{z-pq} = d_z - \chi_j a_{g(j)}$.

Note that $\chi_j a_{g(j)}$ and $\chi_k a_{g(k)}$ are both nonzero by construction, therefore they can be 1 or -1 since $\Phi_{pq}(x)$ is flat. Since $|d_z| = A(pqs)$, we either have $d_z < 0$ or $d_z > 0$. If $d_z < 0$ then we must have $\chi_j a_{g(j)} = -1$ and $\chi_k a_{g(k)} = 1$ since we otherwise get $|d_{z-pq}| > |d_z|$ or $|d_y| > |d_z|$,

which is a contradiction since $|d_z| = A(pqs)$. Similarly if $d_z > 0$, then we must have $\chi_j a_{g(j)} = 1$ and $\chi_k a_{g(k)} = -1$. This means that in all cases we have $\chi_j a_{g(j)} = -\chi_k a_{g(k)}$. □

Next we are going to prove that $A(pqs) = A(pqr)$ when $s \equiv r \,(\mathrm{mod}\, pq)$. Since we have $r \equiv s \,(\mathrm{mod}\, pq)$, we can assume without loss of generality that $s > r$, which implies that $s > pq$. In the first part of the proof we will show that for any coefficient c_n of $\Phi_{pqr}(x)$ we can find a coefficient d_l of $\Phi_{pqs}(x)$ such that $c_n = d_l$. In the second and longest part of the proof we will assume that for a coefficient d_l with $|d_l| = A(pqs)$ there exists no c_n such that $c_n = d_l$. We are then going to use Lemma 3.2.2 and Lemma 3.2.6 to show that this results in a contradiction. These can be used since we have $s > pq$. The following was the second main result in [5] by Kaplan.

Theorem 3.2.7. *For primes $2 < p < q < r, s$ if $r \equiv s \,(mod\ pq)$ then $A(pqr) = A(pqs)$.*

Proof. We assume without loss of generality that $r < s$, which means $s > pq$. Let c_n be any coefficient of $\Phi_{pqr}(x)$. We are going to prove that there exists d_l of $\Phi_{pqs}(x)$ such that $c_n = d_l$.

We can write $c_n = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{q+p-1} a'_{f(m)}$. Choose d_l with $l \equiv n \,(\mathrm{mod}\, pq)$, which is possible since $\deg(\Phi_{pqr}(x)) < \deg(\Phi_{pqs}(x))$. We can write $d_l = \sum_{m=0}^{p-1} a^*_{g(m)} - \sum_{m=q}^{q+p-1} a^*_{g(m)}$. Since $r \equiv s \,(\mathrm{mod}\, pq)$ and $n \equiv l \,(\mathrm{mod}\, pq)$, we have $g(m) \equiv s^{-1}(l-m) \equiv r^{-1}(n-m) \equiv f(m) \,(\mathrm{mod}\, pq)$, which means that $f(m) = g(m)$. Thus we have $d_l = \sum_{m=0}^{p-1} a^*_{f(m)} - \sum_{m=q}^{q+p-1} a^*_{f(m)}$.

Now we write n in the form $n = \left\lfloor \frac{n}{r} \right\rfloor \cdot r + n_0$ with $0 \le n_0 < r$. We specify l as $l = \left\lfloor \frac{n}{r} \right\rfloor s + n_0$. Since $r \equiv s \,(\mathrm{mod}\, pq)$, we indeed have $n \equiv l \,(\mathrm{mod}\, pq)$.

Suppose we have $a'_{f(m)} = a_{f(m)}$, then we must have $rf(m) \le \left\lfloor \frac{n}{r} \right\rfloor + n_0$, which implies that $f(m) \le \left\lfloor \frac{n}{r} \right\rfloor$ since $n_0 < r$. Therefore we get $sf(m) \le s\left\lfloor \frac{n}{r} \right\rfloor + n_0$, which yields $a^*_{f(m)} = a_{f(m)}$. Thus we have $a^*_{f(m)} = a_{f(m)}$ if $a'_{f(m)} = a_{f(m)}$. Similar reasoning the other way around yields that $a'_{f(m)} = a_{f(m)}$ if $a^*_{f(m)} = a_{f(m)}$. This means that we have $a^*_{f(m)} = a'_{f(m)}$ for all m. Therefore we get $\sum_{m=0}^{p-1} a^*_{f(m)} - \sum_{m=q}^{q+p-1} a^*_{f(m)} = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{q+p-1} a'_{f(m)}$, which yields $d_l = c_n$. Let c_n be the coefficient such that $|c_n| = A(pqr)$, then we find $d_l = c_n$ with $|d_l| = A(pqr)$, therefore we get $A(pqr) \le A(pqs)$.

Now let d_l be a coefficient of $\Phi_{pqs}(x)$, such that $|d_l| = A(pqs)$. We assume that there exists no c_n of $\Phi_{pqr}(x)$ with $c_n = d_l$.

Recall that $g(j)$ was defined as $\min_{m \in U}\{g(m)\}$, where $U = \{m \,|\, \chi_m a_{g(m)} \neq 0\,,\ a^*_{g(m)} \neq 0\}$. We define $n = j + rg(j)$, which means that $n \equiv j + r \cdot s^{-1}(l-j) \equiv j + r \cdot r^{-1}(l-j) \equiv l \,(\mathrm{mod}\, pq)$.

Therefore we get $f(m) \equiv r^{-1}(n-m) \equiv s^{-1}(l-m) \equiv g(m) \pmod{pq}$. This implies that we have $f(m) = g(m)$ for all m.

By construction of n we have $rg(j) \leq n$, therefore if $g(m) \leq g(j)$, we have $a'_{g(m)} = a_{g(m)}$. Now we can write $c_n = \sum_{m=0}^{q+p-1} \chi_m a'_{g(m)} = \sum_{\substack{m\in[0,p+q-1] \\ g(m)\leq g(j)}} \chi_m a_{g(m)} + \sum_{\substack{m\in[0,p+q-1] \\ g(m)\geq g(k)}} \chi_m a'_{g(m)}$, as for $m \in [0, p+q-1]$ with $g(j) < g(m) < g(k)$ we have $m \notin U$ and $m \notin V$, which means that $\chi_m a_{g(m)} = 0$.

From the proof of Lemma 3.2.6 we got that $d_l = \sum_{\substack{m\in[0,p+q-1] \\ g(m)\leq g(j)}} \chi_m a_{g(m)}$. Since we have $d_l \neq c_n$ by assumption, we must have $\sum_{\substack{m\in[0,p+q-1] \\ g(m)\geq g(k)}} \chi_m a'_{g(m)} \neq 0$. This means that there exists some $a'_{g(m)} \neq 0$ with $g(m) \geq g(k) > g(j)$.

This implies that $rg(m) \leq n = j + rg(j)$. Note that therefore we must have $0 \leq r \leq j \leq p+q-1 < pq$ and since $p < q < r$, we have $j \leq p+q-1 < 2r$. Therefore we have $rg(m) < 2r + rg(j)$, which means that $g(m) \leq g(j) + 1$. Together with $g(m) \geq g(k) > g(j)$ this implies that $g(m) = g(k) = g(j) + 1$.

Recall from the proof of Lemma 3.1.5 that $rg(k) \leq n$ implies that $rg(k) + k \leq n$. This means that we have $rg(k) + k \leq j + rg(j)$, and thus $r(g(k) - g(j)) \leq j - k$. Since $g(k) = g(j) + 1$, we get that $r \leq j - k$. Because it holds that $0 \leq k, j < 2r$, we have $r \leq j - k < 2r$. As we have $g(k) = g(j)+1$, we get that $r^{-1}(n-k) \equiv r^{-1}(n-j)+1 \pmod{pq}$, which gives us $j - k \equiv r \pmod{pq}$. Since we had $r < pq$ and $r \leq j - k < 2r$, we must have $j - k = r$.

Now we have the tools that we need to derive a contradiction.
We have $\chi_k a_{g(k)} = \chi_{r+j} a_{g(r+j)}$. Since $\chi_k a_{g(k)}$ and $\chi_j a_{g(j)}$ are nonzero by construction, we can use Lemma 3.2.2, which gives us that $\chi_k a_{g(k)} = \chi_{j+r} a_{g(j+r)} = \chi_j a_{g(j)}$. However Lemma 3.2.6 said that $\chi_k a_{g(k)} = -\chi_j a_{g(j)}$, which is a contradiction.
Therefore it is not possible that for d_l with $|d_l| = A(pqs)$ there not being c_n, such that $c_n = d_l$, which means that if $|d_l| = A(pqs)$, there exists c_n with $c_n = d_l$. This implies that $A(pqs) \leq A(pqr)$. Combining this with $A(pqr) \leq A(pqs)$ yields $A(pqr) = A(pqs)$. □

This theorem is very useful, as for given p and q, we can compute the height of all $\Phi_{pqr}(x)$ while only having to compute it for $\varphi(pq) = (p-1)(q-1)$ odd primes r that are in distinct residue classes (mod pq).
Next we are going to prove that if we have $r \equiv -s \pmod{pq}$, then we get $A(pqr) = A(pqs)$. To prove this we use the previous theorem. Our proof strategy will be similar to the one used in the first part of the previous theorem. This was the last main theorem in [5] by Kaplan.

Theorem 3.2.8. *If $r \equiv -s \pmod{pq}$ for primes $2 < p < q < r, s$, then we have $A(pqr) = A(pqs)$.*

Proof. Since we have $A(pqr) = A(pqr')$ if $r \equiv r' \pmod{pq}$, we can choose r and s to be sufficiently large such that $pq < r, s$. Given any coefficient c_n of $\Phi_{pqr}(x)$ and d_l of $\Phi_{pqs}(x)$. We can write $c_n = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{q+p-1} a'_{f(m)}$ and $d_l = \sum_{m=0}^{p-1} a^*_{g(m)} - \sum_{m=q}^{q+p-1} a^*_{g(m)}$.

We can write n as $n = \left\lfloor \frac{n}{r} \right\rfloor r + n_0$ with $0 \leq n_0 < r$. We define l_0 to be the unique value satisfying $0 \leq l_0 < pq$ and $l_0 \equiv q + p - 1 - n_0 \pmod{pq}$. Now we specify l as $l = \left\lfloor \frac{n}{r} \right\rfloor s + l_0$, which yields $l \equiv \left\lfloor \frac{n}{r} \right\rfloor s + (q+p-1-n_0) \equiv -\left\lfloor \frac{n}{r} \right\rfloor r - n_0 + (q+p-1) \equiv (q+p-1) - n \pmod{pq}$. Therefore we get $g(m) \equiv s^{-1}(l-m) \equiv -r^{-1}((q+p-1)-n-m) \equiv r^{-1}(n-((q+p-1)-m)) \equiv f((q+p-1)-m) \pmod{pq}$.

We can use this to get $d_l = \sum_{m=0}^{p-1} a^*_{g(m)} - \sum_{m=q}^{q+p-1} a^*_{g(m)} = \sum_{m=0}^{p-1} a^*_{f((q+p-1)-m)} - \sum_{m=q}^{q+p-1} a^*_{f((q+p-1)-m)}$.

Changing the sums yields $d_l = -\sum_{m=0}^{p-1} a^*_{f(m)} + \sum_{m=q}^{q+p-1} a^*_{f(m)}$.

Since we have $l_0 < pq < s$, we get that $sf(m) \leq \left\lfloor \frac{n}{r} \right\rfloor s + l_0$ if and only if $f(m) \leq \left\lfloor \frac{n}{r} \right\rfloor$, which is if and only if $rf(m) \leq n$. This yields that $a'_{f(m)} = a_{f(m)}$ if and only if $a^*_{f(m)} = a_{f(m)}$, therefore we have $a'_{f(m)} = a^*_{f(m)}$ for all m.

Filling this in yields $d_l = -\sum_{m=0}^{p-1} a^*_{f(m)} + \sum_{m=q}^{q+p-1} a^*_{f(m)} = -\sum_{m=0}^{p-1} a'_{f(m)} + \sum_{m=q}^{q+p-1} a'_{f(m)} = -c_n$.

Since for any c_n of $\Phi_{pqr}(x)$ we can find d_l of $\Phi_{pqs}(x)$ such that $d_l = -c_n$, we can do this for the coefficient c_n that has $|c_n| = A(pqr)$. This yields a coefficient d_l with $|d_l| = A(pqr)$. Therefore we get $A(pqr) \leq A(pqs)$. By symmetry we have $A(pqr) \leq A(pqs)$, which gives us $A(pqr) = A(pqs)$. □

One immediate corollary from this theorem is that we find another infinite family of flat cyclotomic polynomials of order three.

Corollary 3.2.9. *If $2 < p < q < r$ are primes and $r \equiv -1 \pmod{pq}$ then $\Phi_{pqr}(x)$ is flat.*

Another nice thing about this theorem is that it lets us reduce the number of $\Phi_{pqr}(x)$ we have to compute to know all the heights $A(pqr)$ for fixed p and q. Now we only have to compute $\Phi_{pqr}(x)$ for $\frac{(p-1)(q-1)}{2}$ primes r. Since we know that for $r \equiv 1 \pmod{pq}$, $\Phi_{pqr}(x)$ is flat, we only need to compute $\Phi_{pqr}(x)$ for $\frac{(p-1)(q-1)-1}{2}$ values of r. The following is an example of how this could be applied.

Example 3.2.10. Given primes $p = 3$ and $q = 5$. We are going to compute the heights of all values of cyclotomic polynomials of order three with odd prime divisors 3, 5 and r. For $r \equiv \pm 1 \pmod{pq}$, we know that $A(3 \cdot 5 \cdot r) = 1$. Using Sage we find that $A(3 \cdot 5 \cdot 17) = 2$, $A(3 \cdot 5 \cdot 19) = 2$ and we already know that $A(3 \cdot 5 \cdot 7) = A(105) = 2$.

This results in that for an odd prime r we have $A(3 \cdot 5 \cdot r) = \begin{cases} 1 \text{ if } r \equiv \pm 1 \pmod{15}, \\ 2 \text{ else.} \end{cases}$

Now for primes $p = 5$ and $q = 7$ we compute with Sage: $A(5 \cdot 7 \cdot 37) = 2$, $A(5 \cdot 7 \cdot 73) = 2$, $A(5 \cdot 7 \cdot 109) = 2$, $A(5 \cdot 7 \cdot 41) = 2$, $A(5 \cdot 7 \cdot 43) = 2$, $A(5 \cdot 7 \cdot 79) = 2$, $A(5 \cdot 7 \cdot 11) = 2$, $A(5 \cdot 7 \cdot 13) = 2$, $A(5 \cdot 7 \cdot 191) = 2$, $A(5 \cdot 7 \cdot 17) = 3$.

This means that for odd primes r we get $A(5 \cdot 7 \cdot r) = \begin{cases} 1 \text{ if } r \equiv \pm 1 \pmod{35}, \\ 3 \text{ if } r \equiv \pm 17 \pmod{35}, \\ 2 \text{ else.} \end{cases}$

What we see in this example is that when we set $(p, q) = (3, 5)$ or $(5, 7)$, the height of $\Phi_{pqr}(x)$ does not suddenly blow up. One might therefore think that for $A(pqr)$ is bounded by q and p. This thought is correct. In fact $A(pqr)$ is heavily bounded by just the value of p as was proven by Zhou and Zhang [10] in an unpublished paper in 2009. The theorem that they proved is called the corrected Beiter conjecture.

Theorem 3.2.11. ***Corrected Beiter conjecture:*** *For odd primes $p < q < r$, we have $A(pqr) \leq \frac{2p}{3}$.*

It is called the Corrected Beiter conjecture, since it is a variation on a conjecture made earlier by Beiter, which was: $A(pqr) \leq \frac{p+1}{2}$ for odd distinct primes p, q, r. This was proven to be false for all $p \geq 11$ by Gallot and Moree [4].

Chapter 4

Cyclotomic polynomials of order four

In this chapter our aim is to find an infinite family of flat cyclotomic polynomials of order four. We are going to do this by proving a theorem which says that if $n = p_1 \cdot ... \cdot p_r$, a product of distinct odd primes, the set of coefficients of $\Phi_{ns}(x)$ is the same as the set of coefficients of $\Phi_{nt}(x)$, if t and s are primes satisfying $n < s < t$ and $t \equiv s \pmod{n}$. A consequence of this will be that $A(nt) = A(ns)$. This is a slightly different approach than the one taken in Theorem 3.2.7, where we proved the result for the height of cyclotomic polynomials of order three directly rather than looking at the coefficients. Another difference is the extra constraint $n < s < t$ rather than just the largest prime in the factorization of n being less than s and t. The reason for the different approach is that a direct generalization of Theorem 3.2.7 does not hold for cyclotomic polynomials of order four. For instance take $n = 5 \cdot 7 \cdot 13 = 455$ and set primes $s = 17$ and $t = 4567$. We have $17 \equiv 4567 \pmod{455}$, however using Sage we find that $A(455 \cdot 17) = 5$ and $A(455 \cdot 4567) = 6$. We will prove that for primes s and t satisfying the constraint $n < s < t$, the generalization does hold. The first person who came up with this approach was Kaplan [6] and we will follow it throughout this chapter.

4.1 Periodicity of the set of coefficients of cyclotomic polynomials

As mentioned in the introduction of this chapter, our aim is to prove that for primes s and t satisfying $n < s < t$ and $s \equiv t \pmod{n}$, the set of coefficients of $\Phi_{ns}(x)$ is the same as the one of $\Phi_{nt}(x)$. We first abbreviate the set of coefficients of $\Phi_n(x)$.

Definition 4.1.1. *Let* $V_n = \{$*coefficients of* $\Phi_n(x)\}$.

For some cyclotomic polynomials the set of coefficients is easy to compute.

Example 4.1.2. For a prime p, we have $V_p = \{1\}$, moreover $V_1 = \{-1, 1\}$. For distinct primes p and q we have $V_{pq} = \{-1, 0, 1\}$.

In order to give our proof it is useful to consider the following polynomial.

Definition 4.1.3. *We define the* $\boldsymbol{n^{th}}$ ***inverse cyclotomic polynomial****, denoted* $\Psi_n(x)$*, as* $\Psi_n(x) := \dfrac{x^n - 1}{\Phi_n(x)}$*. This is the same as saying* $\Psi_n(x) = \displaystyle\prod_{d|n\,,\, d\neq n} \Phi_d(x)$*.*

We have already seen some inverse cyclotomic polynomials being used throughout this document. In particular we used $\Psi_{pq}(x) = \Phi_1(x) \cdot \Phi_p(x) \cdot \Phi_q(x)$ for distinct primes p and q, which we denoted by $-\displaystyle\sum_{m=0}^{p+q-1} \chi_m x^m$, throughout Chapter 3.

The main lemma that we are going to prove in order to prove the result of this section is going to be a generalization of Proposition 3.1.5. The proof is also very similar to the proof given for Proposition 3.1.5. Before we do this we introduce some notation that is used throughout this section.

Notation 4.1.4. *Throughout this section we denote:*
$\Phi_n(x) = \displaystyle\sum_{j=0}^{\varphi(n)} a_j x^j, \quad \Psi_n(x) = \sum_{m=0}^{n-\varphi(n)} \chi_m x^m.$
For primes $t, s \nmid n$ *we write* $\Phi_{ns}(x) = \displaystyle\sum_{l=0}^{\varphi(n)\cdot(s-1)} c_l x^l$ *and* $\Phi_{nt}(x) = \displaystyle\sum_{i=0}^{\varphi(n)\cdot(t-1)} d_i x^i$*.*

The first three polynomials are used in the proof of the following proposition and all four are used in the proof of the theorem.

Proposition 4.1.5. *Given distinct primes* $p_1, ..., p_r, s$ *and let* $n = p_1 \cdot ... \cdot p_r$*. Then any coefficient* c_l *with* $0 \leq l \leq \deg(\Phi_{ns}(x))$ *of* $\Phi_{ns}(x)$ *is given by* $c_l = -\displaystyle\sum_{(m,j)\in S_l} \chi_m a_j$*, where* $S_l = \{(m, j) \,|\, \chi_m \neq 0\,,\, m + sj \equiv l \,(mod\ n)\,,\, m + sj \leq l\}$*.*

Proof. Since $s \nmid n$, we can write $\Phi_{ns}(x) \cdot \Phi_n(x) = \Phi_n(x^s)$ by Proposition 1.2.7. Multiplying by $-\Psi_n(x)$ on both sides yields

$$(1 - x^n) \cdot \Phi_{ns}(x) = -\Psi_n(x)\Phi_n(x^s). \tag{4.1}$$

Now fix any coefficient c_l of $\Phi_{ns}(x)$ such that $0 \leq l \leq \deg(\Phi_{ns}(x))$. We can write l uniquely in the form $l = d \cdot n + k$ with $0 \leq k < n$ and $d \in \mathbb{N}$. Now for $0 \leq t \leq d$ we define $l_t = t \cdot n + k$, which makes $l_d = l$.

The term with degree l_t on the left side of (4.1) is $c_{l_0} x^{l_0}$ if $t = 0$ and $(c_{l_t} - c_{l_{t-1}})x^{l_t}$ if

$t \geq 1$. On the right side of (4.1) the term with degree l_t is $(-\sum_{\substack{m+sj=l_t \\ m\geq 0}} \chi_m a_j)x^{l_t}$.

Since terms with the same degree must be equal on both sides, we get the equations $c_{l_0} = -\sum_{\substack{m+sj=l_0 \\ m\geq 0}} \chi_m a_j$ and $c_{l_t} - c_{l_{t-1}} = -\sum_{\substack{m+sj=l_t \\ m\geq 0}} \chi_m a_j$ for all $1 \leq t \leq d$. Adding all these equations yields $c_{l_0} - c_{l_0} + c_{l_1} - ... + c_{l_{d-1}} - c_{l_{d-1}} + c_{l_d} = \sum_{0\leq t\leq d} (-\sum_{\substack{m+sj=l_t \\ m\geq 0}} \chi_m a_j)$. We see that on the left hand side the only term that survives is $c_{l_d} = c_l$.

Notice that the set $\{l_t \,|\, 0 \leq t \leq d\}$ is exactly the set $\{a \,|\, a \equiv l \,(\mathrm{mod}\, n)\,, 0 \leq a \leq l\}$. This means that we can write $\sum_{0\leq t\leq d} (-\sum_{\substack{m+sj=l_t \\ m\geq 0}} \chi_m a_j)$, as $-\sum_{(m,j)\in S_l} \chi_m a_j$, where S_l is given by $S_l = \{(m,j) \,|\, \chi_m \neq 0\,,\, m + sj \equiv l \,(\mathrm{mod}\, n)\,,\, m + sj \leq n\}$. This yields the desired formula $c_l = -\sum_{(m,j)\in S_l} \chi_m a_j$ with S_l given in the line above. □

Next we are going to use this lemma to prove the main theorem. To prove that $V_{nt} = V_{ns}$, we first take any coefficient of $\Phi_{ns}(x)$ and prove that it equals some coefficient of $\Phi_{nt}(x)$, which implies $V_{ns} \subset V_{nt}$ and then we do this the other way around, which implies $V_{nt} \subset V_{ns}$. The longest part of the proof is $V_{nt} \subset V_{ns}$ because we have $t > s$. We distinguish between several cases in this part. The following theorem was proven by Kaplan [6].

Theorem 4.1.6. *Given distinct odd primes $p_1, ..., p_r, t, s$ such that $n := p_1 \cdot ... \cdot p_r < s < t$ and $s \equiv t \,(mod\ n)$. Then $V_{ns} = V_{nt}$.*

Proof. We are going to assume that n is the product of at least two distinct odd primes since we already know V_{pq}. This implies that $n \geq 15$.

First we prove that $V_{ns} \subset V_{nt}$. For $0 \leq l \leq \deg(\Phi_{ns}(x)) = \varphi(n) \cdot (s-1)$, let c_l be a coefficient of $\Phi_{ns}(x)$. By last lemma we have that $c_l = -\sum_{(m,j)\in S_l} \chi_m a_j$, where S_l is the set of pairs $S_l = \{(m,j) \,|\, \chi_m \neq 0\,,\, m + sj \equiv l \,(\mathrm{mod}\, n)\,,\, m + sj \leq l\}$.

We can write $l = ks + \alpha$ with $k \in \mathbb{N}$ and $0 \leq \alpha < s$. Now we define $i := kt + \alpha$ and we consider the coefficient d_i of $\Phi_{nt}(x)$. Since we have $0 \leq ks + \alpha \leq \varphi(n) \cdot (s-1)$, we must have $k < \varphi(n)$. Therefore we get

$$kt + \alpha = k(t-s) + ks + \alpha \leq k(t-s) + \varphi(n)(s-1) < \varphi(n)(t-s) + \varphi(n)(s-1) = \varphi(n)(t-1).$$

So we have $0 \leq i \leq \varphi(n)(t-1) = \deg(\Phi_{nt}(x))$, therefore by the lemma $d_i = -\sum_{(m,j)\in T_i} \chi_m a_j$, where T_i is given by $T_i = \{(m,j) \,|\, \chi_m \neq 0\,,\, m + tj \equiv i \,(\mathrm{mod}\, n)\,,\, m + tj \leq i\}$. We are going to prove that S_l and T_i are the same sets, which will impy that $c_l = d_i$.

Since we have $s \equiv t \,(\mathrm{mod}\, n)$ by assumption, we get $ks + \alpha \equiv kt + \alpha \,(\mathrm{mod}\, n)$, therefore $l \equiv i \,(\mathrm{mod}\, n)$. So if we have $m + sj \equiv l \,(\mathrm{mod}\, n)$ for some pair (m,j) then we also have

$m + tj \equiv i \,(\mathrm{mod}\ n)$ and vice versa.

Now suppose that we have $m + sj \leq l$ with $\chi_m \neq 0$, so $0 \leq m \leq \deg(\Psi_n(x)) = n - \varphi(n)$. Since $l = ks + \alpha$, we have $m + sj \leq l$ if and only if $j \leq k + \lfloor \frac{\alpha - m}{s} \rfloor$. Since we have $0 \leq m \leq n - \varphi(n) < n < s$ and $0 \leq \alpha < s$, we get $-s < \alpha - m < s$. So we get $\lfloor \frac{\alpha - m}{s} \rfloor = 0$ for $m \leq \alpha$ and $\lfloor \frac{\alpha - m}{s} \rfloor = -1$ for $m > \alpha$. We therefore see that, if we assume that $\chi_m \neq 0$, for a pair (m, j) with $m > \alpha$ we have $m + sj \leq l$ if and only if $j \leq k - 1$ and for $m \leq \alpha$ we have $m + sj \leq l$ if and only if $j \leq k$.

Let (m, j) still be a pair with $\chi_m \neq 0$. Since $i = tk + \alpha$, we have $m + tj \leq i$ if and only if $j \leq k + \lfloor \frac{\alpha - m}{t} \rfloor$. Since we have $s < t$, we get $-t < \alpha - m < t$, which means that $\lfloor \frac{\alpha - m}{t} \rfloor = 0$ if $m \leq \alpha$ and $\lfloor \frac{\alpha - m}{t} \rfloor = -1$ if $m > \alpha$. This means that, if we assume $\chi_m \neq 0$, for a pair (m, j) with $m \leq \alpha$ we have $m + tj \leq i$ if and only if $j \leq k$ and for $m > \alpha$ we have $m + tj > i$ if and only if $j \leq k - 1$.

If we compare the previous two paragraphs we can see that for $\chi_m \neq 0$, both in the $m \leq \alpha$ and the $m > \alpha$ case $m + sj \leq l$ happens if and only if $m + tj \leq i$. Together with $m + sj \equiv l \,(\mathrm{mod}\ n)$ if and only if $m + tj \equiv i \,(\mathrm{mod}\ n)$, this implies that the sets S_l and T_i are the same. By the first part we therefore get $c_l = d_i$. Since c_l was chosen arbitrarily we conclude that $V_{ns} \subset V_{nt}$.

Now we are going to prove that $V_{nt} \subset V_{ns}$. Given any coefficient d_i of $\Phi_{nt}(x)$, since for $n \geq 2$, $\Phi_n(x)$ is symmetric, we may assume that $0 \leq i \leq \frac{\deg(\Phi_{nt}(x))}{2} = \frac{\varphi(n)}{2} \cdot (t - 1)$. Again we have $d_i = -\sum_{(m,j) \in T_i} \chi_m a_j$ by the lemma, where T_i is given by the set of pairs $T_i = \{(m, j) \,|\, \chi_m \neq 0\,,\ m + tj \equiv i \,(\mathrm{mod}\ n)\,,\ m + tj \leq i\}$.

We write can write $i = kt + \beta$ with $k \in \mathbb{N}$ and $0 \leq \beta < t$. Since $kt + \beta \leq \frac{\varphi(n)}{2} \cdot (t - 1)$ we have $k < \frac{\varphi(n)}{2}$. Now we define $l := ks + \alpha$, where α is the unique value satisfying $0 \leq \alpha < n$ and $\alpha \equiv \beta \,(\mathrm{mod}\ n)$.

Since $\alpha < n < s$, we have $ks + \alpha < s(\frac{\varphi(n)}{2} + 1)$. Since $n > 15$ we get $\frac{\varphi(n)}{2} + 1 \leq \varphi(n) - 1$, therefore we get $ks + \alpha < s(\varphi(n) - 1) < (s - 1)\varphi(n)$ since $\varphi(n) < n < s$. So we get $0 \leq l \leq (s - 1)\varphi(n) = \deg(\Phi_{ns}(x))$, therefore the lemma gives us $c_l = -\sum_{(m,j) \in S_l} \chi_m a_j$, where $S_l = \{(m, j) \,|\, \chi_m \neq 0\,,\ m + sj \equiv l \,(\mathrm{mod}\ n)\,,\ m + sj \leq l\}$. As in the previous part we are going to prove that $S_l = T_i$, which will imply $d_i = c_l$.

As we have $l \equiv i \,(\mathrm{mod}\ n)$, since $s \equiv t \,(\mathrm{mod}\ n)$ and $\alpha \equiv \beta \,(\mathrm{mod}\ n)$, we again have $m + sj \equiv l \,(\mathrm{mod}\ n)$ if and only if $m + tj \,(\mathrm{mod}\ n)$.

Similar to the first part, we have $m + sj \leq l$ if and only if $j \leq k + \lfloor \frac{\alpha - m}{s} \rfloor$ and we have

$m + tj \leq i$ if and only if $j \leq k + \lfloor \frac{\beta - m}{t} \rfloor$.

Suppose that for $\chi_m \neq 0$ we have $m > \beta$. Since $0 \leq m < n - \varphi(n) < n$, we then must have $0 \leq \beta < n$. By definition of α this means $\beta = \alpha$, so we get $l = ks + \alpha$ and $i = kt + \alpha$ with $0 \leq \alpha < n < s$. We have already seen in the previous part of the proof that this leads to $S_l = T_i$.

Now we look at the case where for all $\chi_m \neq 0$ we have $m < \beta$. Because we have $0 \leq m \leq n - \varphi(n) < t$ and $0 \leq \beta < t$, we have $0 < \beta - m < t$, which implies $\lfloor \frac{\beta - m}{t} \rfloor = 0$. We have $0 \leq \alpha < n < s$ and $0 \leq m \leq n - \varphi(n) < s$, and thus we have $-s < \alpha - m < s$, therefore $\lfloor \frac{\alpha - m}{s} \rfloor \in \{-1, 0\}$. This means that we have $k + \lfloor \frac{\alpha - m}{s} \rfloor \leq k + \lfloor \frac{\beta - m}{t} \rfloor$. So we see that $m + sj \leq l$ implies that $j \leq k + \lfloor \frac{\alpha - m}{s} \rfloor \leq k + \lfloor \frac{\beta - m}{t} \rfloor$, which implies $m + tj \leq i$.

Suppose that we have $m + tj \leq i$ and $m + tj \equiv i \pmod{n}$, however $m + sj > l$. We are going to show that this is not possible. We have $m + sj > l$ if and only if $j > k + \lfloor \frac{\alpha - m}{s} \rfloor$ and $m + tj \leq i$ if and only if $j \leq k$. Since we had $\lfloor \frac{\alpha - m}{s} \rfloor \in \{-1, 0\}$, this means that we must have $j = k$ and $\lfloor \frac{\alpha - m}{s} \rfloor = -1$.

The condition $m + tj \equiv i \pmod{n}$ is equivalent to $m + sj \equiv l \pmod{n}$, which yields $m + sk \equiv sk + \alpha \pmod{n}$, therefore $m \equiv \alpha \pmod{n}$. Since we have $\lfloor \frac{\alpha - m}{s} \rfloor = -1$, we have $\alpha < m$ and because $0 \leq \alpha < n$, we get $m \geq n$. However we had $\chi_m \neq 0$, which meant that $m \leq \deg(\Psi_n(x)) = n - \varphi(n)$, which is a contradiction. Therefore $m + tj \leq i$ and $m + sj \equiv l \pmod{n}$ implies that $m + sj \leq l$.

Now we have all the tools to show that $S_l = T_i$ in the case of $m < \beta$ for all $\chi_m \neq 0$. Suppose that $(m, j) \in S_l$, then we have $\chi_m \neq 0$ with $m + sj \leq l$, which implies that $m + tj \leq i$ and we have $m + sj \equiv l \pmod{n}$, which implies that $m + tj \equiv i \pmod{n}$. Therefore $(m, j) \in T_i$ if $(m, j) \in S_l$.

Now suppose that (m, j) is an element of T_i, then we have $\chi_m \neq 0$, $m + tj \equiv i \pmod{n}$ and $m + tj \leq i$, which means that $m + sj \leq l$ and $m + sj \equiv l \pmod{n}$, and thus (m, j) is an element of S_l.

Since in both cases for β we get $S_l = T_i$, we have $c_l = d_i$. Since d_i was arbitrary, we get $V_{nt} \subset V_{ns}$, which yields $V_{ns} = V_{nt}$. We conclude that $V_{ns} = V_{nt}$ for $n = p_1 \cdot ... \cdot p_r$ and t, s primes satisfying $t, s > n$ and $t \equiv s \pmod{n}$. □

Now that we have proven this theorem for a general cyclotomic polynomial $\Phi_n(x)$ it allows us to prove a similar theorem for the height of general cyclotomic polynomials.

Corollary 4.1.7. *Let $p_1, ..., p_r, s, t$ be distinct primes and let $n := p_1 \cdot ... \cdot p_r < s, t$. Then $A(n \cdot s) = A(n \cdot t)$.*

Proof. Since the set of coefficients of $\Phi_{ns}(x)$ and $\Phi_{nt}(x)$ is the same, they have the same maximum of the absolute value of their coefficients. □

This allows us to show that there exist infinitely many flat cyclotomic polynomials of order four, though not in such an elegant way as we did in last chapter for order three.

Corollary 4.1.8. *There exist infinitely many flat cyclotomic polynomials of order four.*

Proof. Using Sage we find that $A(3 \cdot 5 \cdot 31 \cdot 929) = 1$. By Dirichlet's theorem on arithmetic progressions, there exist infinitely many primes $p > 3{\cdot}5{\cdot}31$ that satisfy $p \equiv 929 \pmod{3{\cdot}5{\cdot}31}$. By the previous corollary we get that for all of these primes p we have $A(3 \cdot 5 \cdot 31 \cdot p) = 1$. □

4.2 More results on flat cyclotomic polynomials and open questions regarding them

To this day the coefficients of cyclotomic polynomials are still being studied. In 2010 Kaplan [6] made an interesting conjecture.

Conjecture 4.2.1. ([6]) Let n be any number and let p be a prime. Then $A(pn) > 1$ if $A(n) > 1$.

Suppose that we would know all flat cyclotomic polynomials of a certain order k. Then this conjecture would imply that, when searching for flat cyclotomic polynomials of order $k+1$, we only need to consider those of the form $\Phi_{pn}(x)$, where p is a prime and $\Phi_n(x)$ is a flat cyclotomic polynomial of order k. Although we know all flat cyclotomic polynomials of order two, this does not tell us much about those of order three. The conjecture could however tell us more about those of order four in particular if Conjecture 4.2.3 is true.

Later in 2012, Elder [3] wrote an unpublished paper on flat cyclotomic polynomials. By introducing and utilizing 'pseudo-cyclotomic polynomias' he was able to expand the knowledge about flat cyclotomic polynomials. In this paper the existence of another infinite family of cyclotomic polynomials of order three was proven.

Theorem 4.2.2. *For primes $p < q < r$, if there exists a positive integer ω such that $r \equiv \pm\omega \,(mod\ pq)$, $p \equiv 1 \,(mod\ \omega)$ and $q \equiv 1 \,(mod\ \omega p)$, then $\Phi_{pqr}(x)$ is flat.*

The following conjecture about cyclotomic polynomials of order three was made in this paper.

Conjecture 4.2.3. For odd primes $p < q < r$, if $A(pqr) = 1$ then $r \equiv \pm 1 \pmod{pq}$ or $q \equiv \pm 1 \pmod{p}$

In the same paper Elder generalized the infinite family of cyclotomic polynomials of order four found by Kaplan, which is mentioned in Corollary 4.1.8.

Theorem 4.2.4. *Let $p < q < r < s$ be primes, that satisfy $q \equiv -1 \,(mod\, p)$ and $r \equiv \pm 1 \,(mod\, pq)$ as well as $s \equiv \pm 1 \,(mod\, pqr)$, then $\Phi_{pqrs}(x)$ is flat.*

This is a generalization since $5 \equiv -1 \,(\text{mod } 3)$ and $31 \equiv 1 \,(\text{mod } 15)$ and $3 \cdot 5 \cdot 31 = 465$, which means $929 \equiv -1 \,(\text{mod } 465)$. A question that remains unanswered is whether there exist flat cyclotomic polynomials of order five.

The following conjecture might explain to the reader why we did not mention any cyclotomic polynomials of order higher than four.

Conjecture 4.2.5. There are no flat cyclotomic polynomials of order five.

This conjecture is very likely to be true since no flat cyclotomic polynomials of order five has been found yet (though the heights of many cyclotomic polynomials of order five have been computed). Another reason that this is probable is that Elder [3] proved that for primes $p < q < r < s < t$ if $r \equiv \pm 1 \,(\text{mod } pq)$, $s \equiv \pm 1 \,(\text{mod } pqr)$ and $t \equiv \pm 1 \,(\text{mod } pqrs)$, then $A(pqrst) > 1$, while in the order four and order three cases similar constraints on the primes yielded a flat cyclotomic polynomial.

Note that if both this conjecture and Kaplans conjecture that $A(pn) > 1$ if $A(n) > 1$ are true, then this would imply that all flat cyclotomic polynomials have order less or equal to four.

Bibliography

[1] Gennady Bachman. "Flat Cyclotomic Polynomials of Order Three". *Bulletin of the London Mathematical Society* 38.1 (2006), pp. 53–60. DOI: https://doi.org/10.1112/S0024609305018096.

[2] P. T. Bateman, C. Pomerance, and R. C. Vaughan. "On the size of the coefficients of the cyclotomic polynomial". In: *Topics in classical number theory*. Ed. by Gábor Halász. Vol. I. Colloquia Mathematica Societatis János Bolyai 34. (Budapest, 20–25 July 1981). Note that an article with the same title had been published by Bateman alone in 1982. MR:781138. Zbl:0547.10010. Amsterdam: North-Holland, 1984, pp. 171–202. ISBN: 9789638021595.

[3] Sam Elder. *Flat Cyclotomic Polynomials: A New Approach*. 2012. arXiv: 1207.5811 [math.NT].

[4] Yves Gallot and Pieter Moree. "Ternary cyclotomic polynomials having a large coefficient". *Journal für die reine und angewandte Mathematik (Crelles Journal)* 632 (Jan. 2008). DOI: 10.1515/CRELLE.2009.052.

[5] N. Kaplan. "Flat cyclotomic polynomials of order three". *Journal of Number Theory* 127 (2007), pp. 118–126.

[6] Nathan Kaplan. "Flat Cyclotomic Polynomials of Order Four and Higher". *Integers* 10 (Jan. 2010), pp. 357–363. DOI: 10.1515/INTEG.2010.030.

[7] T. Y. Lam and K. H. Leung. "On the Cyclotomic Polynomial Phipq (X)". *The American Mathematical Monthly* 103.7 (1996), pp. 562–564.

[8] Helmut Maier. "The Coefficients of Cyclotomic Polynomials". In: *Analytic Number Theory: Proceedings of a Conference in Honor of Paul T. Bateman*. Ed. by Bruce C. Berndt et al. Boston, MA: Birkhäuser Boston, 1990, pp. 349–366. ISBN: 978-1-4612-3464-7. DOI: 10.1007/978-1-4612-3464-7_22. URL: https://doi.org/10.1007/978-1-4612-3464-7_22.

[9] Jiro Suzuki. "On coefficients of cyclotomic polynomials". *Proceedings of the Japan Academy, Series A, Mathematical Sciences* 63.7 (1987), pp. 279–280. DOI: 10.3792/pjaa.63.279.

[10] Jia Zhao and Xianke Zhang. *A proof of the Corrected Beiter conjecture*. 2009. arXiv: 0910.2770 [math.NT].