On coefficients of cyclotomic polynomials

Alhashemi, Wa'el

W. Alhashemi
W.Alhashemi@protonmail.com

On coefficients of cyclotomic polynomials

Bachelor thesis

28 June 2024

Thesis supervisor: Dr. E. Rosu

Leiden University
Mathematical Institute

Contents

1 Introduction

The irreducible factors with integer coefficients of the polynomial $X^n - 1$ are called the cyclotomic polynomials. The cyclotomic polynomials are quite well known and extensively studied because of their applications in number theory, algebra, combinatorics and even cryptography [24]. There are still many open problems concerning the polynomials despite their simple appearance. Especially the coefficients of these polynomials are surprising. It is well known that all coefficients of these cyclotomic polynomials are integers, in fact when one studies these polynomials with low degree one expects these coefficients to all be either $0, 1$ or -1. Surprisingly this is not the case (1.1.2), as one increases the degree more possible coefficients appear, in fact these coefficients in magnitude are unbounded [17]. Part of the reason why this is surprising and why historically this was not expected is because calculations on cyclotomic polynomials are rather difficult to do with pen and paper. In this thesis I will study these coefficients in detail. For cyclotomic polynomials of low degree, where the degree is composed of three or less distinct odd prime numbers, there is a known optimal bound for the corresponding coefficients. But much less is known when the degree has four or more distinct odd prime factors.

In section 2 I will define the setting of these polynomials and prove everything along the way. In section 3.1 I will give an alternative proof of Lam & Leung's theorem, which completely describes the coefficients of cyclotomic polynmials where the degree is composed of two distinct odd primes. The proof uses techniques from Kaplan's Lemma and its proof, which is described in 3.2. In section 3.3 I will give three formulas that describe the coefficients of cyclotomic polynomials where the degree is composed of four distinct odd prime numbers. I will use one of these formulas to give a bound 3.4.3 on the coefficients of these 'quaternary' cyclotomic polynomials. The bound is known and assumes the Corrected Sister Beiter conjecture in both my thesis and literature. In section 4, I will explain the algorithms by Arnold & Monogan that I have used to compute histograms and other graphs. Here I will also show data computed using these algorithms and suggest interesting further research. In the final section, section 5, I will very briefly describe the connection between coefficients of cyclotomic polynomials and prime gaps. Finally In the same section I will point towards further interesting research related to prime gaps and cyclotomic polynomials.

1.1 Definitions

In general the field I am working in is $\mathbb{C}$. The polynomial that is at the forefront of this thesis is the cyclotomic polynomial.

Definition 1.1.1. Let $n \geq 1$. The n-th Cyclotomic Polynomial is defined as

$$\phi_n(X) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^*}^{n} (X - \xi_n^i).$$

Where ξ_n^i is a n-th primitive root of unity. «

This definition implies then that

$$X^n - 1 = \prod_{d|n} \phi_d.$$

With both these definitions it is possible to compute some examples.

Example 1.1.2.

$$\begin{aligned}
\phi_1(X) &= X - 1 \\
\phi_2(X) &= X + 1 \\
\phi_5(X) &= X^4 + X^3 + X^2 + X + 1 \\
\phi_9(X) &= X^6 + X^3 + 1 \\
\phi_{105}(X) &= X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - \mathbf{2} \cdot X^{41} - X^{40} - X^{39} \\
&\quad + X^{36} + X^{35} + X^{34} + X^{33} + X^{32} + X^{31} - X^{28} - X^{26} - X^{24} - X^{22} \\
&\quad - X^{20} + X^{17} + X^{16} + X^{15} + X^{14} + X^{13} + X^{12} - X^9 - X^8 - \mathbf{2} \cdot X^7 - X^6 - X^5 + X^2 + X + 1.
\end{aligned}$$

«

When one computes the first few n-th cyclotomic polynomials one may suspect that all coefficients are bounded in magnitude by 1. The example above for $n = 105$ shows that this is not the case in general.

The next polynomial I want to introduce is closely related to the cyclotomic polynomial.

Definition 1.1.3. Let $n \geq 1$. The nth Inverse Cyclotomic Polynomial is defined as

$$\psi_n(X) = \prod_{\substack{1 \leq i \leq n \\ \gcd(i,n) > 1}}^{n} (X - \xi_n^i) = \frac{X^n - 1}{\phi_n}.$$

Where ξ_n^i is a n-th primitive root of unity. «

This definition similarly implies that

$$\psi_n = \prod_{d|n, d<n} \phi_d$$

I will sometimes write $a_n(j)$ for the j-th coefficient of ϕ_n and or ψ_n. I do this to specify the degree of the polynomial I am working with explicitly. For convenience I will also define the following terms.

Definition 1.1.4. Whenever n is the product of i distinct odd primes $p_1 p_2 \dots p_i$, I will call ϕ_n or ψ_n binary, ternary and quaternary if $i = 2, i = 3, i = 4$ respectively. I sometimes refer to the coefficients of these polynomials similarly. For example If a_i is term of a ternary cyclotomic polynomial, I will call a_i ternary. «

Now with above definitions given I can start introducing the main topic of this thesis.

Definition 1.1.5. Let $n \geq 1$ and f be an arbitrary polynomial with integer coefficients. Define

$$A(f) := max_{j \geq 0} |a_n(j)|$$

I will call A the height of f. When discussing cyclotomic polynomials I write out $A(\phi_n(X)) = A(n)$ whenever possible and clear. A(n) (inverse) cyclotomic polynomial is called **flat** when the height equals one. «

I will end this section with some more definitions that mainly aid in proving and describing properties in the next section.

Definition 1.1.6. The jump of ϕ_n and ψ_n;

$$J(\phi_n(X)) := max_{j \geq 1} |a_n(j) - a_n(j-1)|, J(\psi_n(X)) := max_{j \geq 1} |b_n(j) - b_n(j-1)|$$

I will call this value the jump. For convenience I write out $J(\phi_n(X)) = J(n)$ or $J(\psi_n(X)) = J(n)$ whenever it is clear. «

Definition 1.1.7. Let $f = \sum_i a_i X^i$ be a polynomial in $K\mathbb{X}$ some arbitrary field K.

$$G(\phi_n(X)) := max\{|i - j| : a_i \neq 0, a_j \neq 0\}$$

I will call this value the gap. «

There are many questions and interesting properties related to the gap of a cyclotomic polynomial [1] [12] [27]. These properties although mentioned here will not be discussed in detail within this thesis.

Definition 1.1.8. Let $f \in \mathbb{C}[X]$ be a polynomial with polynomial degree n. Then define

$$f^* := X^n \cdot f(X^{-1}).$$

f^* is called the the **reciprocal** polynomial or reflected polynomial. If $f = f^*, f = -f^*$ then f is called **palindromic** and **antipalindromic** respectively. «

Here the term palindromic is used because the definition implies that the coefficients of the palindromic polynomial are read the same when reading from the left to the right or vice versa.

Definition 1.1.9. Let

$$\text{rad}(n) := \Pi_{p|n} p$$

where p is prime, be the radical of n. «

Definition 1.1.10. The Möbius function $\mu : \mathbb{Z}_{>0} \to \mathbb{Z}$ is defined as

$$\mu(n) = \begin{cases} 0 & \text{if there exists a } p \text{ such that } p^2 | n \\ (-1)^t & \text{if } n \text{ is the product of } t \text{ distinct primes} \end{cases}$$

«

2 Basic Properties

The Möbius function happens to be a useful tool in proving properties of cyclotomic polynomials. But before I can use it I will have to prove some of its properties. It is clear that the Möbius function is multiplicative, on top of that the Möbius function has the following convenient property;

Proposition 2.0.1. *For $n \in \mathbb{Z}_{>0}$*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{else} \end{cases}$$

«

My proof of this property will make use of induction.

Proof. For $n = 1$ the proposition obviously holds. Next take the prime decomposition of $n > 1$, so $n = p_1^{e_1} \dots p_k^{e_k}$. If a divisor d of n has a factor $p_i^{e_i}$ with $e_i > 1$ then $\mu(d) = 0$. So thus

$$\sum_{d|n} \mu(d) = \sum_{d|p_1 \dots p_k} \mu(d).$$

Now I will with induction on the count of prime factors k, prove that

$$\sum_{d|p_1 \dots p_k} \mu(d) = 0.$$

($k = 1$) Suppose $n = p_1^{e_1}$ then $\sum_{d|p_1} = \mu(1) + \mu(p_1) = 1 + (-1) = 0$. (induction step, IH). Suppose for all p_i with $k \geq i > 1$

$$\sum_{d|p_1 \dots p_i} \mu(d) = 0.$$

Now take

$$\begin{aligned} \sum_{d|p_1 \dots p_k \cdot p_{k+1}} \mu(d) &= \left(\sum_{d|p_1 \dots p_k} \mu(d) \right) + \left(\sum_{d|p_1 \dots p_k} \mu(p_{k+1} d) \right) \\ &= \left(\sum_{d|p_1 \dots p_k} \mu(d) \right) + \left(\sum_{d|p_1 \dots p_k} \mu(d)\mu(p_{k+1}) \right) \\ &\overset{\text{IH}}{=} 0 + 0 \cdot \mu(p_{k+1}) = 0. \end{aligned}$$

In the second equation I used the fact that $p_{k+1} \nmid d$ for all $d | p_1 \dots p_k$. This together with the base case proves the proposition by induction. □

The following function is especially useful with calculations.

Proposition 2.0.2. *(The Möbius inversion function) Let $f, g : \mathbb{Z}_{>0} \to \mathbb{C}$ for all $n \in \mathbb{Z}_{>0}$ have to following property;*

$$\sum_{d|n} f(d) = g(n).$$

Then for every $n \in \mathbb{Z}_{>0}$

$$f(n) = \sum_{d|n} \mu(d) g(n/d).$$

«

Proof. Suppose n has k non-zero divisors $1 = d_1 < \cdots < d_k = n$. Also define

$$h_j(d) = \begin{cases} f(d) & \text{if } d|\frac{n}{j} \\ 0 & \text{else} \end{cases}.$$

Then

$$\begin{aligned}
\mu(d_i)g(n/d_i) &= \Big(\mu(d_i)\cdot h_{d_i}(1) + \mu(d_i)\cdot h_{d_i}(d_2) + \cdots + \mu(d_i)\cdot h_{d_i}(d_k)\Big) \\
\sum_{i=1}^{k} \mu(d_i)g(n/d_i) &= \sum_{i=1}^{k} \mu(d_i)\cdot h_{d_i}(1) + \sum_{i=1}^{k} \mu(d_i)\cdot h_{d_i}(d_2) + \cdots + \sum_{i=1}^{k} \mu(d)\cdot h_{d_i}(d_k) \\
&= \sum_{i=1}^{k} \mu(d_i)\cdot f(1) + \sum_{i=1}^{k} \mu(d_i)\cdot f(d_2) + \cdots + \sum_{i=1}^{k} \mu(d)\cdot h_{d_i}(d_k) - \sum_{i=1}^{k-1} \mu(d_i)\cdot f(d_i) \\
&= 0 + 0 + \cdots + \mu(1)\cdot f(d_k) - 0 = f(n).
\end{aligned}$$

□

The Möbius inversion function yields the following very useful equality

Corollary 2.0.3.

$$\phi_n(X) = \Pi_{d|n}(X^{n/d} - 1)^{\mu(d)}. \tag{1}$$

«

Proof. Let $n \in \mathbb{Z}_{\geq 1}$. Take $f, g : \mathbb{Z}_{\geq 1} \to \mathbb{C}$ defined by $f : i \mapsto \log(\phi_i)$ and $g : i \mapsto \log(X^i - 1)$. Then

$$\sum_{d|n} f(d) = \sum_{d|n} \log(\phi_d) = \log(\Pi_{d|n}\phi_d) = \log(X^n - 1) = g(n).$$

So then by the Möbius inversion function for every $m \in \mathbb{Z}_{\geq 0}$

$$\begin{aligned}
\log(\phi_m) = \sum_{d|m} \mu(d) \log(X^{m/d} - 1) \implies \\
\phi_m = \Pi_{d|m}(X^{m/d} - 1)^{\mu(d)}.
\end{aligned}$$

□

With the tools above I am ready to prove these very useful facts below for cyclotomic polynomials. The following properties will be used extensively throughout this thesis.

Proposition 2.0.4. *Let p be prime and $n \in \mathbb{Z}_{\geq 1}$*

$$\phi_{pn}(X) = \phi_n(X^p) \text{ if } p|n, \tag{i}$$
$$\phi_{pn}(X) = \phi_n(X^p)/\phi_n(X) \text{ if } p \nmid n, \tag{ii}$$
$$\phi_{2n}(X) = \phi_n(-X) \text{ if } 2 \nmid n, n > 1, \tag{iii}$$
$$\phi_n(X) = \phi_{rad(n)}(X^{n/rad(n)}), \tag{iv}$$
$$\phi_n(1/X) = X^{-\varphi(n)}\phi_n(X) \text{ if } n > 1. \tag{v}$$

«

Proof. Let p be prime and $n \in \mathbb{Z}_{\geq 1}$
(i) Suppose $p|n$. Take ϕ_{pn} with the Möbius inversion 1. Then

$$\begin{aligned}\phi_{pn}(X) &= \Pi_{d|pn}(X^{pn/d}-1)^{\mu(d)} \\ &\overset{p|n}{=} \Pi_{d|n}(X^{pn/d}-1)^{\mu(d)} \cdot \Pi_{d|\frac{n}{p}}(X^{pn/p^2d}-1)^{\mu(p^2d)} \\ &= \Pi_{d|n}(X^{pn/d}-1)^{\mu(d)} \cdot \Pi_{d|\frac{n}{p}}(X^{pn/p^2d}-1)^{0} \\ &= \phi_n(X^p).\end{aligned}$$

(ii) Suppose $p \nmid n$. Take ϕ_{pn} with the Möbius inversion 1. Then

$$\begin{aligned}\phi_{pn}(X) &= \Pi_{d|pn}(X^{pn/d}-1)^{\mu(d)} \\ &= \Pi_{d|n}(X^{pn/d}-1)^{\mu(d)} \cdot \Pi_{d|n}(X^{pn/pd}-1)^{\mu(pd)} \\ &= \Pi_{d|n}(X^{pn/d}-1)^{\mu(d)} \cdot \Pi_{d|n}(X^{n/d}-1)^{\mu(p)\mu(d)} \\ &= \phi_n(X^p) \cdot \phi_n(X)^{\mu(p)} = \frac{\phi_n(X^p)}{\phi_n(X)}.\end{aligned}$$

(iii) Suppose $2 \nmid n$ and $n > 1$. Using (ii) for $p = 2$ gives

$$\begin{aligned}\phi_{2n}(X) &\overset{(ii)}{=} \frac{\Pi_{d|n}(X^{2n/d}-1)^{\mu(d)}}{\Pi_{d|n}(X^{n/d}-1)^{\mu(d)}} = \Pi_{d|n}\Big(\frac{X^{2n/d}-1}{X^{n/d}-1}\Big)^{\mu(d)} \\ &= \Pi_{d|n}\Big(X^{n/d}+1\Big)^{\mu(d)} \\ &= \Pi_{d|n}(-1)^{\mu(d)}\big((-X)^{n/d}-1\big)^{\mu(d)} = \phi_n(-X).\end{aligned}$$

(iv) Assume that $rad(n) \neq n$, else the statement holds trivially. I note that in this case if $d|rad(n) \cdot d'$ with $d'|n$ and $d' > 1$ then $\mu(d) = 0$.

$$\begin{aligned}\phi_n(X) &= \Pi_{d|n}(X^{n/d}-1)^{\mu(d)} \\ &= \Pi_{d|rad(n)}(X^{n/d}-1)^{\mu(d)} = \phi_{rad(n)}(X^{n/rad(n)}).\end{aligned}$$

(v) Suppose $n > 1$.

$$X^{\varphi(n)}\phi_n(1/X) = X^{\varphi(n)} \prod_{\substack{i=1 \\ (i,n)=1}}^{n} (\frac{1}{X} - \xi_n^i) = \prod_{\substack{i=1 \\ (i,n)=1}}^{n} (1 - \xi_n^i X)$$
$$= \prod_{\substack{i=1 \\ (i,n)=1}}^{n} (X - \xi_n^{n-i}) \cdot \xi_n^i = \phi_n(X) \cdot \xi_n^{\sum_{(i,n)=1}^{n} i} = \phi_n(X).$$

□

The above proposition gives a lot of insight into the behavior of cyclotomic polynomials. The first three properties relate the coefficients of cyclotomic polynomials to that of polynomials of lower degree, this is very useful when studying these coefficients. The last property tells us that ϕ_n is palindromic, and this means as the name suggests that their corresponding coefficients are palindromic. Because an inverse cyclotomic polynomial is a product of cyclotomic polynomials it comes as no surprise that these polynomials exhibit similar properties.

Proposition 2.0.5. *Let p be prime and $n \in \mathbb{Z}_{\geq 1}$ then*

$$\psi_{pn}(X) = \psi_n(X^p) \text{ if } p|n, \tag{i}$$
$$\psi_{pn}(X) = \phi_n(X)\psi_n(X^p) \text{ if } p \nmid n, \tag{ii}$$
$$\psi_{2n}(X) = (1 - X^n)\psi_n(-X) \text{ if } 2 \nmid n, n > 1, \tag{iii}$$
$$\psi_n(X) = \psi_{rad(n)}(X^{n/rad(n)}), \tag{iv}$$
$$\psi_n(1/X) = -X^{-(n-\varphi(n))}\psi_n(X) \text{ if } n > 1. \tag{v}$$

«

Proof. Let p be prime and $n \in \mathbb{Z}_{\geq 1}$
(i) and (ii) follow immediately from 2.0.4.(i), (ii) and the fact that $\psi_n = \frac{X^n-1}{\phi_n(X)}$.
(iii) Suppose $n > 1$ and $2 \nmid n$. Then

$$\psi_{2n}(X) = \frac{X^{2n}-1}{\phi_{2n}(X)} \overset{2.0.4.(iii)}{=} \frac{X^{2n}-1}{\phi_n(-X)} = \frac{((-X)^n+1)((-X)^n-1)}{\phi_n(-X)}$$
$$\overset{2\nmid n}{=} (1 - X^n)\frac{((-X)^n-1)}{\phi_n(-X)} = (1 - X^n)\psi_n(-X).$$

(iv) Suppose $n > 1$ and $2 \nmid n$. Then

$$\psi_n(X) = \frac{X^n-1}{\phi_n(X)} \overset{2.0.4.(iv)}{=} \frac{X^n-1}{\phi_{rad(n)}(X^{n/rad(n)})} = \psi_{rad(n)}(X^{n/rad(n)}).$$

(vi) Suppose $n > 1$. Then

$$\psi_n(1/X) = \frac{(1/X)^n-1}{\phi_n(1/X)} \overset{2.0.4.(v)}{=} \frac{(1/X)^n-1}{X^{-\varphi(n)}\phi_n(X)} = \frac{-X^{-n}(X^n-1)}{X^{-\varphi(n)}\phi_n(X)}$$
$$= -X^{-n+\varphi(n)}\frac{(X^n-1)}{\phi_n(X)} = -X^{-(n-\varphi(n))}\psi_n(X).$$

□

similar to the non-inverse case, above tells us a lot about the behaviors of coefficients of these inverse cyclotomic polynomials. Note that inverse cyclotomic polynomials are anti palindromic (vi). With these properties we can further inspect these polynomials and their coefficients. Easy examples where the (inverse) cyclotomic polynomials are of low degree are given below.

Proposition 2.0.6. *Let p prime. Then $\phi_p(X) = 1 + X + \cdots + X^{p-1}$.* «

Proof.

$$\phi_p(X) \overset{2.0.4.(ii)}{=} \frac{\phi_1(X^p)}{\phi_1(X)} = \frac{X^p - 1}{X - 1} = (X^{p-1} + \cdots + 1).$$

Here the last equality is calculated using the polynomial division algorithm. □

Proposition 2.0.7. *$p < q$ primes. Then*

$$\psi_{pq}(X) = \frac{(X^p - 1)(X^q - 1)}{X - 1} = (X^{p+q-1} + \cdots + X^q - X^{p-1} - \cdots - X^2 - X - 1).$$

«

Proof.

$$\begin{aligned}\psi_{pq}(X) = \phi_1(X) \cdot \phi_p(X) \cdot \phi_q(X) = \frac{(X^p - 1)(X^q - 1)}{X - 1} &= X^q \cdot \frac{X^p - 1}{X - 1} - \frac{X^p - 1}{X - 1} \\ &= (X^{p+q-1} + \cdots + X^q - X^{p-1} - \cdots - X^2 - X - 1).\end{aligned}$$

Here the last equality is calculated again using the polynomial division algorithm. □

3 Coefficients of cyclotomic polynomials

Now, as previously stated in the introduction the behavior of coefficients of cyclotomic polynomials are quite surprising and erratic at first glance. In this section I will prove tools that will aid in understanding their structure. I will start by noting that by 2.0.4, in the previous section, heights of cyclotomic polynomials are completely determined by the prime factors in the corresponding degree of the polynomial.

Proposition 3.0.1. *Take $n \in \mathbb{Z}_{\geq 1}$ and let $k := p_1 \cdot \cdots \cdot p_l$ be the product of all its odd prime factors then*

$$A(\phi_n) = A(\phi_{p_1 \cdots p_l})$$

«

Proof. Let $n \in \mathbb{Z}_{\geq 1}$.Because of the unique factorization theorem n can be written as $p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$. So then

$$A(\phi_n(X) = A(\phi_{p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}}(X)) = A(\phi_{p_1 p_2 \cdots p_k}(X^{p_1^{n_1-1} p_2^{n_2-1}})) = A(\phi_{p_1 p_2 \cdots p_k}(X))$$

In the second equation I repeatedly applied 2.0.4.1.i. Now suppose one of the prime factor is even $p_i = 2$, then because of 2.0.4.1.iii.

$$A(\phi_{p_1 p_2 \cdots p_k}(X)) = A((-1)^{\varphi(n)} \phi_{\frac{p_1 p_2 \cdots p_k}{p_i}}(-X)) = A(\phi_{\frac{p_1 p_2 \cdots p_k}{p_i}}(X))$$

and with this the proof is complete. □

Above proposition says that when searching for heights of cyclotomic polynomials it is sufficient to look at the prime factors of the degree. So since the case where a cyclotomic polynomial is unary is trivial, I will start at the case where the polynomial is binary. Recall that binary ϕ_n means that $n = p_1 \cdot p_2$ with p_1, p_2 odd primes.

3.1 Binary cyclotomic polynomials

Theorem 3.1.1. *(Lam and Leung, 1996) [16] Suppose $\phi_{pq}(X) = \sum_{i=0}^{\varphi}(pq)a_i X^i$. Take $p < q$ prime numbers. Let r, s be the unique positive integers such that $(p-1)(q-1) = pr + qs$. Then*

$$a_n = \begin{cases} +1 & \iff n = ip + jq \text{ with } i \in [0, r], j \in [0, s] \\ -1 & \iff n = ip + jq - pq \text{ with } i \in [r+1, q-1], j \in [s+1, p-1] \\ 0 & \text{otherwise} \end{cases}$$

«

The theorem above and its proof are well known. The proof makes use of the group structure generated by the n-th root of unity. Although H. Lenstra much earlier in 1979, in his paper [18] achieved similar results, the theorem above in specific was proven by Lam and Leung. Here I want to give an alternative proof. Before I am able to give the proof I have to adjust the theorem as follows.

Theorem 3.1.2. *Suppose $\phi_{pq}(X) = \sum_i a_i X^i$. Take $p < q$ prime numbers. Let $\bar{p} > 0$ be the unique inverse of p modulo q and $\bar{q}$ the inverse of q modulo p, they exist because $(q,p) = 1$. Then*
(1) Every $0 \leq n \leq pq$ is of the form $ip + jq - \delta pq$ with $\delta \in \{0,1\}$ and $0 \leq i < q, 0 \leq j < p$ the unique integers such that $ip \equiv n \mod q$ and $jq \equiv n \mod p$.
(2) And

$$a_n = \begin{cases} +1 & \iff n = ip + jq \text{ with } i \in [0, \bar{p}), j \in [0, \bar{q}) \\ -1 & \iff n = ip + jq - pq \text{ with } i \in [\bar{p}, q-1], j \in [\bar{q}, p-1] \\ 0 & \text{otherwise} \end{cases}.$$

«

It is clear that this theorem is equivalent to the one Lam and Leung gave. With this I am able to start the proof.

Proof. I will start with the proof of (1). Let $0 \leq X < pq$. Let $0 \leq i < p$, $0 \leq j < q$ be the unique integers such that $i \equiv X\bar{p} \mod q$ and $j \equiv X\bar{q} \mod p$. Then the Chinese Remainder Theorem says that there exists a unique $0 \leq X' < pq$ such that $X' \equiv ip \mod q$ and $X' \equiv jq \mod p$. So thus $X' \equiv X \equiv ip + jq \mod qp$ and $X' = X = ip + jp - k \cdot pq$ with k some integer. And $0 \leq k \leq 1$ as $0 \leq jp + qp \leq 2qp$.

The remainder of the proof will cover (2). Let n be given. I will try to find a_n the n-th coefficient of $\phi_{pq}(X)$. Because of the properties 2.0.4, the following holds

$$\phi_{pq}(X) = \frac{\phi_p(X^q)}{\phi_p(X)} = \frac{(1-X)\phi_p(X^q)}{1-X^p}$$

Now assume $|X| < 1$. Then take the series expansion $1/(1-X^{pq}) = (1 + X^p + X^{2q} + \dots)$, so

$$\phi_{pq}(X) = (1-X)\phi_p(X^q)(1 + X^p + X^{2p} + \dots) = \Big(\sum_{j=0}^{p-1} X^{jq} - \sum_{k=0}^{p-1} X^{kq+1}\Big)(1 + X^p + X^{2p} + \dots)$$

Take some terms $X^{jq}(1 + X^p + \dots)$ in the above product. This term has exactly one monomial of degree n if and only if $jq \equiv n \mod p$ and $jq \leq n$ and this monomial has coefficient 1. Similarly the term $-X^{kq+1}(1 + X^p + \dots)$ has exactly one monomial of degree n if and only if $kq + 1 \equiv n \mod p$ and $kq + 1 \leq n$ and this monomial has coefficient -1. So thus

$$a_n = \sum_{\substack{i,j \\ jq \equiv n \mod p}} g(X^{jq+ip}) + \sum_{\substack{i,k \\ kq+1 \equiv n \mod p}} g(-X^{kq+1+ip}), \quad \text{where} \quad g(d_m X^m) = \begin{cases} d_m & \text{if } m \leq n \\ 0 & \text{otherwise} \end{cases}.$$

Now note that the term $a_n X^n$ in $\phi_{pq}(X)$ has exactly one of the following form

$$a_n X^n = X^{jq+ip}, \quad a_n X^n = -X^{kq+ip+1} \quad \text{or} \quad a_n X^n = X^{jq+ip} - X^{kq+i_1 p+1} = 0$$

for some $0 \leq j, k < p$ and $i, i_1 \geq 0$. Because the $j, k < p$ in the exponents such that $jq \equiv n \mod p$ with $jq \leq n$ and $kq + 1 \equiv n \mod p$ with $kq + 1 \leq n$ if they exist, are unique.

Take again a look at the term $a_n X^n$ in $\phi_{pq}(X)$.

$$\begin{aligned}
a_n = 1 &\iff a_n X^n = X^{jq+ip} && && \text{for some } 0 \le j < q, \quad 0 \le i \\
&\iff n = jq + ip && \text{and} && n \neq kq + lp + 1, \text{ for some } 0 \le j,k < q, 0 \le i,l \\
&\iff n \equiv jq \mod p && \text{and} && n \not\equiv kq + 1 \mod p \text{ for some } 0 \le k < q \\
&\quad\ n \equiv ip \mod q && \text{and} && n \not\equiv lp + 1 \mod q \text{ for some } l \ge 0 \\
&\iff n = jq + ip && \text{with} && 0 \le i < \bar{p}, 0 \le j < \bar{q}.
\end{aligned}$$

Where in the third and fourth "if and only if" statement I used the fact that $\bar{p}p \equiv 1 \mod q$, $\bar{q}q \equiv 1 \mod p$ and I also used the Chinese Remainder Theorem to create the congruences.

$$\begin{aligned}
a_n = -1 &\iff a_n X^n = -X^{kq+ip+1} && && \text{for some } 0 \le k < q, \quad 0 \le i \\
&\iff n = kq + ip + 1 && \text{and} && n \neq jq + lp, \text{ for some } 0 \le j < q, \quad 0 \le i \\
&\iff n \equiv kq + 1 \mod p && \text{and} && n \not\equiv jq \mod p \text{ for some } 0 \le j < q \\
&\quad\ n \equiv ip + 1 \mod q && \text{and} && n \not\equiv lp \mod q \text{ for some } l \ge 0 \\
&\iff n = kq + ip + p\bar{p} + \bar{q}q - pq && \text{with} && 0 \le i < q - \bar{p}, 0 \le k < p - \bar{q}. \\
&\iff n = (k + \bar{q})q + (i + \bar{p})p - pq && \text{with} && 0 \le i < q - \bar{p}, 0 \le k < p - \bar{q}.
\end{aligned}$$

Where in the third and fourth "if and only if" statement I used the fact that $\bar{p}p \equiv 1 \mod q$, $\bar{q}q \equiv 1 \mod p$ and I also used the Chinese Remainder Theorem to create the congruences. Furthermore I used the identity $pq + 1 = p\bar{p} + q\bar{q}$ in the last two statements. The case that $a_n = 0$ is then clear as well, and the proof is done. □

Even though I used the bound $|X| < 1$ to find values for the coefficients it should be noted that the result holds for all X as coefficients of polynomials are the same for all X. The proof was inspired by Kaplan's Lemma and its proof 3.2.2. Here I do want to mention that H. Lenstra much earlier in 1979 had a similar idea to take the series expansion of $1/(X^q - 1)$ in his paper in [18] to conclude properties of binary cyclotomic polynomials.

The theorem says a lot about the structure of binary cyclotomic polynomials. An interesting property that Lam and Leung noticed while giving the above theorem was that the non zero coefficients of binary cyclotomic polynomials alternate between $+1$ and -1. H. Lenstra noted this again much earlier as well. One can see that these coefficients indeed alternate by examining the $1 - X$ factor in $\phi_{pq}(X) = (1 - X)\phi_p(X^q)(1 + X^p + X^{2p} + \dots)$ in the proof above. So

Corollary 3.1.3. *The non zero coefficients of binary cyclotomic polynomials alternate between $+1$ and -1.* «

In his paper [22], Moree gave a nice visualization of the theorem above in calculating coefficients of binary cyclotomic polynomials. He called this the LLL diagram and named it after Lenstra, Lam and Leung. I end this section with an example of this visualization.

Example 3.1.4. Let $p = 3$ and $q = 7$. Take a look at $\phi_{3\cdot7}(X) = \sum_{i=0}^{\varphi(3\cdot7)} a_i X^i$. This polynomial has coefficients that are either $-1, 0$ or 1 by above theorem. One can find out exactly what value each coefficient of this polynomial is, in the following way:

Create a $p \times q$ matrix. Start at the bottom left with zero and add $p = 3$ and reduce modulo pq every time you move right, add $q = 7$ and reduce modulo pq everytime you move up. Calculate $\bar{p} = 5$ and $\bar{q} = 1$. The bottom left $\bar{p} \times \bar{q}$ sub-matrix will give the coefficient indices with positive value and the top right sub-matrix $(q - \bar{p}) \times (p - \bar{q})$ will give the coefficient indices with negative value.

14	17	20	2	5	8	11
7	10	13	16	19	1	4
0	3	6	9	12	15	18

A verification shows that for the indices in the bottom left corner $a_0 = a_3 = a_6 = a_9 = a_{12} = 1$ indeed holds. Notice also that for the indices in the upper right corner $a_1 = a_4 = a_8 = a_{11} = -1$ holds as well. Verify with $\phi_{3.7}(X) = X^{12} - X^{11} + X^9 - X^8 + X^6 - X^4 + X^3 - X + 1$. «

3.2 Ternary cyclotomic polynomials

In the last section I discussed the binary cyclotomic polynomials. In this subsection I want to look at the ternary cyclotomic polynomials. The ternary cyclotomic polynomials exhibit many interesting properties that have been researched [2] [9]. A particular interest in the height of these polynomials was shown, as the first possible non-flat cyclotomic polynomial is ternary. It became clear that cyclotomic polynomials are not always flat and that they have a more complex structure than previously thought. One such early research was done by Emma Lehmer (1936) [17] who in her paper showed that coefficients of ternary cyclotomic polynomials are unbounded. Conversely, for fixed primes these coefficients are in fact known to be bounded, Bang (1895) [5]. Recently there has been an interest in finding an optimal bound.

The following (corrected) conjecture was first proposed by Sister Marion Beiter (1968) [7] and later corrected by mainly Moree and Gallot (2008) [10]. Moree and Gallot showed in this article that one can get arbitrarily close to this corrected bound, and thus if it exists it is optimal.

Conjecture 3.2.1. *(Corrected Beiter Cojecture, 2008, [10]) For odd primes $p < q < r$,*

$$A(pqr) \leq \frac{2}{3}p.$$

«

There is a proof of this conjecture that is currently in pre-print and it will not be further discussed here. Instead I will refer to [13].

A lot of recent discoveries in (ternary) cyclotomic polynomials stem from a paper released by Nathan Kaplan in 2007 [14]. In his paper he gave a formula where he reduces the calculations of ternary coefficients to calculations of coefficients in binary cyclotomic polynomials.

Lemma 3.2.2. *(Kaplan's Lemma [14], 2007, p120) Suppose $\phi_{pqr}(X) = \sum_{i=0}^{\varphi(pqr)} c_i X^i$, $\phi_{pq}(X) = \sum_{i=0}^{\varphi(pq)} a_i X^i$. Given n let $a'_i = a_i$ if $ri \leq n$, and 0 otherwise. Further let $f(m)$ be the unique value $0 \leq f(m) < pq$ such that*

$$f(m) \equiv r^{-1}(n - m) \mod pq$$

Note that r^{-1} exists because it is coprime to pq. Then

$$c_n = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{q+p-1} a'_{f(m)}$$

«

The proof of the lemma is given by Kaplan which I rewrote and adjusted slightly here.

Proof. Let n be given. I will try to find c_n the n-th coefficient of ϕ_{pqr}. Because of the properties 2.0.4, the following holds

$$\phi_{pqr}(X) = \frac{\phi_{pq}(X^r)}{\phi_{pq}(X)} = \frac{X^{pq}-1}{\phi_{pq}(X)} \cdot \frac{\phi_{pq}(X^r)}{X^{pq}-1} = -\frac{\psi_{pq}(X)\phi_{pq}(X^r)}{1-X^{pq}}$$

Now assume $|X| < 1$. Let $-\psi_{pq}(X)\phi_{pq}(X^r) = \sum_{m=0}^{k} d_m X^m$ with k the degree of the polynomial. Then take the series expansion $1/(1-X^{pq}) = (1 + X^{pq} + X^{2pq} + \dots)$, this gives

$$\phi_{pqr}(X) = -\psi_{pq}(X)\phi_{pq}(X^r) \cdot (1 + X^{pq} + \dots) = \sum_{m=0}^{k} d_m X^m \cdot (1 + X^{pq} + \dots).$$

Take some term $d_m X^m (1 + X^{pq} + \dots)$ in the above product. This term has exactly one monomial of degree n if and only if $m \equiv n \mod pq$ and $m \leq n$, this monomial has coefficient d_m. So thus

$$c_n = \sum_{\substack{m \\ m \equiv n \mod pq}} g(d_m X^m), \quad \text{where} \quad g(d_m X^m) = \begin{cases} d_m & \text{if } m \leq n \\ 0 & \text{otherwise} \end{cases}.$$

The remaining task then is to find all terms in the product $-\psi_{pq}(X)\phi_{pq}(X^r)$ containing a monomial with degree smaller or equal to n and congruent to $n \mod pq$. First note that because of 2.0.7

$$-\psi_{pq}(X)\phi_{pq}(X^r) = -\sum_{m=0}^{q+p-1} \chi(m) X^m \cdot \phi_{pq}(X^r),$$

where $\chi(m) = -1$ if $m \in [0, p-1]$, 1 if $m \in [q, q+p-1]$ and 0 otherwise. So an arbitrary term in this product is of the form $\chi(m) a_v X^{rv+m}$ for some integers $0 \leq m \leq q+p-1$ and $0 \leq v \leq \varphi(pq)$. Suppose the degree of this term is congruent to n modulo pq. Then $v \equiv r^{-1}(n-m) \equiv f(m) \mod pq$ and so $v = f(m)$ as $f(m) < pq$ was unique. So

$$\begin{aligned} c_n &= \sum_{m=0}^{q+p-1} g(\chi(m) a_{f(m)} X^{rf(m)+m}) \quad \text{where} \quad g(d_m X^m) = \begin{cases} d_m & \text{if } m \leq n \\ 0 & \text{otherwise} \end{cases} \\ &= \sum_{m=0}^{q+p-1} \chi(m) a'_{f(m)}. \end{aligned}$$

In the last equality I used the fact that $rf(m) + m \leq n$ if and only if $rf(m) \leq n$ because $m < pq$ and $rf(m) + m \equiv n \mod pq$. □

As before in the proof for Lam and Leung, Kaplan has assumed $|X| < 1$ for the series expansion to calculate the value of coefficients. As the coeffecients of the polynomial are the same for all X, it is sufficient to look at $|X| < 1$. The tools used in the proof as well as the lemma itself are very useful. Rosu and Moree gave a nice reformulation of theorem 3.1.1 applied to Kaplan's Lemma which I slightly adjusted to fit my theorem notations.

Lemma 3.2.3. *(Rosu & Moree, 2012, Lemma 3 [23])*
let $0 \leq m < pq$ then $m = ap + bq$ or $m = ap + bq - pq$ with $a \in [0, q-1]$ and $b \in [0, q-1]$ the unique values such that $ap \equiv m \mod p$ and $bq \equiv m \mod q$. Write $[m]_p := a$ and $[m]_q := b$ let a_i be a binary coefficient. Then

$$a_i = \begin{cases} 1 & \text{if } [i]_p < \bar{p}, [i]_q < \bar{q} \quad \text{and} \quad [i]_p p + [i]_q q \leq n/r, \\ -1 & \text{if } f[i]_p \geq \bar{p}, [i]_q \geq \bar{q} \quad \text{and} \quad [i]_p p + [i]_q q - pq \leq n/r, . \\ otherwise & \end{cases}$$

Recall that n is n-th coefficient in ϕ_{pqr}. «

In his paper Kaplan used the lemma to prove the following;

Theorem 3.2.4. *(Kaplan [14], 2007, p120) Let $p < q < r$ be odd primes. Let $r \equiv \pm 1 \mod pq$ be prime. Then ϕ_{pqr} is flat.* «

The proof of this theorem reduces the calculations of ternary polynomials to calculations of binary cyclotomic polynomials by Kaplan's lemma. Then one uses 3.1.3 among other steps to conclude that the value of the coefficients are less than one in magnitude. I will not further go into detail about this proof here in this thesis. Instead I will refer to his paper [14].

3.3 Quaternary cyclotomic polynomials

There is less known about the behavior of quaternary cyclotomic polynomials compared to the ternary case. Even though there are bounds known for the quartenary cyclotomic polynomials, Bzdega (2010) [8], it is unknown whether the bounds are optimal. Unlike the ternary case where the corrected sister Beiter conjecture if true is optimal. Furthermore there are no convenient formulas one can use like Kaplan's Lemma for the ternary case. In this section I want to present some formulas that describe the quartenary cyclotomic polynomial. I also want to give a bound assuming the Corrected Sister Beiter conjecture. First I will note a few basic properties.

$$\phi_{pqrs}(X) = \frac{\phi_{pqr}(X^s)}{\phi_{pqr}(X)} = \frac{X^{pqrs}-1}{\phi_{pqr}(X)} \cdot \frac{\phi_{pqr}(X^s)}{X^{pqrs}-1} = \frac{\psi_{pqr}(X)\phi_{pqr}(X^s)}{X^{pqr}-1} \tag{4}$$

Proposition 3.3.1. *$\psi_{pqr}(X)\phi_{pqr}(X^s)$ is anti palindromic.* «

Proof. I compute:

$$\begin{aligned} \psi_{pqr}(1/X)\phi_{pqr}((1/X)^s) &= \psi_{pqr}(1/X)\phi_{pqr}(1/(X^s)) = X^{-\varphi(pqr)} \cdot \psi_{pqr}(1/X)\phi_{pqr}(X^s) \\ &= -X^{-\varphi(pqr)-(pqr-\varphi(pqr))} \cdot \psi_{pqr}(X)\phi_{pqr}(X^s) \\ &= -X^{-pqr} \cdot \psi_{pqr}(X)\phi_{pqr}(X^s) \end{aligned}$$

where the second equality follows from 2.0.4.(v) and the third equality from 2.0.5.(v). So this means that $-f^* = f$ and thus anti palindromic. □

Proposition 3.3.2. *For every $s > \deg \psi_{pqr}$ the following holds*

$$A(\psi_{pqr}(X)\phi_{pqr}(X^s)) = A(\psi_{pqr}(X)) \cdot A(\phi_{pqr}(X^s))$$

«

Proof. Take $\phi_{pqr}(X) = \sum_{i=0}^{\varphi(pqr)} c_j X^j$ and $\psi_{pqr}(X) = \sum_{i=0}^{\varphi(pqr)} \bar{c}_i X^i$. Suppose $A(\psi_{pqr}(X)) = |\bar{c}_k|$ then $-|\bar{c}_k|$ is also a coefficient in $\psi_{pqr}(X)$ as ψ is anti palindromic. The elements of $\psi_{pqr}(X)\phi_{pqr}(X^s)$ are $\bar{c}_i c_j X^{js+i}$. Because $s > \deg \psi_{pqr}$ all the $js + i$ are distinct. This then gives the equality. □

A first possible step in creating a formula that would describe the quaternery coefficients might invlove using the Möbius inversion formula. Recall

$$\phi_n(X) = \Pi_{d|n}(X^{n/d} - 1)^{\mu(d)}, \quad \mu(n) = \begin{cases} 0 & \text{if there exists a } p \text{ such that } p^2|n \\ (-1)^t & n \text{ is the product of } t \text{ distinct primes.} \end{cases}$$

Proposition 3.3.3. *(Gallot, Moree & Hommersom, p. 4, (8)) [11]*

$$\phi_n(X) = \Pi_{d|n}\Big(1 - \mu(d)X^{n/d} + \frac{1}{2}(1 - \mu(d))\mu(d)(\sum_{k=0}^{\infty} X^k n/d)\Big).$$

«

Proof. Suppose once again $|X| < 1$ notice then

$$\begin{aligned} \mu(d) = 0 &\implies (X^{n/d} - 1)^{\mu(d)} = 1 \\ \mu(d) = 1 &\implies (X^{n/d} - 1)^{\mu(d)} = (X^{n/d} - 1) \\ \mu(d) = -1 &\implies (X^{n/d} - 1)^{\mu(d)} = 1/(X^{n/d} - 1) = (1 + X^{n/d} + X^{2n/d} + \dots). \end{aligned}$$

So then

$$\begin{aligned} (X^{n/d} - 1)^{\mu(d)} &= (1 - \mu(d))(1 + \mu(d)) + \frac{1}{2}\mu(d)(1 + \mu(d))(X^{n/d} - 1) \\ &\quad + \frac{1}{2}(1 - \mu(d))\mu(d)(1 + X^{n/d} + X^{2n/d} + \dots) \\ &= 1 - \mu(d)X^{n/d} + \frac{1}{2}(1 - \mu(d))\mu(d)(X^{2n/d} + \dots). \end{aligned}$$

So then substituting this in the M obius inversion formula of ϕ_n will complete the proof. □

Now with this proposition it is possible to compute some coefficients, note that $a_n(j) = \frac{1}{j!}\phi^{(n)}(0)$ where $a_n(j)$ is the j-th coefficient of ϕ_n. With this we can compute some examples:

Example 3.3.4. Let $f(X) = \Pi_{d|n,d<n}\Big(1-\mu(d)X^{n/d}+\frac{1}{2}(1-\mu(d))\mu(d)(X^{2n/d}+\dots)\Big)$. Note further that $f(0)=1, f'(0)=0$.

$$\begin{aligned}
\phi_n(X) &= g\cdot f = \Big(1-\mu(n)X+\frac{1}{2}(1-\mu(n))\mu(n)(X^2+\dots)\Big)\cdot f,\\
\phi_n(0) &= \Big(1-\mu(n)\cdot 0+\frac{1}{2}(1-\mu(d))\mu(d)(0^2+\dots)\Big)\cdot f(0)=1,\\
\phi_n'(X) &= \Big(-\mu(n)+\frac{1}{2}(1-\mu(d))\mu(d)(2X+\dots)\Big)\cdot f+g\cdot f',\\
\phi_n'(0) &= \mu\cdot f(0)+g(0)\cdot f'(0)=\mu(n),\\
a_n(0) &= \phi_n(0)=1,\\
a_n(1) &= \phi_n'(0)=-\mu(n).
\end{aligned}$$

«

The above example and proposition can be taken further to create a formula for the j-th coefficient of an arbitrary cyclotomic polynomial. The formula that is created by doing this was first introduced by Möller (1970) [19] and then his formula had been generalized and the proof simplified by Gallot and Moree in 2008 [11]. I will not write out the formula instead I will use the technique that is used here and in Kaplan's lemma to create another formula. The proof is similar to the proof in Kaplan's Lemma.

Theorem 3.3.5. *Suppose $\phi_{pqrs}(X)=\sum_i d_iX^i$, $\phi_{pqr}(X)=\sum_i c_iX^i$, $\psi_{pqr}(X)=\sum_i \bar{c}_iX^i$. Given n let $c_i'=c_i$ if $si\le n$, and 0 otherwise. Further let $f(m)$ be the unique value $0\le f(m)<pqr$ such that*

$$f(m)\equiv s^{-1}(n-m) \mod pqr$$

Note that s^{-1} exists because it is co-prime to pqr. Then

$$d_n=\sum_{m=0}^{pqr-\varphi(pqr)}\bar{c}_m\cdot c'_{f(m)}$$

«

Proof. Let n be given. I will try to find d_n the n-th coefficient of ϕ_{pqrs}. Because of the properties 2.0.4, the following holds

$$\phi_{pqrs}(X)=\frac{\phi_{pqr}(X^s)}{\phi_{pqr}(X)}=\frac{X^{pqr}-1}{\phi_{pqr}(X)}\cdot\frac{\phi_{pqr}(X^s)}{X^{pqr}-1}=-\frac{\psi_{pqr}(X)\phi_{pqr}(X^s)}{1-X^{pqr}}.$$

Similarly to the ternary case in Kaplan's Lemma assume $|X|<1$. Let $-\psi_{pqr}(X)\phi_{pqr}(X^s)=\sum_{v=0}^k z_vX^v$ with k the degree of the polynomial. Then take the series expansion $1/(1-X^{pqr})=(1+X^{pqr}+X^{2pqr}+\dots)$, this gives

$$\phi_{pqrs}(X)=-\psi_{pqr}(X)\phi_{pqr}(X^s)\cdot(1+X^{pqr}+\dots)=\sum_{v=0}^k d_vX^v\cdot(1+X^{pqr}+\dots).$$

Take some term $d_vX^v(1+X^{pqr}+\dots)$ in the above product. This term has exactly one monomial

of degree n if and only if $v \equiv n \mod pq$ and $v \leq n$, this monomial has coefficient d_v. So thus

$$d_n = \sum_{\substack{v \\ v \equiv n \mod pqr}} g(d_v X^v), \quad \text{where} \quad g(d_v X^v) = \begin{cases} d_v & \text{if } v \leq n \\ 0 & \text{otherwise} \end{cases}.$$

The remaining task then is to find all terms in the product $-\psi_{pqr}(X)\phi_{pqr}(X^s)$ containing a monomial with degree smaller or equal to n and congruent to $n \mod pqr$. An arbitrary term in this product is of the form $-\bar{c}_m X^m \cdot c_v X^{sv}$ for some integers $0 \leq m \leq \deg \psi_{pqr}(X)$ and $0 \leq v \leq \varphi(pqr)$. Suppose the degree of this term is congruent to n modulo pqr. Then $v \equiv s^{-1}(n-m) \equiv f(m) \mod pqr$ and so $v = f(m)$ as $f(m) < pqr$ was unique. So

$$\begin{aligned} d_n &= \sum_{m=0}^{pqr-\varphi(pqr)} g(-\bar{c}_m X^m \cdot c_{f(m)} X^{sf(m)}) \quad \text{where} \quad g(d_v X^v) = \begin{cases} d_v & \text{if } v \leq n \\ 0 & \text{otherwise} \end{cases} \\ &= \sum_{m=0}^{pqr-\varphi(pqr)} -\bar{c}_m X^m \cdot c'_{f(m)} X^{sf(m)} \end{aligned}$$

In the last equality I used the fact that $sf(m) + m \leq n$ if and only if $sf(m) \leq n$ because $m < pqr$ and $sf(m) + m \equiv n \mod pqr$. □

The above theorem is useful in the sense that it reduces calculation of the coefficients of a quartenary cyclotomic polynomial in to calculations of the (inverse) ternary cyclotomic polynomial. Below is an example of one such calculation.

Example 3.3.6. Take $s \equiv 1 \mod pqr$ prime and let $g(m)$ be the unique value $0 \leq g(m) \leq pqr$ such that $g(m) \equiv m \mod pqr$. If $n \leq pqr - \varphi(pqr)$ then note that the only indices m such that $sf(m) \leq n$ and $f(m) \leq pqr - \varphi(pqr)$ are the indices with $f(m) = 0$ (else $\bar{c}_m c'_{f(m)} = 0$). And this only happens when $m = n$. This shows that the values in the first row of the table below are correct.

Next note that for $pqr - \varphi(pqr) < n < pqr$ the only indices m such that $sf(m) \leq n$ and $f(m) \leq pqr - \varphi(pqr)$ are again the indices such that $f(m) = 0$ (else $\bar{c}_m c'_{f(m)} = 0$). No indices such that $\bar{c}_m c'_{f(m)} \neq 0$ exist as $m \leq pqr - \varphi(pqr)$. This shows the second row. And the third row is similar to above.

Suppose finally $s \leq n < 2s$. Then $sf(m) \leq n$ if $f(m) \leq 1$. If $g(n) \leq pqr - \varphi(pqr) + 1$ then $d_n = -\bar{c}_{g(n)} c_0 - \bar{c}_{g(n)+1} c_1$. If $g(n) > pqr - \varphi(pqr) + 1$ then similar to before no $m \leq pqr - \varphi(pqr)$ exists such that $\bar{c}_m c'_{f(m)} \neq 0$ and so $d_n = 0$ and this explains the final row. Note that if $s \not\equiv 1 \mod pqr$ then the $d_n = 0$ conclusions are false in general. «

$n \leq pqr - \varphi(pqr)$	$d_n = -\bar{c}_n c_0$
$pqr - \varphi(pqr) < n < pqr$	$d_n = 0$
$pqr \leq n < s$	$g(n) \leq pqr - \varphi(pqr) \iff d_n = -\bar{c}_{g(n)} c_0$ $pqr - \varphi(pqr) \leq g(n) \leq pqr \iff d_n = 0$
$n \geq s$	$g(n) \leq pqr - \varphi(pqr) + \lfloor \frac{n}{s} \rfloor \iff d_n = \sum_{m=0}^{\lfloor \frac{n}{s} \rfloor} -\bar{c}_{g(n)+m} c_m$ $pqr - \varphi(pqr) + \lfloor \frac{n}{s} \rfloor < g(n) < pqr \iff d_n = 0$

The coefficients $\bar{c}_n$ of the inverse ternary are quite clunky and it might be better if there were no terms of this kind in a formula. Below are two other formulas that each reduce this further. The first reduces the quaternary coefficient to sums of ternary coefficient and the second to sums of binary coefficients.

Theorem 3.3.7. *Suppose $\phi_{pqrs} = \sum_i d_i X^i$, $\phi_{pqr} = \sum_i c_i X^i$. Given n let $c'_i = c_i$ if $si \leq n$, and 0 otherwise. Further let $f(k,l,m), g(k,l,m)$ be the unique values with $0 \leq f(k,l,m) < pqr$ and $0 \leq g(k,l,m) < pqr$ such that*

$$f(k,l,m) \equiv s^{-1}(n - kp - lq - mr) \mod pqr$$
$$g(k,l,m) \equiv s^{-1}(n - kp - lq - mr - 1) \mod pqr$$

Note that s^{-1} exists because it is coprime to pqr. Then

$$d_n = \sum_{k,l,m} c'_{f(k,l,m)} - \sum_{k,l,m} c'_{g(k,l,m)}$$

with $0 \leq k < r, 0 \leq l < p, 0 \leq m < q$. «

Proof. Let n be given. I will try to find d_n the n-th coefficient of ϕ_{pqrs}. Because of the properties 2.0.4, the following holds

$$\begin{aligned}\phi_{pqrs}(X) &= \frac{\phi_{pqr}(X^s)}{\phi_{pqr}(X)} = \frac{X^{pqr}-1}{\phi_{pqr}(X)} \cdot \frac{\phi_{pqr}(X^s)}{X^{pqr}-1} = -\frac{\psi_{pqr}(X)\phi_{pqr}(X^s)}{1-X^{pqr}} \\ &= -\frac{\phi_1(X)\phi_p(X)\phi_q(X)\phi_r(X)\phi_{pq}(X)\phi_{pr}(X)\phi_{qr}(X)\phi_{pqr}(X^s)}{1-X^{pqr}} \\ &= \frac{(1-X)\phi_p(X^q)\phi_q(X^r)\phi_r(X^p)\phi_{pqr}(X^s)}{1-X^{pqr}}.\end{aligned}$$

Similarly to the ternary case in Kaplan's Lemma assume $|X| < 1$. Let $(1-X)\phi_p(X^q)\phi_q(X^r)\phi_r(X^p) = \sum_{v=0}^{k} z_v X^v$ with k the degree of the polynomial. Then take the series expansion $1/(1-X^{pqr}) = (1 + X^{pqr} + X^{2pqr} + \dots)$, this gives

$$\phi_{pqrs}(X) = (1-X)\phi_p(X^q)\phi_q(X^r)\phi_r(X^p) \cdot (1 + X^{pqr} + \dots) = \sum_{v=0}^{k} z_v X^v \cdot (1 + X^{pqr} + \dots).$$

Take some term $z_v X^v (1 + X^{pqr} + \dots)$ in the above product. This term has exactly one monomial of degree n if and only if $v \equiv n \mod pqr$ and $v \leq n$, this monomial has coefficient z_v. So thus

$$d_n = \sum_{v \equiv n \mod pqr} g(z_v X^v), \quad \text{where} \quad g(z_v X^v) = \begin{cases} z_v & \text{if } v \leq n \\ 0 & \text{otherwise} \end{cases}.$$

The remaining task then is to find all terms in the product $(1-X)\phi_p(X^q)\phi_q(X^r)\phi_r(X^p)$ containing a monomial with degree smaller or equal to n and congruent to $n \mod pqr$. An arbitrary term in this product is either of the form $X^{kp} \cdot X^{lq} \cdot X^{rm} \cdot c_{v_1} X^{sv_1}$ or $-X \cdot X^{kp} \cdot X^{lq} \cdot X^{rm} \cdot c_{v_2} X^{sv_2}$ for some integers with $0 \leq k < r, 0 \leq l < p, 0 \leq m < q$ and $0 \leq v_1, v_2 \leq \varphi(pqr)$. Suppose the degree of the first term is congruent to n modulo pqr. Then $v_1 \equiv s^{-1}(n - kp - lq - rm) \equiv f(k,l,m) \mod pqr$ and so $v = f(m)$ as $f(m) < pqr$ was unique. Similarly for the second term, suppose the degree of the term is congruent to n modulo pqr. Then $v_2 = g(k,l,m)$. Thus

$$
\begin{aligned}
d_n &= \sum_{k,l,m} g(X^{kp}\cdot X^{lq}\cdot X^{rm}\cdot c_{f(k,l,m)}X^{sf(k,l,m)}) \\
&+ \sum_{k,l,m} g(-X\cdot X^{kp}\cdot X^{lq}\cdot X^{rm}\cdot c_{f(k,l,m)}X^{sf(k,l,m)}) \quad \text{where} \quad g(d_vX^v)=\begin{cases} d_v & \text{if } v\le n \\ 0 & \text{otherwise}\end{cases} \\
&= \sum_{k,l,m} c'_{f(k,l,m)} - \sum_{k,l,m} c'_{g(k,l,m)}
\end{aligned}
$$

In the last equality I used the fact that $f(k,l,m)s+kp+lq+rm \le n$ if and only if $f(k,l,m)s \le n$ because $kp+lq+rm \le (r-1)p+(p-1)q+(q-1)r < pqr$ and similarly $g(k,l,m)s+kp+lq+rm+1 \le n \iff g(k,l,m)s \le n$ because $n \equiv f(k,l,m)s+kp+lq+rm \equiv g$ and $n \equiv (k,l,m)s+kp+lq+rm+1 \mod pqr$. □

Formula 3.3.7 has reduced quaternary coefficients to sums of ternary coefficients. So I can turn to Kaplan's lemma once again and reduce it even further.

Theorem 3.3.8. *Suppose $\phi_{pqrs}=\sum_i d_iX^i$, $\phi_{pqr}=\sum_i c_iX^i$, $\phi_{pq}=\sum_i a_iX^i$. Given $n\in\mathbb{Z}_{\ge 0}$. Let $f(k,l,m), g(k,l,m), \bar{f}(n,m)$ be the unique values with $0\le f(k,l,m)<pqr$, $0\le g(k,l,m)<pqr$ and $0\le \bar{f}(n,m)<pq$ such that*

$$
\begin{aligned}
f(k,l,m) &\equiv s^{-1}(n-kp-lq-mr) \mod pqr \\
g(k,l,m) &\equiv s^{-1}(n-kp-lq-mr-1) \mod pqr \\
\bar{f}(j,z) &\equiv r^{-1}(j-z) \mod pq
\end{aligned}
$$

Write $f:=f(k,l,m)$ and $g:=g(k,l,m)$. Further let $\mathbb{1}_f=1$ if $sf\le n$, and 0 otherwise. Also let $h(a_i,f)=a_i$ if $ri\le f$, and 0 otherwise. Note that s^{-1} exists because it is co-prime to pqr and r^{-1} exists because it is coprime to pq. Then

$$
d_n=\sum_{k,l,m}\mathbb{1}_f\Big(\sum_z h(f,a_{\bar{f}(f,z)})-h(f,a_{\bar{f}(f,z+q)})\Big)-\mathbb{1}_g\Big(\sum_z h(g,a_{\bar{f}(g,z)})-h(g,a_{\bar{f}(g,z+q)})\Big)
$$

with $0\le k<r, 0\le l<p, 0\le m<q$, and $0\le z<p$. «

Proof. This theorem follows directly from above theorems. Let $\bar{f}(j,z)\equiv r^{-1}(j-z)$ and h as described above.

$$
\begin{aligned}
d_n &\overset{3.3.7}{=} \sum_{k,l,m}\mathbb{1}_f c_{f(k,l,m)} - \sum_{k,l,m}\mathbb{1}_f c_{g(k,l,m)} \\
&\overset{3.2.2}{=} d_n=\sum_{k,l,m}\mathbb{1}_f\Big(\sum_z h(f,a_{\bar{f}(f,z)})-h(f,a_{\bar{f}(f,z+q)})\Big)-\mathbb{1}_g\Big(\sum_z h(g,a_{\bar{f}(g,z)})-h(g,a_{\bar{f}(g,z+q)})\Big)
\end{aligned}
$$

□

With this theorem the quaternary coefficients are reduced even further to calculations involving binary coefficients.

3.4 Bounds on Quaternary Cyclotomic Polynomials

Recently there has been increasing interest in the inverse cyclotomic polynomial [21] [3]. There is a strong connection between the inverse and the non-inverse cyclotomic polynomials. If one can understand the inverse then one can in turn use these tools for properties about the cyclotomic polynomials and vice versa. I will start as in the quaternary case by giving a formula for its coefficients. After I will give a bound on the coefficients of the inverse ternary cyclotomic polynomial. I will use this bound and the formulas from the previous section together with the Sister Beiter Conjecture to give a bound on the Quaternary cyclotomic polynomial. The bound that I give in this section was previously discussed by Bzdęga (2010) [8]. He assumed a known bound for the ternary cyclotomic polynomial as well and theory shown in [6] to give a conditional proof.

Lemma 3.4.1. *Suppose* $\psi_{pqr}(X) = \sum_i \bar{c}_i X^i$ *and* $\phi_{pq}(X) = \sum_i a_i X^i$
Let $2 < p < q < r$ *be primes. Take* $f(i)$ *be the unique value* $0 \leq f(i) < r$ *such that* $f(i) \equiv i \mod r$. *Then,*

$$\bar{c}_i = \sum_{k=0}^{g(i)} (a_{f(i)+r\cdot k}) \cdot \chi(g(i)-k) \quad \textit{with} \quad g(i) = \left\lfloor \frac{i}{r} \right\rfloor.$$

Where $\chi(h) = -1$ *if* $h \in [0, p-1]$, 1 *if* $h \in [q, q+p-1]$ *and* 0 *otherwise.* «

Proof. Because of the properties in 2.0.5 and 2.0.7 it follows that

$$\begin{aligned}
\psi_{pqr}(X) =& \phi_{pq}(X)\psi_{pq}(X^r) \\
=& \phi_{pq}(X)(-1 - X^r - \cdots - X^{r(p-1)} + X^{rq} + \cdots + X^{r(p+q-1)}) \\
=& -\sum_{i=0}^{\varphi(pq)} a_i X - \cdots - \sum_{i=0}^{\varphi(pq)} a_i X^{r(p-1)+i} + \sum_{i=0}^{\varphi(pq)} a_i X^{rq+i} + \cdots + \sum_{i=0}^{\varphi(pq)} a_i X^{r(p+q-1)+i}.
\end{aligned}$$

$$\begin{array}{llll|l}
-a_0 - \ldots & -a_r X^r - a_{r+1} X^{r+1} - \ldots & -a_{2r} X^{2r} - a_{2r+1} X^{2r+1} + \ldots & & \sum_{i=0}^{\varphi(pq)} -a_i X^i \\
 & -a_0 X^r - a_1 X^{r+1} - \ldots & -a_r X^{2r} - a_{r+1} X^{2r+1} + \ldots & & \sum_{i=0}^{\varphi(pq)} -a_i X^{r+i} \\
= & & -a_0 X^{2r} - a_1 X^{2r+1} + \ldots & & \sum_{i=0}^{\varphi(pq)} -a_i X^{2r+i} \\
 & & & & \vdots
\end{array}$$

The claim then follows directly from matching the exponent terms above. □

With this formula I can prove a bound on the height of the inverse cyclotomic polynomials.

Proposition 3.4.2. *Suppose* $2 < p < q < r$ *primes. The height of the ternary inverse cyclotomic polynomial is bounded by:*

$$A(\psi_{pqr}) \leq p - 1$$

«

Proof. Because of above 3.4.1 the following holds

$$\begin{aligned}
A(\psi_{pqr}) &\leq \left\lfloor \frac{\varphi(pq)}{r} \right\rfloor + 1 \leq \left\lfloor \frac{(p-1)(q-1)}{r} \right\rfloor + 1 \leq \frac{(p-1)(q-1)}{r} + 1 \\
&\leq (p-1)\frac{q-1}{r} + 1 < p - 1 + 1 = p.
\end{aligned}$$

In the last inequality I used the fact that $r > q$. Thus $A(\psi_{pq}) \leq p - 1$. □

Pieter Moree in 2009 [21] had found this bound with similar arguments. He went on to show the conditions needed to be set on the inverse cyclotomic polynomial to find equality. Here I will instead use this together with the Sister Beiter Conjecture 3.2.1 and previous built tools in proving a bound on quaternary cyclotomic polynomials.

Theorem 3.4.3. *Assuming the corrected sister beiter conjecture*

$$A(\phi_{pqrs}(X)) \leq \frac{2}{3}p^3q.$$

«

Proof. Suppose $\phi_{pqrs}(X) = \sum_i d_i X^i$, $\phi_{pqr}(X) = \sum_i c_i X^i$ and $\psi_{pqr}(X) = \sum_i \bar{c}_i X^i$. As in 3.3.5 given n let $c'_i = c_i$ if $si \leq n$, and 0 otherwise. Take let $f(m)$ be the unique value $0 \leq f(m) < pqr$ such that

$$f(m) \equiv s^{-1}(n-m) \mod pqr$$

Note that s^{-1} exists because it is coprime to pqr. Then

$$d_n = \sum_{m=0}^{pqr-\varphi(pqr)} \bar{c}_m \cdot c'_{f(m)}$$

The same arguments as in example 3.3.6 (for arbitrary prime $s > r$) can be reproduced to see that are at most $\lfloor \frac{pqr}{s} \rfloor + 1$ indices such that $c'_{f(m)} \neq 0$. So then

$$\begin{aligned}
|a_l| &\leq \sum_{m=0}^{pqr-\varphi(pqr)} |\bar{c}_m| \cdot |c'_{f(m)}| \\
&\leq \sum_{m=0}^{pqr-\varphi(pqr)} |c_i| \frac{2p}{3} && \text{corrected sister Beiter conjecture} \\
&\leq \sum_{m=0}^{pqr-\varphi(pqr)} (p-1)\frac{2p}{3} \leq (\left\lfloor \frac{pqr}{s} \right\rfloor + 1)(p-1)\frac{2p}{3} && 3.4.2 \\
&\leq (pq+1)(p-1)\frac{2p}{3} \leq (p^2q - pq + p - 1)\frac{2p}{3} \leq \frac{2}{3}p^3q && s > r
\end{aligned}$$

□

4 Computations on cyclotomic polynomials

As was noted in the introduction, part of the reason why so much of the information on coefficients of cyclotomic polynomials were unknown for a long time, was because of its difficulty in computation. The quaternary cyclotomic polynomial $\phi_{3\cdot5\cdot7\cdot11}$ already has $\varphi(3\cdot5\cdot7\cdot11) = 480$ coefficients. Writing out coefficients of these polynomials with pen and paper is practically impossible. An efficient algorithm that minimizes time and space complexity in computations is thus of great use herein. With this motivation I will briefly discuss two algorithms and give some data computed with these algorithms in this section. Both the algorithms are implemented using the Pari library in *C*. The algorithms are given by Andrew Arnold and Michael Monagan (2011) [4]. In their paper Arnold and Monogan mentioned the algorithms below and supported the claims. I rephrased the first as a theorem and briefly covered the proof as it is similar to 3.3.5.

4.1 Big prime algorithm

A big problem in computation of coefficients in the millions and billions of digits is space complexity; there may not be enough space for these coefficients to be held in memory. The way Arnold and Monogan approached this problem was by considering these coefficient modulo some prime. The approach is very similar to the approach in Kaplan's lemma and essentially a generalization of the theorem 3.3.5 I gave in the previous section.

Suppose $n = mp$ where m is a product of odd primes and $p >> m$. Let $\phi_{mp}(X) = \sum_l d_l X^l$, $\phi_m(X) = \sum_l c_l X^l$ and $\psi_m(X) = \sum_l \bar{c}_l X^l$.

Theorem 4.1.1. *(Arnold and Monogan, 2011 [4])*

$$d_k = -\sum_{(i,j)} b_i c_j$$

with $i \leq \deg m - \varphi(m)$ *and* $j \leq s\varphi(m)$ *with* $ip + j \equiv k \mod m$ *and* $ip + j \leq n$. *And the following recurrence holds.*

$$d_k = d_{k-m} - \sum_{ip+j=k} \bar{c}_i c_j$$

«

Proof. Take again the decomposition (assuming $|X| < 1$)

$$\phi_n(X) = \frac{\psi_m(X)\phi_m(X^p)}{X^m - 1} = -\psi_m(X)\phi_m(X^p)(1 + X^m + X^{2m} + \dots) \tag{5}$$

So the terms $-\bar{c}_i c_j X^{i+jp+lm}$ in $-\psi_m(X)\phi_m(X^s)(1 + X^m + X^m + \dots)$ will have exactly one term with exponent equal to k if and only if the exponent in the term is congruent to k modulo m and smaller or equal to k. And thus d_n is as given. Note that the exponents of the monomials in the terms all differ with value lm from each other. So the recurrence holds as well. □

The recurrence is the key observation as it essentially removes the need to store in between calculations of the unnecessary coefficients. It takes $\mathcal{O}(m^2) = \mathcal{O}(n^2/p^2)$ integer operations assuming $\phi_m(X)$ and $\psi_m(X)$ are given. And with this it is clear that it is most useful when $p >> m$. To reduce disk space required even further Arnold and Monagan make use of the palindromic nature of $\phi_n(X)$ and only look at the first half of the coefficients.

Algorithm 1 Big prime algorithm for computing the height of ϕ_n

Input: $n = mp$, square free odd positive integer with largest prime divisor p
$b_0, \ldots, b_{\varphi(m)/2}$, first half of coefficients of ϕ_m
$c_0, \ldots, c_{m-\varphi(m)}$, coefficients of ψ_m
Output: H, height of ϕ_n

```
ā(0), ..., ā(m − 1) ← 0, ..., 0
H ← 0
for 0 ≤ i ≤ ⌊φ(n)/2p⌋ do
    for 0 ≤ j ≤ m − φ(m) do
        k ← ip + j  mod m
        ā(k) ← ā(k) − b_i c_j
        if j < p and |ā(k)| > H then
            H ← |ā(k)|
return H
```

4.2 Sparse power series (SPS) algorithm

The big prime algorithm works best for $n = mp$ with $p >> m$. For general cases however the SPS algorithm works better.

Algorithm 2 Sparse power series (SPS) algorithm for computing the height of ϕ_n

Input: $n = p_1 p_2 \ldots p_k$, a product of k disting primes

Output: $a_0, \ldots, a_{\varphi(m)/2}$, first half of coefficients of ϕ_m

```
D ← φ(n)/2, a_0 ← 1
for 1 ≤ i ≤ D do
    a_i ← 0
    for d|n such that d > 0 do
        if μ(n/d) then                          ▷ multiply by (1 − X^d)
            for i = D down to d by −1 do
                a_i ← a_i − a_{i−d}
        else                                    ▷ divide by (1 − X^d)
            for i = d to D do
                a_i ← a_i + a_{i−d}
return a_0, ..., a_{φ(m)/2}
```

The sparse power series considers $\phi_n(X) = \sum_{i=0}^{\infty} a_i X^i$ with $a_i = 0$ if $i > \varphi(n)$ a power series. Like in the introduction because of the Möbius inversion function

$$\phi_n(X) = \Pi_{d|n}(X^{n/d} - 1)^{\mu(d)}$$

And

$$\phi_{pq}(X) = \frac{(1 - X^p)(1 - X^q)(1 - X)}{(1 - X^{pq})}$$

So every cyclotomic polynomial is constructed by multiplication and division of $1 - X^d$. Since division is computationally expensive, multiplication by its power series expansion is instead used. Multiplication is simple and computationally cheap. The SPS algorithm requires $\mathcal{O}(2^k \cdot \varphi(n))$ integer operations to compute $\phi_n(X)$ of order k. This in brief describes the (SPS) algorithm. Below I will write some observations I made while computing coefficients of cyclotomic polynomials with these algorithms that may require further research.

(1) During computations as one gets closer to the center coefficient of $\phi_n(X)$ one will with more frequently encounter bigger coefficients in magnitude. A further research might answer why this is the case. (see figure 6)

(2) During computations the maximum observed height of cyclotomic polynomials with $n = 7 \cdot 11 \cdot p_r \cdot p_s$ and $p_r \in \{p_6, \ldots, p_{100}\}, p_s \in \{p_{r+1}, \ldots, p_{101}\}$ was $A(n) = 89$. The maximum observed height of cyclotomic polynomials with $n = 3 \cdot 5 \cdot p_r \cdot p_s$ and $p_r \in \{p_4, \ldots, p_{103}\}, p_s \in \{p_{r+1}, \ldots, p_{104}\}$ was $A(n) = 10$. (see figure 4.)

The heights observed are much less than the prescribed bound in 3.4.3 of $\frac{2}{3}pq^3$. A further research might include how close one can get to these bounds computationally. Improving on existing algorithms in this research might be fruitful and interesting.

(3) During computations the maximum observed jump of cyclotomic polynomials with $n = 7 \cdot 11 \cdot p_r \cdot p_s$ and $p_r \in \{p_6, \ldots, p_{100}\}, p_s \in \{p_{r+1}, \ldots, p_{101}\}$ was $J(n) = 137$. The maximum observed jump of cyclotomic polynomials with $n = 3 \cdot 5 \cdot p_r \cdot p_s$ and $p_r \in \{p_4, \ldots, p_{103}\}, p_s \in \{p_{r+1}, \ldots, p_{104}\}$ was $J(n) = 19$. (see figure 5.)

The jumps behave oddly. In the latter case I have not observed a jump such that $J(n) < 9$ or $J(n) = 96$ for some n, I did observe $J(n) = 95$ and $J(n) = 97$. There appears to be gaps in between the possible jumps for some values n. An interesting further research question might be: does every natural number appear as some jump value of a (quartenary) cyclotomic polynomial.

Another interesting question would be whether there is a bound for the jump of quaternary cyclotomic polynomials, when fixing odd primes $p < q < r < s$.

(4) During computations the lowest observed height of cyclotomic polynomials with $n = pqrs, p = 3, q = 5, r = 7$ and $s > pqr$ was $A(n) = 2$. They all were polynomials with $s \equiv \pm 1 \mod pqr$ and $s \equiv \pm 4 \mod pqr$. (see figure 2.)

I will end this section with tables and graphs using both algorithms. They can be seen at the end of this thesis.

5 Prime gaps

In 2013 Yitang Zhang [28] released an unexpected paper on bounds of prime pairs. He found that there are infinite prime pairs that differ by less than 70 million from each other. This brought a lot of interest in the famous twin prime conjecture and prime gaps in general. Years later in 2022 another mathematician by the name of James Alexander Maynard even won a fields medal in this same field partly for his contributions in prime gaps. This setting created not only interest in prime gaps but also in everything related to it. An example of this is the very related and recent article by Pieter Moree (2021) [20] in which he explains results in specific from Moree & Rosu (2012) [23] and relates it to cyclotomic polynomials and prime gaps. Much of this section resembles Moree's article.

Take the ternary cyclotomic polynomial ϕ_{pqr}. Let H be the set of possible heights for these polynomials. As one computes heights of ternary cyclotomic polynomials (figure.4, figure.2) one might suspect that every single integer appears in H with the ternary polynomial suitably large. Thus

Conjecture 5.0.1. *Every natural numbers, excluding zero, occurs as the height of some ternary cyclotomic polynomial.* «

Using the reformulation of Lam and Leung's theorem about coefficients of binary cyclotomic polynomials 3.2.3 and Kaplan's Lemma 3.2.2 Moree and Rosu showed.

Theorem 5.0.2. *(Rosu, Moree, 2012 [23]) Let $m \geq 0$ be an arbitrary integer and $p \geq 4m2 + 2m + 3$ be any prime. Then there exist primes q_1, r_1, q_2, r_2 such that $\phi_{pq_1r_1}$ and $\phi_{pq_2r_2}$ have maximum coefficient $\frac{(p-1)}{2} - m$, respectively $\frac{(p+1)}{2} + m$.* «

This theorem implies that the set of possible heights is $\{\frac{p-1}{2} + m, p \geq 4m^2 + 2m + 3 \text{ prime}, m \geq 0\} \cup \{\frac{p-1}{2} - m, p \geq 4m^2 + 2m + 3 \text{ prime}, m \geq 0\}$ [23]. So the above conjecture is true if this set equals $\mathbb{Z}_{\geq 1}$. The validity of the conjecture thus depends heavily on the behaviour of gaps within prime numbers. This conjecture appears to be very hard to solve. To illustrate this I will take a look at some famous conjectures in number theory and relate it to this problem.

Legendre's conjecture is part of the 4 problems proposed by Landau in 1912 it is still unsolved at the time of writing. An even stronger statement is Andrica's conjecture which is shown below. Both these conjectures are far out of reach for this thesis and will not be discussed themselves.

Conjecture 5.0.3. *(Legendre's conjecture) There is a prime number between n^2 and $(n+1)^2$ for every $n \in \mathbb{Z}_{>0}$.* «

Conjecture 5.0.4. *(Andrica's conjecture)*

$$\sqrt{p_{n+1}} - \sqrt{p_n} < 1$$

«

Proposition 5.0.5. *Andrica's conjecture implies legendres conjecture.* «

PROOF. Suppose Andrica's conjecture holds. Then

$$\begin{aligned}\sqrt{p_{n+1}} - \sqrt{p_n} &< 1\\ p_{n+1} - p_n &< \sqrt{p_{n+1}} + \sqrt{p_n}\\ &< 2\sqrt{p_n} + 1 < 2p_n + 1\\ &< p_n + 2\sqrt{p_n} + 1 - p_n\\ &< (\sqrt{p_n} + 1)^2 - p_n.\end{aligned}$$

So now suppose n arbitrary. Take p_i to be the largest prime smaller or equal to $(n+1)^2$. Suppose $p_i < n^2$ but then

$$p_{i+1} < (\sqrt{p_i} + 1)^2 < (n+1)^2.$$

This leads to a contradiction because p_i was supposed to be the largest prime smaller or equal to $(n+1)^2$. □

Now Kosyak and Moree proved [15].

Theorem 5.0.6. *Andrica's conjecture implies* $H = \mathbb{N}$. «

This relationship is quite surprising. From above it is clear that involved conjectures in (analytic) number theory show a lot about coefficients of cyclotomic polynomials. It is unclear whether notions and properties of cyclotomic polynomial can be of help in the opposite direction. This could be another interesting direction a further research could take.

6 Acknowledgment

First and foremost, I would like to express my gratitude towards my thesis supervisor Dr. Eugenia Rosu for her valuable and helpful guidance while writing this thesis. Her enthusiasm and immense knowledge was very inspiring. Without her help I could have never written this thesis.

Furthermore, I would like to thank Prof.dr. Hendrik Lenstra, Dr. Marco Streng and Prof.dr. Jan Vonk for their valuable input and motivating feedback. Their enthusiasm and sincere interest during the bachelor seminars were very valuable to me.

Finally, I would also like to thank all the people who have contributed in some way towards writing this thesis that I have not mentioned here.

7 References

[1] Ala'a Al-Kateeb, Mary Ambrosino, Hoon Hong, and Eunjeong Lee, *Maximum gap in cyclotomic polynomials*, 2020.

[2] Ala'a Al-Kateeb, Hoon Hong, and Eunjeong Lee, *Explicit expression for a family of ternary cyclotomic polynomials*, 2018.

[3] Dorin Andrica and Ovidiu Bagdasar, *Remarks on the coefficients of inverse cyclotomic polynomials*, Mathematics **11** (2023), no. 17.

[4] Andrew Arnold and Michael B. Monagan, *Calculating cyclotomic polynomials*, Math. Comput. **80** (2011), no. 276, 2359–2379.

[5] A. S. Bang, *Om ligningen œÜ n (x) = o*, Nyt tidsskrift for matematik **6** (1895), 6–12.

[6] P. T. Bateman, C. Pomerance, and R. C. Vaughan, *On the size of the coefficients of the cyclotomic polynomial*, Topics in classical number theory (Amsterdam) (Gábor Halász, ed.), vol. I, Colloquia Mathematica Societatis János Bolyai, no. 34, North-Holland, Amsterdam, 1984, (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., pp. 171–202.

[7] Marion Beiter, *Magnitude of the coefficients of the cyclotomic polynomial fpqr(x)*, The American Mathematical Monthly **75** (1968), no. 4, 370–372.

[8] Bartlomiej Bzdega, *On the height of cyclotomic polynomials*, 2010.

[9] ———, *Jumps of ternary cyclotomic coefficients*, 2013.

[10] Yves Gallot and Pieter Moree, *Ternary cyclotomic polynomials having a large coefficient*, 2008.

[11] Yves Gallot, Pieter Moree, and Huib Hommersom, *Value distribution of cyclotomic polynomial coefficients*, 2008.

[12] Hoon Hong, Eunjeong Lee, Hyang-Sook Lee, and Cheol-Min Park, *Maximum gap in (inverse) cyclotomic polynomial*, 2011.

[13] Branko Juran, Pieter Moree, Adrian Riekert, David Schmitz, and Julian Völlmecke, *A proof of the corrected sister beiter cyclotomic coefficient conjecture inspired by zhao and zhang*, 2023.

[14] Nathan Kaplan, *Flat cyclotomic polynomials of order three*, Journal of Number Theory **127** (2007), no. 1, 118–126.

[15] Alexandre Kosyak, Pieter Moree, Efthymios Sofos, and Bin Zhang, *Cyclotomic polynomials with prescribed height and prime number theory*, 2020.

[16] T. Y. Lam and K. H. Leung, *On the cyclotomic polynomial $\phi_{pq}(x)$*, The American Mathematical Monthly **103** (1996), no. 7, 562–564.

[17] Emma Lehmer, *On the magnitude of the coefficients of the cyclotomic polynomial*, Bulletin of the American Mathematical Society **42** (1936), no. 6, 389 – 392.

[18] H.W. Lenstra, *Vanishing sums of roots of unity*, in: Proceedings, Bicentennial Congress Wiskundig Genootschap, no. Part II, Vrije Universiteit, 1979, pp. 249–268.

[19] Herbert Möller, *Über diei-ten koeffizienten der kreisteilungspolynome*, Mathematische Annalen **188** (1970), no. 1, 26–38.

[20] P. Moree, *Prime gaps and cyclotomic polynomials*.

[21] Pieter Moree, *Inverse cyclotomic polynomials*, Journal of Number Theory **129** (2009), no. 3, 667–680.

[22] ———, *Numerical semigroups, cyclotomic polynomials and bernoulli numbers*, 2013.

[23] Pieter Moree and Eugenia Rosu, *Non-beiter ternary cyclotomic polynomials with an optimally large set of coefficients*, International Journal of Number Theory **08** (2012), no. 08, 1883–1902.

[24] So Hyun Park, Suhri Kim, Dong Hoon Lee, and Jong Hwan Park, *Improved ring lwr-based key encapsulation mechanism using cyclotomic trinomials*, IEEE Access **8** (2020), 112585–112597.

[25] Carlo Sanna, *A survey on coefficients of cyclotomic polynomials*, 2021.

[26] P. Stevenhagen, *Algebra III*, Universiteit Leiden, 2020.

[27] Bin Zhang, *Remarks on the maximum gap in binary cyclotomic polynomials*, 109–115.

[28] Yitang Zhang, *Bounded gaps between primes*, Ann. Math. (2) **179** (2014), no. 3, 1121–1174 (English).

$$A(n) := A(\phi_n(X)) := max_{j\geq 0}|a_n(j)|$$

Figure 1: Height table for ϕ_n with $n = 3 \cdot 5 \cdot 7 \cdot p_s$ with primes $p_s > 105$ on the two left, and some primes $p_s < 105$ opposite.

p_s	$p_s \mod 105$	$A(105 \cdot p_s)$
211	1	2
107	2	3
109	4	2
113	8	4
431	11	3
223	13	4
331	16	3
227	17	5
229	19	4
127	22	4
233	23	4
131	26	6
239	29	3
241	31	4
137	32	4
139	34	7
457	37	5
353	38	5
251	41	4
463	43	4
149	44	4
151	46	3
257	47	3
157	52	3

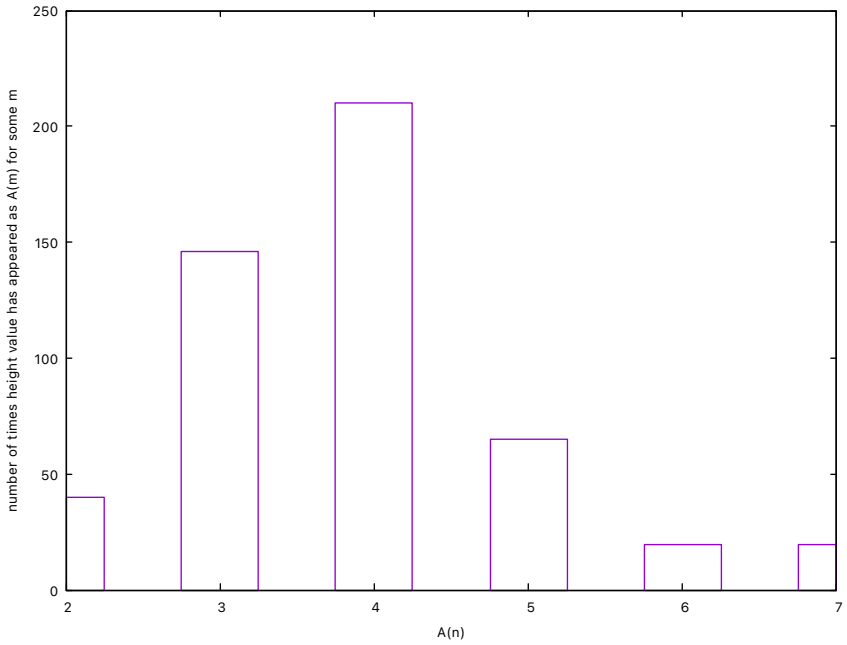
p_s	$p_s \mod 105$	$A(105 \cdot p_s)$
263	53	3
163	58	3
269	59	3
271	61	4
167	62	4
379	64	4
277	67	5
173	68	5
281	71	7
283	73	4
179	74	4
181	76	3
499	79	6
397	82	4
293	83	4
191	86	4
193	88	5
509	89	3
197	92	4
199	94	3
307	97	4
311	101	2
313	103	3
419	104	2

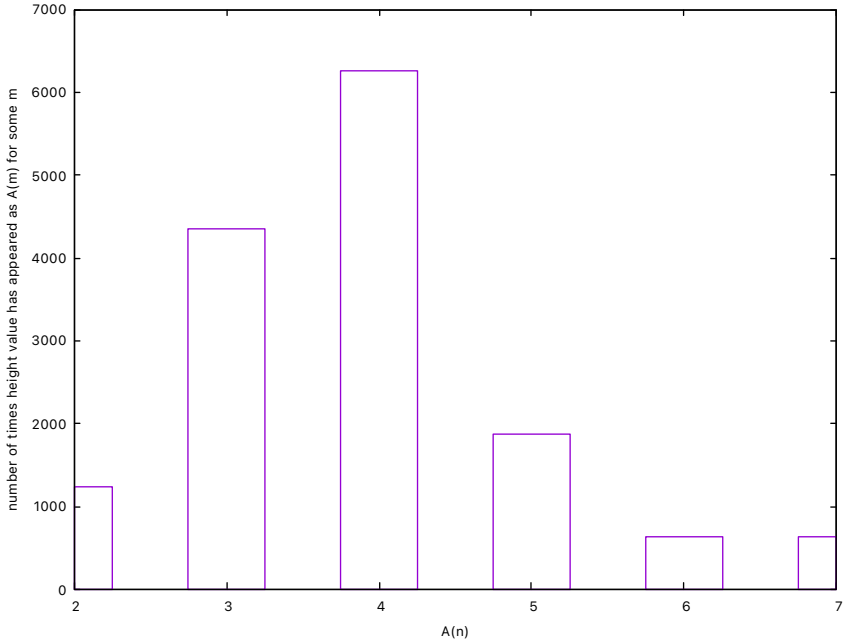
p_s	$p_s \mod 105$	$A(105 \cdot p_s)$
11	11	3
13	13	4
17	17	5
19	19	4
23	23	4
29	29	3
31	31	4
37	37	5
41	41	4
43	43	4
47	47	3
53	53	3
59	59	3
61	61	4
67	67	5
71	71	7
73	73	4
79	79	6
83	83	4
89	89	3
97	97	4
101	101	2
103	103	3

$$A(n) := A(\phi_n(X)) := max_{j \geq 0} |a_n(j)|$$

Height Histograms for ϕ_n with $n = 3 \cdot 5 \cdot 7 \cdot p_s$

Figure 2: Histograms for $A(3 \cdot 5 \cdot 7 \cdot p_s), p_s \in \{p_5, \ldots, p_{503}\}$ and $p_s \in \{p_5, \ldots, p_{15003}\}$ respectively.

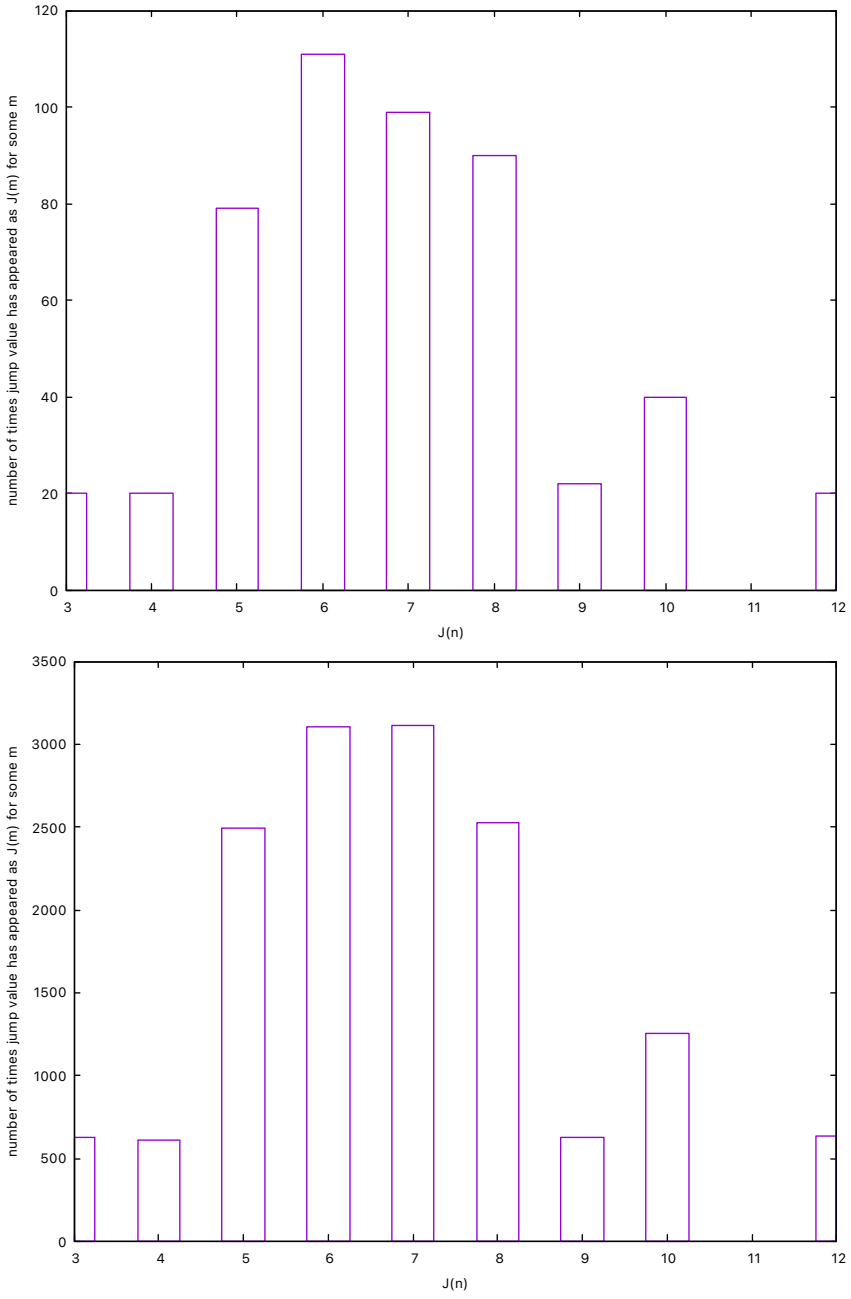




$$J(n) := J(\phi_n(X)) := max_{j\geq 1}|a_n(j) - a_n(j-1)|$$

Jump Histograms for ϕ_n with $n = 3 \cdot 5 \cdot 7 \cdot p_s$

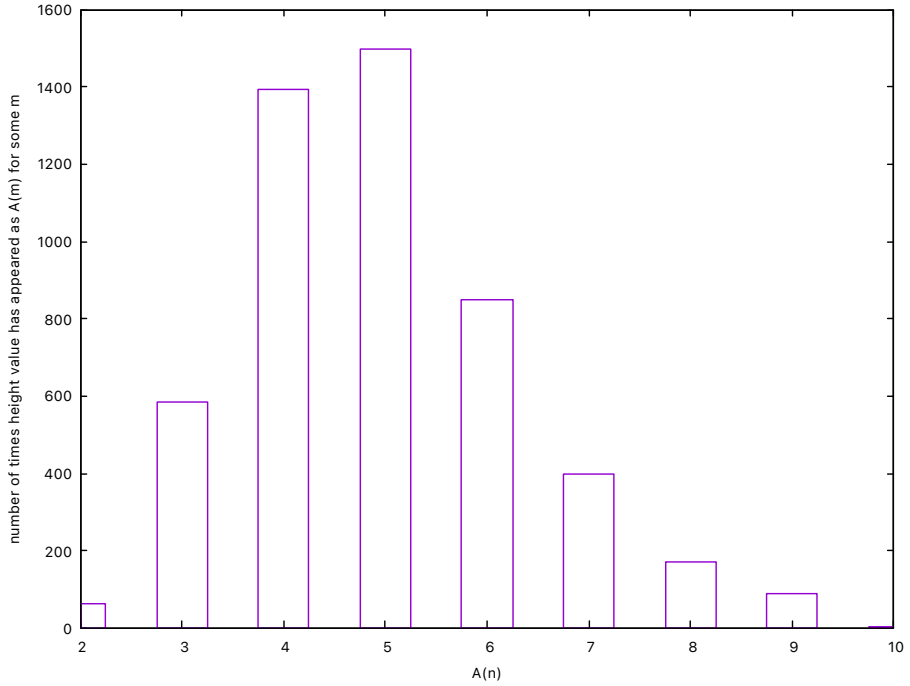
Figure 3: Histograms for $J(3 \cdot 5 \cdot 7 \cdot p_s)$ with $p_s \in \{p_4, \ldots, p_{503}\}$ and $p_s \in \{p_4, \ldots, p_{15003}\}$ respectively.

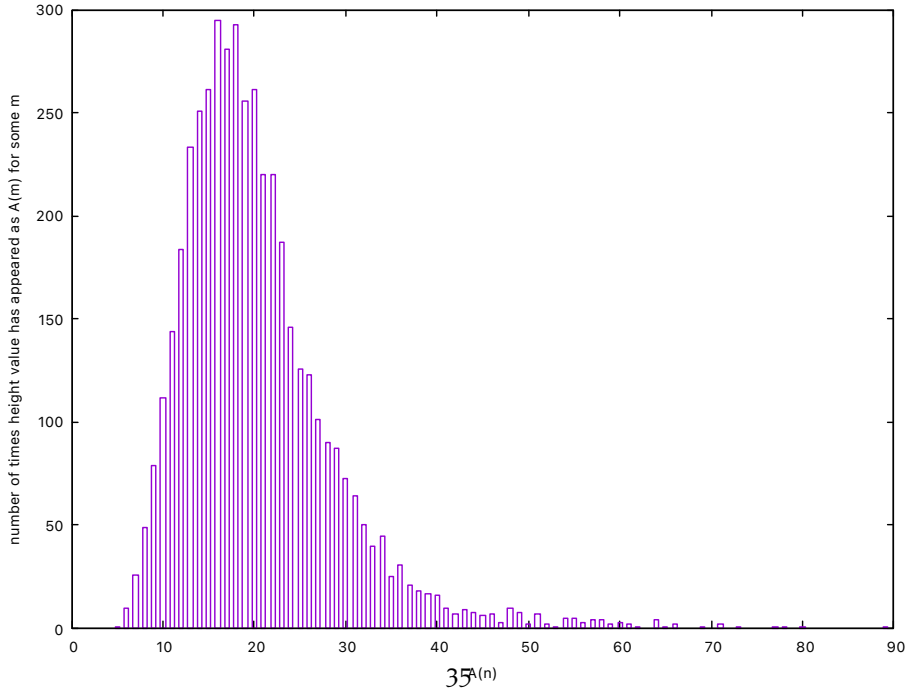


$$A(n) := A(\phi_n(X)) := max_{j\geq 0}|a_n(j)|$$

Height Histograms for ϕ_n with $n = 3 \cdot 5 \cdot p_r \cdot p_s$

Figure 4: Histograms for $A(3 \cdot 5 \cdot p_r \cdot p_s), p_r \in \{p_5, \ldots, p_{103}\}, p_s \in \{p_{r+1}, \ldots, p_{104}\}$
Opposite Histogram for $A(7 \cdot 11 \cdot p_r \cdot p_s), p_r \in \{p_6, \ldots, p_{100}\}, p_s \in \{p_{r+1}, \ldots, p_{101}\}$

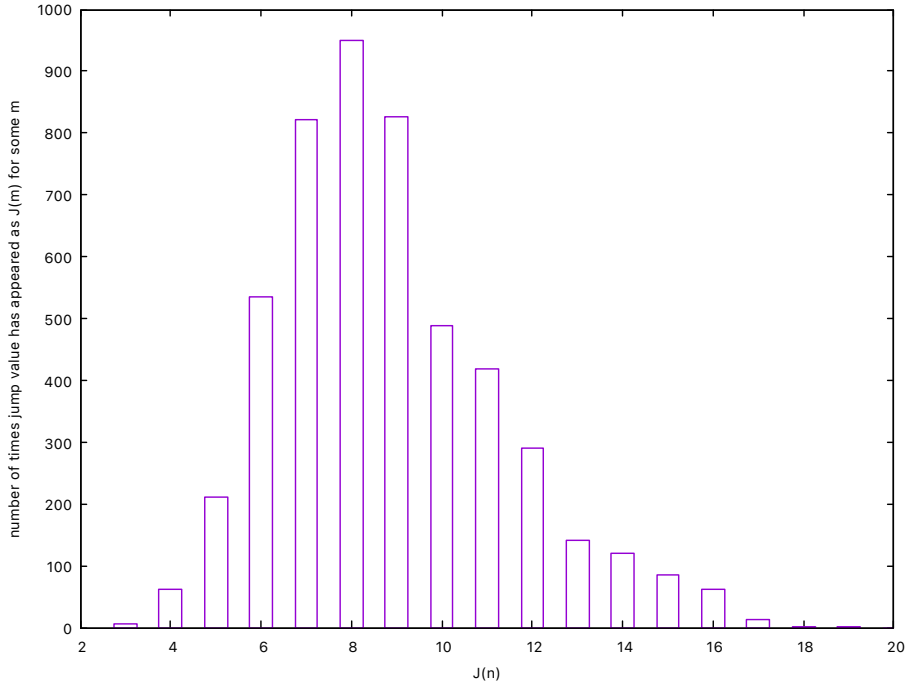


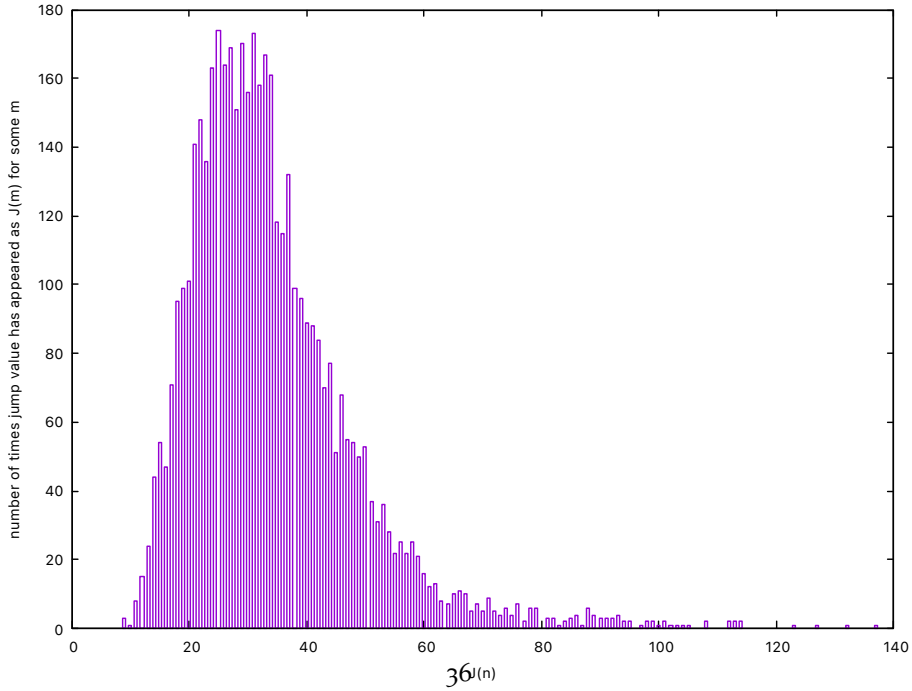


$$J(n) := J(\phi_n(X)) := max_{j\geq 1}|a_n(j) - a_n(j-1)|$$

Jump Histograms for ϕ_n with $n = 3 \cdot 5 \cdot p_r \cdot p_s$

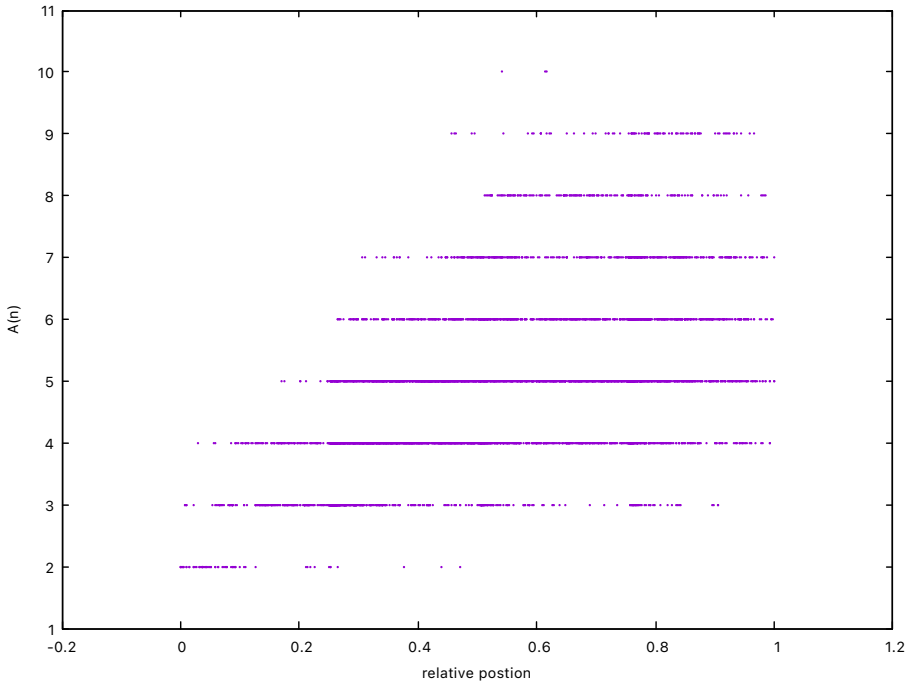
Figure 5: Above Histogram for $J(3 \cdot 5 \cdot p_r \cdot p_s), p_r \in \{p_4, \ldots, p_{103}\}, p_s \in \{p_{r+1}, \ldots, p_{104}\}$
Opposite Histogram for $J(7 \cdot 11 \cdot p_r \cdot p_s), p_r \in \{p_6, \ldots, p_{100}\}, p_s \in \{p_{r+1}, \ldots, p_{101}\}$

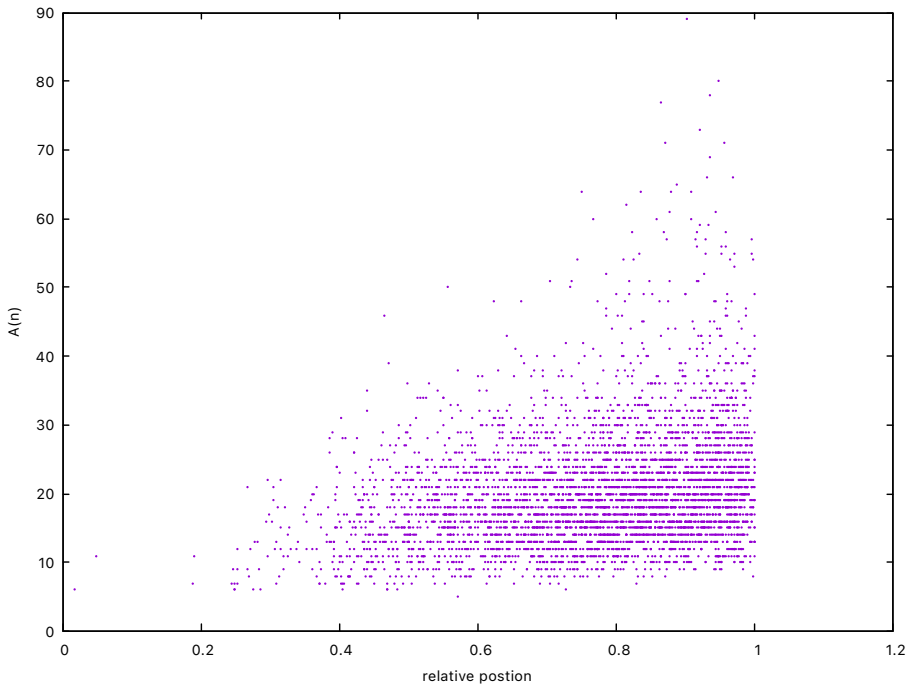




Height versus position

Figure 6: Height versus position above for $A(3 \cdot 5 \cdot p_r \cdot p_s), p_r \in \{p_4, \ldots, p_{54}\}, p_s \in \{p_{r+1}, \ldots, p_{55}\}$
Height versus position opposite for $A(7 \cdot 11 \cdot p_r \cdot p_s), p_r \in \{p_6, \ldots, p_{100}\}, p_s \in \{p_{r+1}, \ldots, p_{101}\}$





The coefficient of first found height in $\phi_n(X)$ on the x axis is plotted against the magnitude of the height on the y axis. On the horizontal axis 0 is the first coefficient and 1 is the $\varphi(n)/2$-th coefficient of $\phi_n(X)$.

```
#include <pari/pari.h>
#include <stdbool.h>

//simple search method to find the maximal coefficient
//in magnitude of a polynomial (column or pari t_Pol).
GEN FindMaxCoeff(GEN Poly)
{
  GEN MaxCoeff, MaxIndex, MaxJump;
  GEN ReturnArray = zerocol(3);
  int firstIndex = 2;

  if (typ(Poly) == t_POL)
    firstIndex = 3;

  MaxCoeff = (GEN) Poly[firstIndex];
  MaxJump = stoi(0);
  MaxIndex = stoi(0);

  //3 because 0 and 1 are reference positions or smtn
  for (long i = firstIndex + 1; i <= glength(Poly); i++)
  {
    if ( gcmp(absi((GEN) Poly[i]),MaxCoeff) == 1)
    {
      MaxCoeff = absi((GEN) Poly[i]);
      MaxIndex = stoi(i-(firstIndex + 2));
    }
    if (gcmp(absi(gsub((GEN) Poly[i],(GEN) Poly[i-1])),MaxJump) == 1)
      MaxJump = absi(gsub((GEN) Poly[i],(GEN) Poly[i-1]));
  }

  ReturnArray[1] = (long) MaxCoeff;
  ReturnArray[2] = (long) MaxIndex;
  ReturnArray[3] = (long) MaxJump;
  return ReturnArray;
}

//SPS algorithm to compute half of phi_n By Arnold & Monogan 2011
GEN SPS(GEN n)
{
  GEN OutputPolHalf, D = gdiv(eulerphi(n),stoi(2));
  OutputPolHalf = zerocol(gtos(gadd(gdiv(eulerphi(n),stoi(2)),stoi(2))));
  OutputPolHalf[2] = (long) stoi(1);

  for(int d = 1; d <= gtos(n); d++)
  {
    if(gcmp(gmod(n,stoi(d)),stoi(0)) == 0)
    {
      if(gcmp(stoi(moebius(gdiv(n,stoi(d)))),stoi(1)) == 0)
      {
        for(int i = gtos(D); i >= d; i--)
        {
```

```
          OutputPolHalf[i+2] = (long) gsub((GEN) OutputPolHalf[i+2],(GEN)
              OutputPolHalf[i-d+2]);
        }
      }
      else
      {
        for(int i = d; i <= gtos(D); i++)
        {
          OutputPolHalf[i+2] = (long) gadd((GEN) OutputPolHalf[i+2],(GEN)
              OutputPolHalf[i-d+2]);
        }
      }
    }
  }

  return FindMaxCoeff(OutputPolHalf);
}

//Big prime algorithm to compute the height of phi_n By Arnold & Monogan
    2011
GEN BigPrime(GEN CycloP,GEN InvCycloP, GEN m, GEN p)
{
  GEN OutputPolHalf, H = stoi(0), k = stoi(0);
  OutputPolHalf = zerocol(gtos(m));
  GEN ReturnArray = zerocol(2);

  for(int i = 0; gequal1(gle(stoi(i),gfloor(gdiv(eulerphi(gmul(m,p)),gmul(
      stoi(2),p))))) == 1; i++)
  {
    for (int j = 0; gequal1(gle(stoi(j),gsub(m,eulerphi(m)))) == 1;j++)
    {
      k = gmod(gadd(gmul(stoi(i),p),stoi(j)),m);
      OutputPolHalf[gtos(k)+1] = (long) gsub((GEN)OutputPolHalf[gtos(k)+1],
          gmul((GEN)CycloP[i+2],(GEN)InvCycloP[j+2]));

      if(gequal1(glt(stoi(j),p)) == 1 && gequal1(glt(H,absi((GEN)
          OutputPolHalf[gtos(k)+1]))) == 1)
      {
        H = absi((GEN)OutputPolHalf[gtos(k)+1]);
        ReturnArray[1] = (long) H;
        ReturnArray[2] = (long) gadd(gmul(stoi(i),p),stoi(j));
      }
    }
  }
  return ReturnArray;
}

//Big prime algorithm to compute half of phi_n By Arnold & Monogan 2011
GEN BigPrimeWholePoly(GEN CycloP,GEN InvCycloP, GEN m, GEN p)
{
  GEN PolHalf, OutputPolHalf, H = stoi(0), k = stoi(0);
  PolHalf = zerocol(gtos(m));
```

```
  OutputPolHalf = zerocol(gtos(gadd(gdiv(eulerphi(gmul(m,p)),stoi(2)),stoi
      (2))));

  for(int i = 0; gequal1(gle(stoi(i),gfloor(gdiv(eulerphi(gmul(m,p)),gmul(
      stoi(2),p))))) == 1; i++)
  {
    for (int j = 0; gequal1(gle(stoi(j),gsub(m,eulerphi(m)))) == 1;j++)
    {
      k = gmod(gadd(gmul(stoi(i),p),stoi(j)),m);
      PolHalf[gtos(k)+1] = (long) gsub((GEN)PolHalf[gtos(k)+1],gmul((GEN)
          CycloP[i+2],(GEN)InvCycloP[j+2]));
    }
    for (int l = i*gtos(p); gcmp(stoi(l),gmul(p,stoi(i+1))) == -1;l++)
    {
      OutputPolHalf[l+2] = PolHalf[gtos(gmod(stoi(l),m))+1];
    }
  }
  return FindMaxCoeff(OutputPolHalf);
}


//Inverse cycltomic polynomial calculator divdes (x^n-1) by phi_n to get
    psi_n
GEN FindInvCycloPol(GEN CycloP,GEN m)
{
  GEN xm = mkpoln(2, gen_1,stoi(-1));
  xm = RgX_inflate(xm,gtos(m));
   //pari_printf("cyclo is %Ps \n", CycloP);
  xm = RgX_div(xm,CycloP);
  //pari_printf("inCyclo is %Ps \n", xm);
  return xm;
}

long modInverse(long a, long m)
{
  for (long x = 1; x < m; x++)
    if (((a % m)*(x % m)) % m == 1)
      return x;
  return 0;
}


//Method to use Pari's internal way of calculating phi_n
GEN PariMethod(GEN m, GEN p, GEN n, int printInfo)
{
  int startTime, elapsedTime;
  GEN CycNPolynomial,CycPolynomial, InvCycPolynomial, InflateCycPolynomial,
      ProductPoly, MaxCoeff,MaxIndex,MaxJump, RelPos;
  GEN ReturnVal;

  if(printInfo >= 0)
  {
```

```
    gettime();
    startTime = gettime();
  }

  CycNPolynomial = polcyclo_eval(gtos(n),NULL);
  ReturnVal = FindMaxCoeff(CycNPolynomial);

  if(printInfo >= 2)
    pari_printf("Cyclo_n Polynomial = %Ps \n", CycNPolynomial);

  MaxCoeff = (GEN) ReturnVal[1];
  MaxIndex = gmin(eulerphi(n),(GEN) ReturnVal[2]);
  MaxJump = (GEN) ReturnVal[3];
  RelPos = gdiv(MaxIndex,gdiv(eulerphi(n),stoi(2)));
  ReturnVal[4] = (long) RelPos;

  if(printInfo >= 0)
  {
    elapsedTime = gettime();
    printf("------ START PARI ------\n");
    pari_printf("Max coeff is %Ps \n", MaxCoeff);
    pari_printf("Max Jump is %Ps \n", MaxJump);
    pari_printf("first index containing max coeff is %Ps \n", MaxIndex);
    pari_printf("relative pos of max coeff is %Ps \n", RelPos);
    printf("Time it it took to calculate with PARI %dms\n", elapsedTime);
    printf("------------\n");
  }

  return ReturnVal;
}

//Method to use the Big prime algorithm and print relevant information
GEN BPMethod(GEN m, GEN p, GEN n, int printInfo)
{
  int startTime, elapsedTime;
  GEN CycNPolynomial,CycPolynomial, InvCycPolynomial, InflateCycPolynomial,
      ProductPoly, MaxCoeff,MaxIndex,MaxJump, RelPos;
  GEN ReturnVal;

  if(printInfo >= 0)
  {
    gettime();
    startTime = gettime();
  }

  CycPolynomial = polcyclo(gtos(m),0);
  InvCycPolynomial = FindInvCycloPol(CycPolynomial,m);

  //ReturnVal = BigPrime(CycPolynomial,InvCycPolynomial,m,p);          //this
      method only returns the height
  ReturnVal = BigPrimeWholePoly(CycPolynomial,InvCycPolynomial,m,p);  //this
      method returns all coefficients (first half)
```

```
  MaxCoeff = (GEN) ReturnVal[1];
  MaxIndex = (GEN) ReturnVal[2];
  MaxJump = (GEN) ReturnVal[3];
  RelPos = gdiv(MaxIndex,gdiv(eulerphi(n),stoi(2)));;
  ReturnVal[4] = (long) RelPos;

  if(printInfo >= 0)
  {
    elapsedTime = gettime();
    printf("------ START BIG Prime ------\n");
    if(printInfo >= 1)
    {
      pari_printf("Cyclo_m Polynomial = %Ps \n", CycPolynomial);
      pari_printf("InvCyclo_m Polynomial = %Ps \n", InvCycPolynomial);
    }
    if(printInfo >= 3)
    {
      InflateCycPolynomial = RgX_inflate(CycPolynomial,gtos(p));
      ProductPoly = gmul(InflateCycPolynomial,InvCycPolynomial);
      pari_printf("Cyclo_m(x^p) Polynomial = %Ps \n", InflateCycPolynomial);
      pari_printf("Cyclo_m(x^p)*InvCyclo_m Polynomial = %Ps \n", ProductPoly
          );
    }
    pari_printf("Max coeff is %Ps \n", MaxCoeff);
    pari_printf("Max Jump is %Ps \n", MaxJump);
    pari_printf("first index containing max coeff is %Ps \n", MaxIndex);
    pari_printf("relative pos of max coeff is %Ps \n", RelPos);
    printf("Time it it took to calculate with BP %dms\n", elapsedTime);
    printf("------------\n");
  }
  return ReturnVal;
}

GEN SPSMethod(GEN n,int printInfo)
{
  int startTime, elapsedTime;
  GEN CycNPolynomial,CycPolynomial, InvCycPolynomial, InflateCycPolynomial,
      ProductPoly, MaxCoeff,MaxIndex,MaxJump, RelPos;
  GEN ReturnVal;

  if(printInfo >= 0)
  {
    gettime();
    startTime = gettime();
  }

  ReturnVal = SPS(n);

  MaxCoeff = (GEN) ReturnVal[1];
  MaxIndex = (GEN) ReturnVal[2];
  MaxJump = (GEN) ReturnVal[3];
```

```
  RelPos = gdiv(MaxIndex,gdiv(eulerphi(n),stoi(2)));;
  ReturnVal[4] = (long) RelPos;

  if(printInfo >= 0)
  {
    elapsedTime = gettime();
    printf("------ START SPS ------\n");
    pari_printf("Max coeff is %Ps \n", MaxCoeff);
    pari_printf("Max Jump is %Ps \n", MaxJump);
    pari_printf("first index containing max coeff is %Ps \n", MaxIndex);
    pari_printf("relative pos of max coeff is %Ps \n", RelPos);
    printf("Time it it took to calculate with PARI %dms\n", elapsedTime);
    printf("------------\n");
  }

  return ReturnVal;
}

void findHeights()
{
  //These variables represent the index of the odd primes p,q,r,s the i.e. p
      = 6th prime number
  long r_start = 6, r_end = 50;
  long s_start = 7, s_end = 51;
  int p_n = 4,q_n = 5;

  //verbosity level to avoid clutter or show more information
  int printInfoVerbose = 0;
  int methods[3] = {0,1,0}; // first is Pari internal, second is BP third is
      sps
  bool writeInfo = false;

  GEN l,m, n, p = prime(p_n), q = prime(q_n), s, r;
  GEN ReturnVal, TempPoly;

  l =  gmul(p,q);

  FILE *fpt,*fpt2,*fpt3,*fpt4,*fpt5,*fpt6;

  if(writeInfo)
  {
    fpt = fopen("MaxCoeffvsOrder.dat", "w+");
    fpt2 = fopen("MaxCoeffFirstRelPos.dat", "w+");
    fpt3 = fopen("MaxCoeffHistogram.dat", "w+");
    fpt4 = fopen("MaxJumpHistogram.dat", "w+");
    fpt5 = fopen("MaxJumpvsOrder.dat", "w+");
    fpt6 = fopen("MaxCoeffvsPosition.dat", "w+");
  }

  pari_sp av;
  gettime();
  //loop trough r,s and find possible heights
```

```
for (long i = (r_start > q_n) ? r_start: q_n + 1; i <= r_end; i++)
{
  r = prime(i);
  m = gmul(1,r);

  for (long j = (s_start > i) ? s_start: i + 1; j <= s_end; j++)
  {
    s = prime(j);
    n = gmul(m,s);

    if(printInfoVerbose >= 0 || (i == r_end && j == s_end) ||(i == r_start
        && j == r_start + 1))
    {
      printf("------␣General␣------\n");
      printf("Time␣is:␣%ld␣ms␣\n",gettime());
      pari_printf("i␣=␣%Ps␣\n", stoi(i));
      pari_printf("j␣=␣%Ps␣\n", stoi(j));
      pari_printf("p␣=␣%Ps␣\n", p);
      pari_printf("q␣=␣%Ps␣\n", q);
      pari_printf("r␣=␣%Ps␣\n", r);
      pari_printf("s␣=␣%Ps␣\n", s);
      pari_printf("m␣=␣%Ps␣\n", m);
      pari_printf("n␣=␣%Ps␣\n", n);
    }
    av = avma; // Note the used memory before garbage happens during
        calculations

    if (methods[0] == 1)
    {
      ReturnVal = PariMethod(m,s,n,printInfoVerbose);
    }
    if (methods[1] == 1)
    {
      ReturnVal = BPMethod(m,s,n,printInfoVerbose);
    }
    if (methods[2] == 1)
    {
      ReturnVal = SPSMethod(n,printInfoVerbose);
    }

    if (writeInfo)
    {
      fprintf(fpt,"%f␣%f\n",gtodouble(n),gtodouble((GEN) ReturnVal[1]));
      fprintf(fpt2,"%f\n",gtodouble((GEN) ReturnVal[4]));
      fprintf(fpt3,"%f\n",gtodouble((GEN) ReturnVal[1]));
      fprintf(fpt4,"%f\n",gtodouble((GEN) ReturnVal[3]));
      fprintf(fpt5,"%f␣%f\n",gtodouble(n),gtodouble((GEN) ReturnVal[3]));
      fprintf(fpt6,"%f␣%f\n",gtodouble((GEN) ReturnVal[4]),gtodouble((GEN)
          ReturnVal[1]));
    }
    avma = av;// revert to prev memory after data has been written
  }
```

```
  }

  if (writeInfo)
  {
    fclose(fpt);
    fclose(fpt2);
    fclose(fpt3);
    fclose(fpt4);
    fclose(fpt5);
    fclose(fpt6);

  }
}

int main()
{
  //set initial memory slot size to be  used.
  //pari_init(10000000,2);
  pari_init(6e9,2);
  //
  findHeights();

  pari_close();
  return 0;
}
```