1-1-2007

On the coefficients of ternary cyclotomic polynomials

Thomas Joseph Flanagan
University of Nevada, Las Vegas

NOTE TO USERS

ON THE COEFFICIENTS OF TERNARY CYCLOTOMIIC POLYNOMIALS

by

Thomas Joseph Flanagan

Bachelor of Science
State University of New York, Stony Brook
2001

A thesis submitted in partial fulfillment
of the requirements for the

Master of Sciences Degree in Mathematical Sciences
Department of Mathematical Sciences
College of Sciences

Graduate College
University of Nevada, Las Vegas
May 2007

UNLV

Thesis Approval

The Graduate College
University of Nevada, Las Vegas

November 17, 2006

The Thesis prepared by

Thomas J Flanagan

Entitled

On the Coefficients of Ternary Cyclotomic Polynomials

is approved in partial fulfillment of the requirements for the degree of

Master of Science in Mathematical Sciences

Examination Committee Chair

Dean of the Graduate College

Examination Committee Member

Examination Committee Member

Graduate College Faculty Representative

ASTRACT

On the Coefficients of Ternary Cyclotomic Polynomials

by

Thomas Joseph Flanagan

Dr. Grennady Bachmann, Examination Committee Chair
Professor of Mathematics
University of Nevada, Las Vegas

In this paper we investigate the coefficients of ternary cyclotomic polynomials. That is, we investigate the coefficients polynomials given by, $\Phi_n(z) = \prod_{\substack{1\le k\le n \\ (n,k)=1}} \left(z - e^{2\pi ik/n}\right)$, where n is the product of three distinct odd primes ($n = pqr$).

First we show the coefficients of $\Phi_{pqr}(z)$ are loosely connected to the residue of r modulo pq. In particular we show that if $r_1 \equiv r_2 \bmod pq$ and $r_1 < r_2$, then the set of coefficients of $\Phi_{pqr_1}(z)$ is a subset of the set of coefficients of $\Phi_{pqr_2}(z)$; if in addition, $pq < r_1$, we show these two sets are identical.

Second we establish a new upperbound for the absolute value of the coefficients of ternary cyclotomic polynomials. To illustrate the result let $c \equiv r \bmod pq$, and write $\Phi_{pqr}(z) = \sum_{k=0}^{\varphi(pqr)} a_k(pqr) z^k$. We show that $\max_{0\le k\le\varphi(pqr)} |a_k(pqr)| \le 2c+2$.

In our third result we extend the family of flat ternary cyclotomic polynomials that was established by Bachman. (Note. Flat polynomials are polynomials with coefficients of only ± 1 or 0.) We show that if $r \equiv \pm 1 \mod pq$ and $q \equiv \pm 1 \mod p$, then $\Phi_{pqr}(z)$ is flat.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

For every $n \in \mathbb{N}$ the n-th cyclotomic polynomial is given by,

$$\Phi_n(z) = \prod_{\substack{1 \le k \le n \\ (n,k)=1}} \left(z - e^{2\pi i k/n} \right).$$

The study of cyclotomic polynomials forms a significant branch of mathematics. Cyclotomic polynomials have been extensively studied over the centuries by many prominent mathematicians. If fact, Gauss was the first to show they are irreducible over the integers.

Below we compute $\Phi_n(z)$ for $n = 1, 2, 3, \text{and } 8$,

$$\Phi_1(z) = \prod_{\substack{1 \le k \le 1 \\ (1,k)=1}} \left(z - e^{2\pi i k/1} \right) = z - e^{2\pi i} = z - 1,$$

$$\Phi_2(z) = \prod_{\substack{1 \le k \le 2 \\ (2,k)=1}} \left(z - e^{2\pi i k/2} \right) = z - e^{\pi i} = z + 1,$$

$$\Phi_3(z)=\prod_{\substack{1\le k\le 3\\(3,k)=1}}\left(z-e^{2\pi ik/3}\right)=\prod_{k=1,2}\left(z-e^{2\pi ik/3}\right)=\left(z-e^{2\pi i/3}\right)\left(z-e^{4\pi i/3}\right)=z^2+z+1,$$

$$\Phi_8(z)=\prod_{\substack{1\le k\le 8\\(8,k)=1}}\left(z-e^{2\pi ik/8}\right)=\prod_{k=1,3,5,7}\left(z-e^{\pi ik/4}\right)=z^4+1.$$

The first thing we notice about the coefficients of these four cyclotomic polynomials is that in each case all of the coefficients are integers. This may be surprising considering $\Phi_n(z)$ is defined in terms of complex numbers. Nonetheless, one might speculate whether this is the case for all cyclotomic polynomials. In fact, this turns out to be true. That is, for every $n\in\mathbb{N}$, $\Phi_n(z)$ has integral coefficients. This interesting result can be shown to follow from the equation, $z^n-1=\prod_{d|n}\Phi_d(z)$ (see lemma 2.1), and induction on n.

The next observation one could make concerning the four above cyclotomic polynomials is that each has coefficients of only ±1 or 0. Thus again one might speculate that this is the case for all cyclotomic polynomials. Actually, the study of the coefficients of cyclotomic polynomials began with this conjecture [1]. We call such polynomials *flat*. That is, a polynomial is called *flat* if it has coefficients of only ±1 or 0. However, this conjecture turns out to be false. In fact, $\Phi_{105}(z)$ is the first cyclotomic polynomial which is not flat [5]. An actual computation shows that the coefficient of z^7 in $\Phi_{pqr}(z)$ is -2. We provide an explanation for this curious fact below.

The following well known result, which we prove in Lemma 2.2, shows that $\Phi_p(z)$, where p is a prime, is flat:

(1.1) $$\Phi_p(z) = 1 + z + z^2 + \ldots + z^{p-1}.$$

It is also a well known result (this can be found in [5]) that for p a prime,

(1.2) $$\Phi_{p^2}(z) = \Phi_p(z^p).$$

Therefore one can combine (1.1) and (1.2) to establish that for $n = p^2$, p a prime, $\Phi_{p^2}(z)$ is flat. In fact (1.1) and (1.2) give:

(1.3) $$\Phi_{p^2}(z) = \Phi_p(z^p) = 1 + z^p + z^{2p} + \ldots + z^{p^2-1} + z^{p^2}.$$

The next case to consider, when n is the product of two distinct primes, was tackled by Migotti. In 1883 he proved that $\Phi_{pq}(z)$ is flat for p and q prime [5].

Next we turn to integers which are the product of three primes, that is, $n \in \mathbb{N}$ such that $n = pqr$, with p, q, and r primes. Below is another well known formula, which can be found in [5].

(1.4) $$\Phi_{p^3}(z) = \Phi_{p^2}(z^p)$$

One may combine (1.3) and (1.4) to show that $\Phi_{p^3}(z)$ is flat:

(1.5) $$\Phi_{p^3}(z) = \Phi_{p^2}(z^p) = 1 + z^{p^2} + z^{2p^2} + \ldots + z^{p^3-p} + z^{p^3}.$$

Consider the below known formula, which can be found in [5]:

(1.6) $$\Phi_{p^2q}(z) = \Phi_{pq}(z^p)$$

It is clear that (1.6) and Migotti's result combine to show that $\Phi_{p^2q}(z)$ is flat.

Furthermore it is clear that one may combine the below known formula (which can be found in [5]), (1.7), with Migotti's result to show that $\Phi_{2pq}(z)$ is also flat (for $p,q \neq 2$).

(1.7) $$\Phi_{2pq}(z) = \Phi_{pq}(-z).$$

Thus we have shown that $\Phi_n(z)$ is flat for $n \in \mathbb{N}$ where n is of the form, p, p^2, p^3, pq, p^2q, $2pq$. Hence we have show that $\Phi_n(z)$ is flat for all $n < 105$. Note this is because 105 is the smallest natural number which does not have one of the above six forms; it is the smallest natural number which is the product of three distinct odd primes ($105 = 3 \cdot 5 \cdot 7$) Hence we see now that $\Phi_n(z)$ is flat for $n < 105$.

Nonetheless, this does not answer every question one might ask concerning flat cyclotomic polynomials. To illustrate a few examples, let p_1, p_2, p_3,..., p_i be distinct odd primes. First, while it is not true that every cyclotomic polynomial of the form $\Phi_{p_1p_2p_3}$ (z) is flat ($\Phi_{3\cdot5\cdot7}(z)$ being an example), one might ask whether there exist infinite families of flat cyclotomic polynomials of the form $\Phi_{p_1p_2p_3}(z)$. Secondly, one might further ask whether for every $i \in \mathbb{N}$ there exist infinite families of flat cyclotomic polynomials of the form $\Phi_{p_1p_2\cdots p_i}(z)$. While the latter question remains open, the former

question has recently been answered by Bachman [1]. He proved the following theorem which can be found in [1].

Theorem. Let $p, q,$ and r be primes with $5 < p < q < r$. If $r \equiv 1 \bmod pq$ and $q \equiv -1 \bmod p$, then $\Phi_{pqr}(z)$ is flat.

One of the main aims of this thesis is to generalize this theorem. In Chapter 5 we will prove the following theorem, which we call Theorem 3,

Theorem 3. Let $p, q,$ and r be primes with $5 < p < q < r$. If $r \equiv \pm 1 \bmod pq$ and $q \equiv \pm 1 \bmod p$, then $\Phi_{pqr}(z)$ is flat.

Another direction the study of cyclotomic polynomials has taken is an investigation into questions concerning possible bounds for their coefficients. To illustrate a few know results, let $\varphi(n)$ be the Euler totient function. We can then write,

$$\Phi_n(z) = \sum_{k=0}^{\varphi(n)} a_k(n) z^k, \tag{1.8}$$

and define,

$$A(n) = \max_{0 \le k \le \varphi(n)} |a_k(n)|. \tag{1.9}$$

$$A(n) = \max_{0 \le k \le \varphi(n)} |a_k(n)|.$$

It is natural to ask whether the coefficients of cyclotomic polynomials can be arbitrarily large or small. It was Schur who first answered this question by proving that $A(n)$ is unbounded [1]. That is, Schur proved that for every $m \in \mathbb{N}$ there exists some $n \in \mathbb{N}$ such that $\Phi_n(z)$ has a coefficient larger in absolute value than m.

For $n \in \mathbb{N}$ let $d(n)$ denote the number of divisors of n. P.T. Batman has established the following upperbound for $A(n)$, which holds for arbitrary $n \in \mathbb{N}$,

$$A(n) < \exp\left(\frac{1}{2} d(n) \log n\right). \tag{1.10}$$

R.C. Vaughan has established that this is the best possible upperbound for $A(n)$ for arbitrary $n \in \mathbb{N}$. These two results can be found in [4].

In this thesis we investigate bounds for $A(n)$ for $n \in \mathbb{N}$ where n is the product of three distinct odd primes. That is, we assume $n = pqr$, $2 < p < q < r$, with p, q, r prime. In this case $\Phi_{pqr}(z)$ is called a ternary cyclotomic polynomial. Coefficients of ternary cyclotomic polynomials have been studied by several authors. A classic result of A.S. Bang gives the bound [1],

$$A(pqr) \leq p - 1. \tag{1.11}$$

We note that this upperbound is independent of q and r. Perhaps the most interesting open problem concerning the coefficients of ternary cyclotomic polynomials is the following conjecture, due to M. Beiter [2].

Conjecture. We have,

$$A(pqr) \leq \frac{p+1}{2}. \tag{1.12}$$

H. Moller has shown that, if true, (1.12) is the best possible upperbound for $A(pqr)$ [2]. He gave a construction for a ternary cyclotomic polynomial, $\Phi_{pqr}(z)$, for every p, with a prescribed coefficient equal to $\frac{p+1}{2}$ [2]. The closest result to (1.12) is due to Bachman [2],

$$A(pqr) \leq p - \left\lceil \frac{p}{4} \right\rceil. \tag{1.13}$$

Note that we use $\lceil x \rceil$ denote the ceiling function of x.

One of the main aims of this thesis is to establish a new sort of upperbound for $A(pqr)$. We will show that not only are the coefficients of the ternary cyclotomic polynomials, $\Phi_{pqr}(z)$, bounded above by a function which is independent of q and r, but that they are also bounded above by a function which is only dependent on the residue of $r \bmod pq$. To illustrate, let $c \equiv r \bmod pq$. In Chapter 4 we will prove the following theorem, which we call Theorem 2,

Theorem 2. We have,

$$A(pqr) \leq 2c + 2, \tag{1.14}$$

where $c \equiv r \mod pq$. In particular, if $r \equiv 1 \mod pq$, then $A(pqr) \leq 4$.

We remark that given c and any pair of primes p and q, the existence of infinitely many primes r satisfying $r \equiv c \mod pq$ is guaranteed by Dirichlet's theorem on primes in arithmetic progressions [6].

Another aim of this thesis is to show that the dependence of the coefficients of $\Phi_{pqr}(z)$ is loosely restricted to the residue of $r \bmod pq$. To illustrate this result we denote the set of coefficients of $\Phi_{pqr}(z)$ by Ω_{pqr}. We will prove the following theorem, which we call Theorem 1, in Chapter 1,

Theorem 1. If $r_1 \equiv r_2 \bmod pq$ and $r_1 < r_2$, then $\Omega_{pqr_1} \subseteq \Omega_{pqr_2}$. Moreover, if $pq < r_1$ then $\Omega_{pqr_1} = \Omega_{pqr_2}$.

CHAPTER 2

REVIEW OF RELATED LITERATURE

Fix primes $2 < p < q < r$ and let k be a nonnegative integer. Define x_k, y_k, and z_k by:

$$k \equiv x_k qr \mod p, \tag{2.1}$$

$$k \equiv y_k pr \mod q, \tag{2.2}$$

$$k \equiv z_k pq \mod r, \tag{2.3}$$

where $0 \le x_k < p$, $0 \le y_k < q$, and $0 \le z_k < r$. For example, let $p = 5$, $q = 7$, $r = 11$, and $k = 100$. Then we have,

$$100 \equiv x_{100} 77 \mod 5,$$

$$100 \equiv y_{100} 55 \mod 7,$$

$$100 \equiv z_{100} 35 \mod 11,$$

and therefore, $x_{100} = 0$, $y_{100} = 5$, and $z_{100} = 6$.

Next define a function, χ, on the nonnegative integers by,

$$\chi(k) = \begin{cases} 1 & \text{if} \quad \frac{x_k}{p} + \frac{y_k}{q} \le \frac{k}{pqr} \\ 0 & \text{otherwise} \end{cases}. \tag{2.4}$$

For example, again let $p = 5$, $q = 7$, $r = 11$, and $k = 100$. Then we have,

$$\frac{x_k}{p} + \frac{y_k}{q} = \frac{5}{7} > \frac{100}{385} = \frac{k}{pqr},$$

and therefore, $\chi(100) = 0$.

Recall by (1.8) that we denote the pqr-th cyclotomic polynomial by,

$$\Phi_{pqr}(z) = \sum_{k=0}^{\varphi(pqr)} a_k(pqr) z^k.$$

We claim that the following formula gives the coefficients of $\Phi_{pqr}(z)$:

$$a_k(pqr) = \sum_{k-p<m\le k} \chi(m) - \chi(m-q) - \chi(m-r) + \chi(m-q-r). \tag{2.5}$$

We note that this formula can be found in [1]. We establish this claim through eight lemmas.

Lemma 2.1 For $n \in \mathbb{N}$, we have $z^n - 1 = \prod_{d|n} \Phi_d(z)$.

Proof. Let $f(z) = z^n - 1$ and $g(z) = \prod_{d|n} \Phi_d(z)$. We establish this lemma by showing $f(z)$ and $g(z)$ have the same zeros, all with multiplicity one. Assume $f(w) = 0$. Then since $z^n - 1 = \prod_{0 \le l \le n-1} \left(z - e^{2\pi il/n}\right)$, we have $w = e^{2\pi ik/n}$ for some $k \in \{0,1,2,...,n-1\}$. Now if $\gcd(n,k) = t$, then $n = dt$ and $k = k't$ for some $d, k' \in \mathbb{N}$, where $\gcd(d,k') = 1$. Therefore, $w = e^{2\pi ik/n} = e^{2\pi ik'/d}$. Since $\gcd(d,k') = 1$, we have $\Phi_d(w) = 0$ and thus $g(w) = 0$. Now assume $g(w) = 0$. Then $w = e^{2\pi ik/d}$ where $k \in \{0,1,2,...,d-1\}$, $\gcd(d,k) = 1$, and $n = dt$, for some $t \in \mathbb{N}$. Thus we have, $w = e^{2\pi ik/d} = e^{2\pi ikt/n}$. Since $k < d$, we have $kt < dt = n$ and therefore $kt \in \{0,1,2,...,n-1\}$. Hence $f(w) = 0$.

It is clear that all the zeros of $f(z)$ have multiplicity one. Let $d_1 | n$ and $d_2 | n$ where $d_1 \neq d_2$. To show that all the zeros of $g(z)$ have multiplicity one, it suffices to show we can not have $\Phi_{d_1}(w) = 0$ and $\Phi_{d_2}(w) = 0$ with $d_1 \neq d_2$. Thus assume $\Phi_{d_1}(w) = 0$, $\Phi_{d_2}(w) = 0$, and $d_1 \neq d_2$. Then as above $w = e^{2\pi ik_1 d_1'/d_1 d_1'} = e^{2\pi ik_1 d_1'/n}$ where $\gcd(d_1, k_1) = 1$, and $n = d_1 d_1'$. We also have $w = e^{2\pi ik_2 d_2'/d_2 d_2'} = e^{2\pi ik_2 d_2'/n}$ where $\gcd(d_2, k_2) = 1$, and $n = d_2 d_2'$. This implies $k_1 d_1' = k_2 d_2'$, which gives $k_1 d_2 = k_2 d_1$.

Since $\gcd(d_1, k_1) = 1$, we have $k_1 | k_2$. Likewise since $\gcd(d_2, k_2) = 1$, we have $k_2 | k_1$. Therefore $k_1 = k_2$ and hence $d_1 = d_2$. This is a contradiction.

Lemma 2.2 For p a prime, we have $\Phi_p(z) = \dfrac{z^p - 1}{z - 1}$.

Proof. Applying Lemma 2.1 with $n = p$ gives $z^p - 1 = \Phi_1(z)\Phi_p(z) = (z-1)\Phi_p(z)$, and the result follows.

Lemma 2.3 For p, q prime, we have $\Phi_{pq}(z) = \dfrac{(z^{pq} - 1)(z - 1)}{(z^p - 1)(z^q - 1)}$.

Proof. Applying Lemma 2.1 with $n = pq$ gives:

$$z^{pq} - 1 = \Phi_1(z)\Phi_p(z)\Phi_q(z)\Phi_{pq}(z) = \frac{(z^p - 1)(z^q - 1)\Phi_{pq}(z)}{z - 1},$$

and the result follows.

Lemma 2.4 For p, q, r prime, we have $\Phi_{pqr}(z) = \dfrac{(z^{pqr} - 1)(z^r - 1)(z^q - 1)(z^p - 1)}{(z^{pq} - 1)(z^{pr} - 1)(z^{qr} - 1)(z - 1)}$.

Proof. Applying Lemma 2.1 with $n = pqr$ gives:

$$z^{pqr} - 1 = \Phi_1(z)\Phi_p(z)\Phi_q(z)\Phi_{pq}(z)\Phi_{pr}(z)\Phi_{qr}(z)\Phi_{pqr}(z)$$

$$= \frac{(z^{pq}-1)(z^{pr}-1)(z^{qr}-1)\Phi_{pqr}(z)}{(z^{p}-1)(z^{q}-1)(z^{r}-1)},$$

and the result follows.

Lemma 2.5 For p, q, r prime, we have:

$$\Phi_{pqr}(z) \equiv (1-z^{q}-z^{r}+z^{q+r})\sum_{l=0}^{p-1} z^{l}\sum_{i=0}^{p-1} z^{iqr}\sum_{j=0}^{q-1} z^{jpr}\sum_{k=0}^{r-1} z^{kpq} \mod z^{\varphi(pqr)+1}$$

Proof. For $|z|<1$ we have:

$$\Phi_{pqr}(z) = \frac{(1-z^{pqr})(1-z^{r})(1-z^{q})(1-z^{p})}{(1-z^{pq})(1-z^{pr})(1-z^{qr})(1-z)}$$

$$= (1-z^{pqr})(1-z^{r})(1-z^{q})\frac{(1-z^{p})}{(1-z)}\sum_{i=0}^{\infty} z^{iqr}\sum_{j=0}^{\infty} z^{jpr}\sum_{k=0}^{\infty} z^{kpq}$$

$$= (1-z^{pqr})(1-z^{r})(1-z^{q})\sum_{l=0}^{p-1} z^{l}\sum_{i=0}^{\infty} z^{iqr}\sum_{j=0}^{\infty} z^{jpr}\sum_{k=0}^{\infty} z^{kpq}.$$

Truncating terms with degree larger than $\varphi(pqr)$ gives for $|z|<1$:

$$\Phi_{pqr}(z) \equiv (1-z^{q}-z^{r}+z^{q+r})\sum_{l=0}^{p-1} z^{l}\sum_{i=0}^{p-1} z^{iqr}\sum_{j=0}^{q-1} z^{jpr}\sum_{k=0}^{r-1} z^{kpq} \mod z^{\varphi(pqr)+1}.$$

Lemma 2.6 Every natural number has a unique representation of the form:

$$n = x_n qr + y_n pr + z_n pq - \delta_n pqr,$$

where $0 \le x_n < p$, $0 \le y_n < q$, $0 \le z_n < r$, $\delta_n \in \mathbb{Z}$. Moreover, if $0 \le n \le \varphi(pqr)$, then $\delta_n \in \{0,1,2\}$. Furthermore these values of x_n, y_n, and z_n coincide with the values given by (2.1) – (2.3).

Proof. First we establish existence. Since $\gcd(qr, pr, pq) = 1$, there exists $x, y, z \in \mathbb{Z}$ such that $n = xqr + ypr + zpq$. If $x \notin [0, p)$, then there exists $\omega \in \mathbb{Z}$ such that $(\omega p + x) \in [0, p)$. We then have $n = (x + \omega p)qr + ypr + zpq - \omega pqr$. Likewise there exists $\omega', \omega'' \in \mathbb{Z}$ such that $(\omega' q + y) \in [0, q)$, and $(\omega'' r + z) \in [0, r)$. Now we have, $n = (x + \omega p)qr + (y + \omega' q)pr + (z + \omega'' r)pq - (\omega + \omega' + \omega'')pqr$. Existence then follows with $x_n = \omega p + x$, $y_n = \omega' q + y$, $z_n = \omega'' r + z$, $\delta_n = \omega + \omega' + \omega''$. To establish uniqueness, assume there also exist x_n', y_n', z_n', δ_n', such that $n = x_n' qr + y_n' pr + z_n' pq - \delta_n' pqr$. Then, $x_n qr \equiv x_n' qr \mod p$ which implies $x_n \equiv x_n' \mod p$. Since $x_n, x_n' \in [0, p)$ we have $x_n = x_n'$. Likewise $y_n = y_n'$ and $z_n = z_n'$.

Now let $0 \le n \le \varphi(pqr) = (p-1)(q-1)(r-1)$. First assume $\delta_n < 0$. Then,

$$n = x_n qr + y_n pr + z_n pq + \delta_n pqr \ge x_n qr + y_n pr + z_n pq + pqr \ge pqr$$

$$> (p-1)(q-1)(r-1).$$

This is a contradiction. Hence we must have $\delta_n \geq 0$. Second assume $\delta_n > 2$. Then,

$$n = x_n qr + y_n pr + z_n pq - \delta_n pqr \leq x_n qr + y_n pr + z_n pq - 3pqr$$

$$\leq (p-1)qr + (q-1)pr + (r-1)pq - 3pqr = -qr - pr - pq < 0.$$

This is a contradiction. Hence we must have $\delta_n \leq 2$.

The last part of the lemma is established by noting that $n \equiv x_n qr \mod p$ and $0 \leq x_n < p$. Likewise for y_n and z_n.

Lemma 2.7 For $0 \leq n \leq \varphi(pqr)$, we have $\chi(n) = 1$ if and only if $\delta_n = 0$.

Proof. Assume $\chi(n) = 1$. Then, $\frac{x_n}{p} + \frac{y_n}{q} \leq \frac{n}{pqr}$. This gives $x_n qr + y_n qr \leq n$, or $0 \leq z_n pq - \delta_n pqr$, which implies $\delta_n r \leq z_n$. Since $\delta_n \in \{0,1,2\}$ and $0 \leq z_n < r$, we must have $\delta_n = 0$.

Now assume $\delta_n = 0$. Then $n = x_n qr + y_n pr + z_n pq$. This implies, $\frac{x_n}{p} + \frac{y_n}{q} + \frac{z_n}{r} = \frac{n}{pqr}$, from which $\frac{x_n}{p} + \frac{y_n}{q} \leq \frac{n}{pqr}$ follows. Hence $\chi(n) = 1$.

Lemma 2.8 For p, q, r prime, we have

$$a_k(pqr) = \sum_{k-p<m\leq k} \chi(m) - \chi(m-q) - \chi(m-r) + \chi(m-q-r).$$

Proof. By lemma 2.6 we have

$$\Phi_{pqr}(z) \equiv (1 - z^q - z^r + z^{q+r}) \sum_{l=0}^{p-1} z^l \sum_{i=0}^{p-1} z^{iqr} \sum_{j=0}^{q-1} z^{jpr} \sum_{k=0}^{r-1} z^{kpq} \mod z^{\varphi(pqr)+1}.$$

It follows from this that for z^m to have a nonzero coefficient in $\Phi_{pqr}(z)$, there must exist i, j, and k, with $0 \le i < p$, $0 \le j < q$, and $0 \le k < r$, such that

$$iqr + jpr + kpq = m - \gamma \text{ or}$$

$$iqr + jpr + kpq = m - q - \gamma \text{ or,}$$

$$iqr + jpr + kpq = m - r - \gamma \text{ or,}$$

$$iqr + jpr + kpq = m - q - r - \gamma,$$

for some $\gamma \in \{0,1,...,p-1\}$. That is, there we be a nonzero coefficient if $\chi(n) = 1$, $\chi(n-q) = 1$, $\chi(n-r) = 1$, or $\chi(n-q-r) = 1$ for some $n \in \{m-p+1,...,m\}$. Moreover,

$$a_{pqr}(z) = \sum_{m-p<n\le m} \chi(n) + \sum_{m-p<n\le m} \chi(n-q) + \sum_{m-p<n\le m} \chi(n-r) + \sum_{m-p<n\le m} \chi(n-q-r).$$

CHAPTER 3

THEOREM 1 AND PROOF

Fix p and q prime with $p < q$. Denote the set of coefficients of $\Phi_{pqr}(z)$ by Ω_r, with r prime and $q < r$.

Theorem 1. If $r_1 \equiv r_2 \mod pq$ and $r_1 < r_2$, then $\Omega_{r_1} \subseteq \Omega_{r_2}$. Moreover, if $pq < r_1$, then $\Omega_{r_1} = \Omega_{r_2}$.

Proof. Let $\Phi_{pqr_1}(z) = \sum_{m=0}^{\phi(pqr_1)} a_m z^m$ and $\Phi_{pqr_2}(z) = \sum_{n=0}^{\phi(pqr_2)} b_n z^n$. Let $m = kr_1 + t$, where $k \in \mathbb{Z}$ and $0 \le t < r_1$. We intend to show that if we choose $n = kr_2 + t$, we will have $a_m = b_n$. By (2.5) we have,

$$a_m = \sum_{m-p<x\le m} \chi_1(x) - \chi_1(x-q) - \chi_1(x-r_1) + \chi_1(x-r_1-q)$$

$$\text{where, } \chi_1(m) = \begin{cases} 1 & \text{if } \dfrac{x_m}{p} + \dfrac{y_m}{q} \le \dfrac{m}{pqr_1} \\ 0 & \text{otherwise.} \end{cases}$$

By (2.5) we also have:

$$b_n = \sum_{n-p<x\le n} \chi_2(x) - \chi_2(x-q) - \chi_2(x-r_2) - \chi_2(x-q-r_2)$$

where,

$$\chi_2(n) = \begin{cases} 1 & \text{if} \quad \frac{x_n}{p} + \frac{y_n}{q} \le \frac{n}{pqr_2} \\ 0 & \text{otherwise} \end{cases}$$

For our choices of m and n, we claim $x_m = x_n$ and $y_m = y_n$. First we have, $kr_1 + t \equiv m \equiv x_m q r_1 \pmod{p}$. Now since $r_2 = dpq + r_1$ for some $d \in \mathbb{N}$, we have:

$$kr_2 + t \equiv n \equiv x_n q r_2 \equiv k(dpq + r_1) + t \equiv kr_1 + t \equiv m \equiv x_m q r_1 \pmod{p}.$$

Thus, $x_n q r_1 \equiv x_m q r_1 \mod p$. Hence we have $x_n = x_m$. In exactly the same manner we can conclude $y_n = y_m$.

If $t = 0$ we have, $\frac{m}{pqr_1} = \frac{kr_1}{pqr_1} = \frac{k}{pq} = \frac{kr_2}{pqr_2} = \frac{n}{pqr_2}$

Hence in this case $\chi_1(m) = \chi_2(n)$.

Assume $t > 0$. We claim $\chi_2(n) = 1 \Rightarrow \chi_1(m) = 1$. To establish this claim, assume $\chi_2(n) = 1$. We then have:

$$\frac{x_m}{p}+\frac{y_m}{q}=\frac{x_n}{p}+\frac{y_n}{q}\le\frac{n}{pqr_2}=\frac{kr_2+t}{pqr_2}=\frac{k}{pq}+\frac{t}{pqr_2}=\frac{kr_1}{pqr_1}+\frac{t}{pqr_2}\le\frac{kr_1}{pqr_1}+\frac{t}{pqr_1}=\frac{m}{pqr_1},$$

which implies $\chi_1(m)=1$.

We claim it is impossible to have both $\chi_2(n)=0$ and $\chi_1(m)=1$. To establish this claim assume both $\chi_2(n)=0$ and $\chi_1(m)=1$. Then,

$$\frac{k}{pq}+\frac{t}{pqr_2}=\frac{n}{pqr_2}<\frac{x_n}{p}+\frac{y_n}{q}=\frac{x_m}{p}+\frac{y_m}{q}\le\frac{m}{pqr_1}=\frac{k}{pq}+\frac{t}{pqr_1}.$$

Multiplying through by pq and then subtracting through by k gives,

$$\frac{t}{r_2}<x_m q+y_m p-k<\frac{t}{r_1}.$$

However this is impossible because $x_m q+y_m p-k\in\mathbb{Z}$, $0<\frac{t}{r_2}$, and $\frac{t}{r_1}<1$. If follows that $\chi(m)=\chi(n)$.

We next claim that for our choices of m and n we have $\chi_1(m-x)=\chi_2(n-x)$, when $x\in[0,p)$ Recall we have let $m=kr_1+t$ where $0\le t<r_1$, we have chosen $n=kr_2+t$. Thus for any given $x\in[0,p)$ we have $m-x=kr_1+t-x$ and $n-x=kr_2+t-x$, where $|t-x|<r_1$.

If $0 \le t-x$, then we may apply the same argument as above to conclude $\chi_1(m-x) = \chi_2(n-x)$. The only difference is we must replace t by $t-x$.

If $t-x<0$, we claim $\chi_1(m-x)=1 \Rightarrow \chi_2(n-x)=1$. To establish this claim assume $\chi_1(m-x)=1$. We then have:

$$\frac{x_{n-x}}{p}+\frac{y_{n-x}}{q}=\frac{x_{m-x}}{p}+\frac{y_{m-x}}{q}\le\frac{m-x}{pqr_1}=\frac{kr_1+t-x}{pqr_1}=\frac{k}{pq}+\frac{t-x}{pqr_1}=\frac{kr_2}{pqr_2}+\frac{t-x}{pqr_1}\le\frac{kr_2}{pqr_2}+\frac{t-x}{pqr_2}=\frac{n-x}{pqr_2},$$

which implies $\chi_2(n-x)=1$.

We claim it is impossible to have both $\chi_1(m-x)=0$ and $\chi_2(n-x)=1$. To establish this claim assume both $\chi_1(m-x)=0$ and $\chi_2(n-x)=1$. Then,

$$\frac{k}{pq}+\frac{t-x}{pqr_1}=\frac{m-x}{pqr_1}<\frac{x_{m-x}}{p}+\frac{y_{m-x}}{q}=\frac{x_{n-x}}{p}+\frac{y_{n-x}}{q}\le\frac{n-x}{pqr_2}=\frac{k}{pq}+\frac{t-x}{pqr_2}.$$

Multiplying through by pq and then subtracting through by k gives:

$$\frac{t-x}{r_1}<x_{m-x}q+y_{m-x}p-k<\frac{t-x}{r_2}.$$

However this is impossible because $x_m q+y_m p-k\in\mathbb{Z}$, $-1<\frac{t-x}{r_1}$, and $\frac{t}{r_1}<0$.

Thus we have $\chi_1(m-x)=\chi_2(n-x)$, and therefore $\sum_{m-p<x\le m}\chi_1(x)=\sum_{n-p<x\le n}\chi_2(x)$.

Similarly we can conclude,

$$\sum_{m-p<x\le m}\chi_1(x-q)=\sum_{n-p<x\le n}\chi_2(x-q),$$

$$\sum_{m-p<x\le m}\chi_1(x-r_1)=\sum_{n-p<x\le n}\chi_2(x-r_2),$$

$$\sum_{m-p<x\le m}\chi_1(x-q-r_2)=\sum_{n-p<x\le n}\chi_2(x-q-r_2).$$

Hence $a_m=b_n$. This establishes $\Omega_{r_1}\subseteq\Omega_{r_2}$.

Now assume $pq<r_1$. Let $n=kr_2+t$, where $0\le t<r_2$. If $t<r_1$, we may let $m=kr_1+t$ and have $a_m=b_n$. (This is what we have established above.) If $t\ge r_1$, we let $n_0=kr_2+t_0$, where $t=\omega pq+t_0$ and $0\le t_0<pq$. We want to show $b_n=b_{n_0}$. We have $x_n=x_{n_0}$ and $y_n=y_{n_0}$. Since $n_0\le n$, we have $\chi_2(n_0)=1\Rightarrow\chi_2(n)=1$ and $\chi_2(n)=0\Rightarrow\chi_2(n_0)=0$. We claim it is impossible to have both $\chi_2(n)=1$ and $\chi_2(n_0)=0$. Assume $\chi_2(n)=1$ and $\chi_2(n_0)=0$. Then,

$$\frac{k}{pq}+\frac{t_0}{pqr_2}=\frac{n_0}{pqr}<\frac{x_n}{p}+\frac{y_n}{q}\le\frac{n}{pqr}=\frac{k}{pq}+\frac{t}{pqr_2}.$$

Multiplying through by pq and then subtracting through by k gives,

$$\frac{t_0}{r_2} < x_n q + y_n p - k \leq \frac{t}{r_2}.$$

However this is impossible because, $x_n q + y_n p - k \in \mathbb{Z}$, $0 < \frac{t_0}{r_2}$, and $\frac{t}{r_2} < 1$. Thus we have $\chi_2(n) = \chi_2(n_0)$. Now we may show $\chi_2(n_0 - x) = \chi_2(n - x)$ in exactly the same manner as above. Thus we may conclude $b_n = b_{n_0}$. Now since $r_1 > pq > t_0$, we may let $m = kr_1 + t_0$ and have $b_n = b_{n_0} = a_m$.

CHAPTER 4

THEOREM 2 AND PROOF

Theorem 2. $A(pqr) \leq 2c+2$, where $r \equiv c \mod pq$. In particular, if $r \equiv 1 \mod pq$ we have $A(pqr) \leq 4$.

Proof. Let $r = \lambda pq + c$, where $\lambda \in \mathbb{Z}$ and $0 \leq c < r$. Let $n = \omega r + t$, where $\omega \in \mathbb{Z}$ and $0 \leq t < r$. For $m \in [n-p+1, n]$, let $m = \omega_m r + t_m$, where $0 \leq t_m < r$. Note that for all $m \in [n-p+1, n]$ we must have either $\omega = \omega_m$ or $\omega - 1 = \omega_m$. We claim that if $\chi(m-r+c) = 1$, then $\chi(m) = 1$. To establish this claim assume $\chi(m-r+c) = 1$. Since $m-r+c \equiv m \mod p$, we have $x_{m-r+c} = x_m$. Likewise, since $m-r+c \equiv m \mod q$, we have $y_{m-r+c} = y_m$. This gives,

$$\frac{x_m}{p} + \frac{y_m}{q} = \frac{x_{m-r+c}}{p} + \frac{y_{m-r+c}}{q} \leq \frac{m-r+c}{pqr} \leq \frac{m}{pqr},$$

or $\chi(m) = 1$.

We next claim that there can be at most two $m \in [n-p+1, n]$ such that $\chi(m-r+c) = 0$ and $\chi(m) = 1$. To establish this claim, assume there exists $m \in [n-p+1, n]$ such that $\chi(m-r+c) = 0$ and $\chi(m) = 1$. This gives,

$$\frac{m-r+c}{pqr} < \frac{x_m}{p} + \frac{y_m}{q} \le \frac{m}{pqr},$$

or,

$$-1 + \frac{t_m + c}{r} < x_m q + y_m p - \omega_m \le \frac{t_m}{r}.$$

Since $(x_m q + y_m p - \omega_m) \in \mathbb{Z}$, $0 < \frac{t_m + c}{r}$, and $\frac{t_m}{r} < 1$, we must have $x_m q + y_m p = \omega_m$.

Now assume there exists another $\nu \in [n-p+1, n]$ with $\chi(\nu - r + c) = 0$ and $\chi(\nu) = 1$. As before we must have $x_\nu q + y_\nu p = \omega_\nu$. Without loss of generality we may assume, $\nu < m$. Then we must have either $\omega_m = \omega_\nu$ or $\omega_m - 1 = \omega_\nu$. We claim that we can not have $\omega_m = \omega_\nu$. If $\omega_m = \omega_\nu$, then $x_m q + y_m p = x_\nu q + y_\nu p$, which implies $(x_m - x_\nu)q = (y_\nu - y_m)p$. Since p and q are prime, this implies $q \mid (y_\nu - y_m)$. Since $0 \le y_\nu, y_m < q$, we must have $y_\nu = y_m$. It follows that $m \equiv \nu \mod q$. Hence $m - \nu \ge q$. This however is impossible because $m, \nu \in [n-p+1, n]$ implies $m - \nu < p < q$. Therefore we can only have $\omega_m - 1 = \omega_\nu$. If there were another $\mu \in [n-p+1, n]$ with $\chi(\mu - r + c) = 0$ and $\chi(\mu) = 1$, we must have either $\omega_m = \omega_\mu$ or $\omega_\nu = \omega_\mu$. As above, $\omega_m = \omega_\mu$ leads to the contradiction $q > p > m - \mu \ge q$. And $\omega_\nu = \omega_\mu$ leads to the contradiction $q > p > \nu - \mu \ge q$. Therefore there can be at most two numbers in the interval $[n-p+1, n]$ such that $\chi(m - r + c) = 0$ and $\chi(m) = 1$. Hence with the exception of at most two number in the interval $[n-p+1, n]$ we have $\chi(m - r + c) = \chi(m)$.

Now consider the difference of the two sums:

(4.1) $$\sum_{m-p<n\le m} \chi(n) - \sum_{m-p<n\le m} \chi(n-r).$$

In (4.1), with at most possibly two exceptions the first $p-c-1$ terms in the first sum will cancel with the last $p-c-1$ terms in the second sum. If there are one/two exceptions it/they will contribute positive one/two to (4.1). Therefore,

(4.2) $$-c \le \sum_{m-p<n\le m} \chi(n) - \sum_{m-p<n\le m} \chi(n-r) \le c+2.$$

Next consider the difference of the two sums:

(4.3) $$\sum_{m-p<n\le m} \chi(n-q-r) - \sum_{m-p<n\le m} \chi(n-q).$$

Likewise, with at most possibly two exceptions the last $p-c-1$ terms in the first sum will cancel with the first $p-c-1$ terms in the second sum. If there are one/two exceptions it/they will contribute negative one/two to (4.3). Therefore,

$$-c-2 \le \sum_{m-p<n\le m} \chi(n-q-r) - \sum_{m-p<n\le m} \chi(n-q) \le c.$$

Hence we have $A(pqr) \le 2c+2$.

CHAPTER 5

THEOREM 5 AND PROOF

Throughout this chapter we will use the notion $x \equiv_n y$ to denote $x \equiv y \bmod n$ and assume that p, q, and r are primes with $5 < p < q < r$. We will require the following 17 lemmas.

Lemma 5.1 If $m \le \frac{\varphi(pqr)}{2}$, then $\chi(m) = 0$ unless both $x_m < \frac{p}{2}$ and $y_m < \frac{q}{2}$.

Proof. Assume $m \le \frac{\varphi(pqr)}{2}$ and $x_m \ge \frac{p}{2}$. Then $\frac{x_m}{p} + \frac{y_m}{q} \ge \frac{1}{2} + \frac{y_m}{q} \ge \frac{1}{2}$. We also have $\frac{m}{pqr} \le \frac{\varphi(pqr)}{2pqr} = \frac{(p-1)(q-1)(r-1)}{2pqr} < \frac{1}{2}$. This implies $\frac{x_m}{p} + \frac{y_m}{q} > \frac{m}{pqr}$ and therefore $\chi(m) = 0$. Likewise if $y_m \ge \frac{q}{2}$ we must have $\chi(m) = 0$.

Lemma 5.2 We have $x_{n+m} \equiv_p x_n + x_m$ and $y_{n+m} \equiv_q y_n + y_m$.

Proof. By (2.1) and (2.2) we have $n \equiv_p x_n qr$ and $m \equiv_p x_m qr$. Thus we have $n + m \equiv_p x_n qr + x_m qr \equiv_p (x_n + x_m) qr$. We also have $n + m \equiv_p x_{n+m} qr$. Since $\gcd(p, qr) = 1$ we must have $x_{n+m} \equiv_p x_n + x_m$. Likewise we have $y_{n+m} \equiv_q y_n + y_m$.

Lemma 5.3 Assume $r = \kappa pq - 1$ and $q = \tau p + 1$. Then

(5.1) $x_1 = p - 1$ $y_1 = \tau$

(5.2) $x_p = 0$ $y_p = q - 1$

(5.3) $x_q = p - 1$ $y_q = 0$

(5.4) $x_r = 1$ $y_r = q - \tau$

Proof. These results follow by direct calculation. We have $1 \equiv_p x_1 qr \equiv_p -x_1$. Hence $x_1 = p - 1$. We have $1 \equiv_q y_1 pr \equiv_q -y_1 p$. This implies $\tau \equiv_q -\tau p y_1$. Since $-\tau p \equiv_q 1$, we have $y_1 = \tau$. We have $0 \equiv_p p \equiv_p x_1 qr \equiv_p -x_1$. Hence $x_p = 0$. We have $p \equiv_q y_p pr$, which implies $1 \equiv_q -y_p$. Hence $y_p = q - 1$. We have $q \equiv_p x_q qr$, which implies $1 \equiv_p x_q r \equiv_p -x_q$. Hence $x_q = p - 1$. We have $0 \equiv_q q \equiv_q y_q pr \equiv_q -y_q p$, which implies $y_q = 0$ We have $r \equiv_p x_r qr$, which implies $1 \equiv_p x_q q \equiv_p x_q$. Hence $x_r = 1$. We have $r \equiv_q y_r pr$, which implies $1 \equiv_q y_r p$. Thus we have $\tau \equiv_q y_r \tau p$. Since $\tau p \equiv_q -1$, we have $y_r = q - \tau$.

Lemma 5.4 Assume $r = \kappa pq - 1$ and $q = \tau p + 1$. If $m \le \dfrac{\varphi(pqr)}{2}$ and $\chi(m) = 1$, then:

(5.5) $\chi(m+q) = 1$ $[x_m > 0]$,

(5.6) $\chi(m+r) = 1$ $[y_m \ge \tau]$,

(5.7) $\chi(m-r) = 1$ $[x_m > 0]$.

Proof. Assume $\chi(m)=1$. By Lemma 4.1 we must have $x_m < \frac{p}{2}$ and $y_m < \frac{q}{2}$. Note that since $q=\tau p+1$, we have $\frac{1}{p}-\frac{\tau}{q}=\frac{r}{pqr}$. If $x_m > 0$, by (5.3) and Lemma 4.2 we have $x_{m+q}=x_m-1$ and $y_{m+q}=y_m$. Thus,

$$\frac{x_{m+q}}{p}+\frac{y_{m+q}}{q}=\frac{x_m}{p}+\frac{y_m}{q}-\frac{1}{p}\le\frac{m}{pqr}-\frac{1}{p}\le\frac{m+q}{pqr}.$$

Therefore $\chi(m+q)=1$. This establishes (5.5).

If $y_m \ge \tau$, by (5.4) and Lemma 5.2 we have $y_{m+r}=y_m-\tau$. Since $x_m < \frac{p}{2}$ by (5.4) and Lemma 5.2 we have $x_{m+r}=x_m+1$. Thus,

$$\frac{x_{m+r}}{p}+\frac{y_{m+r}}{q}=\frac{x_m}{p}+\frac{y_m}{q}+\frac{1}{p}-\frac{\tau}{q}\le\frac{m+r}{pqr}.$$

Therefore $\chi(m+r)=1$. This establishes (5.6).

If $x_m > 0$ by (5.4) and Lemma 5.2 we have $x_{m-r}=x_m-1$. We must have $\tau < \frac{q}{2}$ because $\tau \ge \frac{q}{2}$ implies $q=\tau p+1 \ge \frac{qp}{2}+1 > q$, which is a contradiction. Since $y_m < \frac{q}{2}$ and $\tau < \frac{q}{2}$, by Lemma 5.1 and (5.4) we have $y_{m-r}=y_m+\tau$. Therefore,

$$\frac{x_{m-r}}{p}+\frac{y_{m-r}}{q}=\frac{x_m}{p}+\frac{y_m}{q}-\frac{1}{p}+\frac{\tau}{q}\le\frac{m-r}{pqr}.$$

Therefore $\chi(m-r)=1$. This establishes (5.7).

We introduce two functions on the nonnegative integers:

(5.8) $$Q(m)=\chi(m)-\chi(m+q)-\chi(m+r)+\chi(m+q+r);$$

(5.9) $$R(m)=\chi(m)-\chi(m+q)-\chi(m-r)+\chi(m+q-r).$$

Lemma 5.5 Assume $m\le\frac{\varphi(pqr)}{2}$. Then,

(5.10) $$Q(m)\le 1 \qquad [x_m=0],$$

(5.11) $$Q(m)\le 0 \qquad [x_m>0].$$

Proof. Observe that by (5.3) and (5.4) we have $x_{m+q+r}=x_m$ and $y_{m+q+r}\equiv_q y_m-\tau$. First assume $y_m<\tau$. Then since $\tau<\frac{q}{2}$, we have $y_{m+q+r}>\frac{q}{2}$ and therefore by Lemma 5.1 $\chi(m+q+r)=0$. From this and (5.8), (5.10) follows. Now (5.11) follows from (5.5). Next assume $y_m\ge\tau$. Then by (5.6) we have $\chi(m+r)\ge\chi(m)$. Thus (5.10) follows from (5.8). If $x_m>0$ then since $x_{m+q+r}=x_m$ we have $x_{m+q+r}>0$. Therefore we can apply (5.7)

with m replaced by $m+q+r$ This gives $\chi(m+q) \geq \chi(m+q+r)$. Now (5.11) follows from (5.8).

Lemma 5.6 For $m \leq \frac{\varphi(pqr)}{2}$ satisfying $x_m > 1$ and $y_m < q-\tau$ we have:

(5.12) $$R(m) \leq 0.$$

Furthermore if $\chi(m) = 0$, we have:

(5.13) $$R(m) \leq -\chi(m-r).$$

Proof. Assume $x_m > 1$ and $y_m < q-\tau$. We claim that,

(5.14) $$\chi(m+q-r) \leq \chi(m+q).$$

To establish this, note that by Lemma 5.2, (5.3), (5.4), and by assumption on y_m, we have:

(5.15) $$y_{m+q-r} = y_m + \tau \geq \tau.$$

Now by (5.15) we may apply (5.6) with m replaced by $m+q-r$. This gives (5.14). Now (5.12) and (5.13) follow from (5.7), (5.9), and (5.14).

Lemma 5.7 $\Phi_{pqr}(z)$ is flat if $r \equiv -1 \mod pq$ and $q \equiv 1 \mod p$.

Proof. By (2.5) and (5.8), we have $a_k(pqr) = \sum_{k-p-q-r<m\le k-q-r} Q(m)$. By Lemma 5.2 and (5.1), as m runs through the interval $(k-p-q-r, k-q-r]$, x_m runs through the interval $0 \le x_m < p$. In particular, x_m takes on the value 0 exactly once. Thus by Lemma 5.5 we get the required upper bound. That is, $a_k(pqr) \le 1$.

Now we establish the lower bound. First note that by (2.5) and (5.9) we have:

(5.16) $$-a_k(pqr) = \sum_{k-p-q<m\le k-q} R(m).$$

For $i \in \{0,1\}$, let $m_i \in [k-p-q+1, k-q]$ be such that

(5.17) $$x_{m_i} = i.$$

By Lemma 5.2 and (5.1), this is well defined. By Lemma 5.2 and (5.1), there can be at most one $m \in [k-p-q+1, k-q]$ such that $y_m \ge q-\tau$. If there is such an m, let it be denoted by m'. We claim that,

(5.18) $$-a_k(pqr) \le \chi(m_0) + \chi(m_1) - \chi(m_1+q) - \chi(m_1-r) + \chi(m'+q-r).$$

To establish this, note that by Lemma 5.6 we have:

(5.19) $$-a_k(pqr) \le R(m_0) + R(m_1) + R(m' + q - r).$$

Now, since $y_{m'} \ge q - \tau > q/2$, by Lemma 4.1 we have $\chi(m') = 0$. By Lemma 5.2, (5.3), and (5.4) we have $x_{m_0+q-r} = p - 2 > p/2$ (since $p > 4$) and $x_{m_1+q-r} = p - 1 > p/2$. Thus by Lemma 5.1 we have $\chi(m_0 + q - r) = \chi(m_1 + q - r) = 0$. Now (5.18) follows from (5.9) and (5.19).

Now assume $\chi(m_1) \ge \chi(m_0)$. Then (5.5), (5.7), and (5.18) give $-a_m(pqr) \le \chi(m' + q - r)$. Therefore $-a_k(pqr) \le 1$.

Now assume $\chi(m_1) = 0$ and $\chi(m_0) = 1$. By Lemma 5.2 and (5.1), there are two possibilities: either $m_1 = m_0 - 1$ or $m_1 = m_0 - 1 + p$. First assume $m_1 = m_0 - 1$. If $y_{m_0} \ge \tau$, then by Lemma 5.2, (5.1), and (5.3) we have $x_{m_1+q} = 0$ and $y_{m_1+q} = y_{m_0-1+q} = y_{m_0} - \tau$. Thus we have:

$$\frac{x_{m_1+q}}{p} + \frac{y_{m_1+q}}{q} = \frac{y_{m_0}}{q} - \frac{\tau}{q} \le \frac{m_0}{pqr} - \frac{\tau}{q} = \frac{m_0}{pqr} - \frac{1}{p} + \frac{1}{pq} = \frac{m_0 - qr + r}{pqr} \le \frac{m_0 + q - 1}{pqr} = \frac{m_1 + q}{pqr}.$$

Hence $\chi(m_1 + q) = 1$. Thus by (5.18) we have $-a_k(pqr) \le \chi(m' + q - r) \le 1$. If $y_{m_0} < \tau$ then $y_{m_1} = q + y_{m_0} - \tau > q - \tau$. Therefore in this case we have $m_1 = m'$. So $x_{m'+q+r} = x_{m_1+q-r} = p - 1 > p/2$ and therefore by Lemma 5.1 we have $\chi(m' + q - r) = 0$. Hence have $-a_k(pqr) \le \chi(m_0) \le 1$.

Now assume $m_1 = m_0 - 1 + p$. Then we have by Lemma 5.2, (5.3), and (5.17) $x_{m_1+q} = 0$ and $y_{m_1+q} \equiv y_{m_0} - \tau - 1$. If $y_{m_0} \ge \tau + 1$ we have $y_{m_1+q} = y_{m_0} - \tau - 1$. This implies:

$$\frac{x_{m_1+q}}{p}+\frac{y_{m_1+q}}{q}=\frac{y_{m_0}}{q}-\frac{\tau}{q}-\frac{1}{q}\le\frac{m_0}{pqr}-\frac{1}{p}-\frac{1}{q}+\frac{1}{pq}=\frac{m_0+r(1-p-q)}{pqr}\le\frac{m_1+q}{pqr}.$$

Therefore we have $\chi(m_1+q)=1$ and thus by (5.18), $-a_k(pqr)\le\chi(m'+q-r)\le 1$. If $y_{m_0}<\tau+1$ then $y_{m_1}=q+y_{m_0}-\tau-1$. If $y_{m_0}>1$ then $y_{m_1}>q-\tau$ and therefore we have $m_1=m'$. Therefore in this case we have $m_1=m'$. So $x_{m'+q+r}=x_{m_1+q-r}=p-1>p/2$ and therefore by Lemma 5.1 we have $\chi(m'+q-r)=0$. Thus by (4.18), $-a_k(pqr)\le\chi(m_0)\le 1$. If $y_{m_0}\le 1$ then $y_m\le q-\tau$ for all $m\in[m_0,m_1]$. Thus m' does not exists. Hence by (4.18), $-a_k(pqr)\le\chi(m_0)\le 1$.

Thus we have shown that for every case we have, $-a_k(pqr)\le 1$. Hence we have established the lower bound.

Lemma 5.8 Assume $r=\kappa pq+1$ and $q=\tau p+1$. Then,

(5.20) $x_1=1$ $y_1=q-\tau$

(5.21) $x_p=0$ $y_p=1$

(5.22) $x_q=1$ $y_q=0$

(5.23) $x_r=1$ $y_r=q-\tau$

Proof. These results follow by direct calculations. We use (2.1) and (2.20). We have $1\equiv_p x_1qr\equiv_p x_1$, which implies $x_1=1$. We have $1\equiv_q y_1pr\equiv_q py_1$. This gives $-\tau\equiv_q-\tau py_1$. Since $-\tau p\equiv_q 1$, we have $-\tau\equiv_q y_1$, or $y_1=q-\tau$. We have

$0 \equiv_p p \equiv_p x_p qr \equiv_p x_p$. Hence $x_p = 0$. We have $p \equiv_q y_p pr$, which implies $1 \equiv_q y_p$. Hence $y_p = 1$. We have $q \equiv_p x_q qr$, which implies $1 \equiv_p x_q r \equiv_p x_q$. Hence $x_q = 1$. We have $0 \equiv_q q \equiv_q y_q pr \equiv_q y_q p$, which implies $y_q = 0$. We have $r \equiv_p x_r qr$, which gives $1 \equiv_p x_r q \equiv_p x_r$, which implies $x_r = 1$. We have $r \equiv_q y_r pr$, which implies $1 \equiv_q y_r p$. Therefore we have $-\tau \equiv_q -y_r \tau p$. Since $-\tau p \equiv_q 1$, we have $-\tau \equiv_q y_r$, and thus $y_r = q - \tau$.

Lemma 5.9 Assume $r = \kappa pq + 1$ and $q = \tau p + 1$. If $m \le \frac{\varphi(pqr)}{2}$ and $\chi(m) = 1$ then,

(5.24) $\chi(m-q) = 1$ $[x_m > 0]$,

(5.25) $\chi(m+r) = 1$ $[y_m \ge \tau]$,

(5.26) $\chi(m-r) = 1$ $[x_m > 0]$.

Proof. Assume $\chi(m) = 1$. By Lemma 4.1 we must have $x_m < \frac{p}{2}$ and $y_m < \frac{q}{2}$. Note that since $q = \tau p + 1$ we have $\frac{1}{p} - \frac{\tau}{q} = \frac{r}{pqr}$. If $x_m > 0$ by (5.22) and Lemma 5.2 we have $x_{m-q} = x_m - 1$ and $y_{m-q} = y_m$. Thus,

$$\frac{x_{n-q}}{p} + \frac{y_{n-q}}{q} = \frac{x_m}{p} + \frac{y_m}{q} - \frac{1}{p} \le \frac{m}{pqr} - \frac{1}{p} = \frac{m}{pqr} - \frac{q}{pq} \le \frac{m}{pqr} - \frac{q}{pqr}.$$

Therefore $\chi(m-q) = 1$. This establishes (5.24).

If $y_m \geq \tau$ by (5.23) and Lemma 5.2 we have $y_{m+r} = y_m - \tau$. Since $x_m < \frac{p}{2} < q-1$ by (5.23) and Lemma 4.2 we have $x_{m+r} = x_m + 1$. Thus,

$$\frac{x_{m+r}}{p} + \frac{y_{m+r}}{q} = \frac{x_m}{p} + \frac{y_m}{q} + \frac{1}{p} - \frac{\tau}{q} \leq \frac{m+r}{pqr}.$$

Therefore $\chi(m+r) = 1$. This establishes (5.25).

Assume $x_m > 0$. By (5.23) and Lemma 5.2 we have $x_{m-r} = x_m - 1$. We must have $y_{m-r} = y_m + \tau$. This is because $\tau, y_m < \frac{q}{2}$. This gives

$$\frac{x_{m-q}}{p} + \frac{y_{m-q}}{q} = \frac{x_m}{p} + \frac{y_m}{q} - \frac{1}{p} + \frac{\tau}{q} \leq \frac{m}{pqr} - \frac{r}{pqr} = \frac{m-r}{pqr}.$$

Therefore $\chi(m-r) = 1$. This establishes (5.26). This completes the proof.

We introduce two functions on the nonnegative integers,

(5.27) $$S(m) = \chi(m) - \chi(m-q) - \chi(m-r) + \chi(m-q-r);$$

(5.28) $$T(m) = \chi(m) - \chi(m-q) - \chi(m+r) + \chi(m-q+r).$$

Lemma 5.10 For $m \leq \frac{\varphi(pqr)}{2}$, we have

(5.29) $T(m) \le 1 \qquad [x_m = 0],$

(5.30) $T(m) \le 0 \qquad [x_m > 0].$

Proof. If $x_m = 0$ by Lemma 5.2, (5.22), and (5.23) we have $x_{m-q+r} = x_m$ and $y_{m-q+r} \equiv y_m - \tau$. Assume $y_m < \tau$. Then $y_{m-q+r} > \frac{q}{2}$ and therefore by Lemma 5.1, we have $\chi(m-q+r) = 0$. Now (5.29) follows immediately while (5.30) follows from (5.24). Next assume that $y_m \ge \tau$. Then (5.25) gives $\chi(m+r) \ge \chi(m)$. From this (5.29) follows. Moreover, if $x_m > 0$ then by Lemma 5.2, (5.22), and (5.23) so is x_{m-q+r}. Thus we may apply (5.26) with m replaced by $m-q+r$. This gives, $\chi(m-q) \ge \chi(m-q+r)$. Now (5.30) follows.

Lemma 5.11 For $m \le \frac{\varphi(pqr)}{2}$ satisfying $x_m > 1$ and $y_m < q - \tau$ we have,

(5.31) $S(m) \le 0.$

Furthermore if $\chi(m) = 0$ we have,

(5.32) $S(m) \le -\chi(m-r).$

Proof. Assume $x_m > 1$ and $y_m < q - \tau$. By (4.26) we have $\chi(m-r) = 1$. Hence both (5.31) and (5.32) follow from the inequality,

(5.33) $\chi(m-q) \ge \chi(m-q-r).$

To establish (5.33) note that by assumption on y_m we have $y_{m-q-r} = y_m + \tau \geq \tau$. Thus we may apply (5.25) with m replaced by $m-q-r$. This gives (5.33).

Lemma 5.12 $\Phi_{pqr}(z)$ is flat if $r \equiv 1 \mod pq$ and $q \equiv 1 \mod p$.

Proof. By (5.28) and (2.5) we have $-a_k(pqr) = \sum_{k-r-p<m\leq k-r} T(m)$. Now by Lemma 5.2 and (5.20) as m runs through the interval $[k-r-p+!, k-r]$ x_m takes on the value 0 exactly once. Thus $-a_k(pqr) \leq 1$ follows from Lemma 5.10. Now we establish the upperbound.

By (2.5) and (5.27) we have $a_k(pqr) = \sum_{k-p<m\leq k} S(m)$. For $i \in \{0,1\}$ let $m_i \in [k-p+1, k]$ be such that $x_{m_i} = i$. By Lemma 5.2 and (5.20) there can be at most one $m \in [k-p+1, k]$ such that $y_m \geq q - \tau$. If there is such an m let it be denoted by m'. We claim that

$$a_k(pqr) \leq \chi(m_0) + \chi(m_1) - \chi(m_1 - q) - \chi(m_1 - r) + \chi(m' - q - r). \tag{5.34}$$

By Lemma 5.11 we have $a_k(pqr) \leq S(m_0) + S(m_1) + S(m')$. By Lemma 5.1 we have $\chi(m') = 0$ since $y_{m'} \geq q - \tau > q/2$. Thus by Lemma 5.1 we have $\chi(m') = 0$. By Lemma 5.2, (5.22), and (5.23) we have $x_{n_0-q-r} = p-2 > p/2$ and $x_{m_1-q-r} = p-1 > p/2$. Hence by Lemma 5.1 we have $\chi(m_0 - q - r) = \chi(m_1 - q - r) = 0$. Thus (5.34) follows by (5.27).

First assume $\chi(m_1) \geq \chi(m_0)$. Then (4.24) and (4.26) give $a_k(pqr) \leq \chi(m'-q-r) \leq 1$

Alternatively assume $\chi(m_0) = 1$ and $\chi(m_1) = 0$. By Lemma 5.2 and (5.20) there are two possibilities, either $m_1 = m_0 + 1$ or $m_1 = m_0 - p + 1$. First assume $m_1 = m_0 + 1$. Then by Lemma 5.2, (5.20), and (5.22) we have $x_{m_1-q} = x_{m_0+1-q} = 0$ and $y_{m_1-q} \equiv y_{m_0+1-q} \equiv y_{m_0} - \tau$. If $y_{m_0} \geq \tau$ we have,

$$\frac{x_{m_1-q}}{p} + \frac{y_{m_1-q}}{q} = \frac{y_{m_0}}{q} - \frac{\tau}{q} \leq \frac{m_0}{pqr} - \frac{\tau}{q} = \frac{m_0}{pqr} - \frac{1}{p} + \frac{1}{pq} = \frac{m_0 - qr(1-1/q)}{pqr} \leq \frac{m_0 - q(1-1/q)}{pqr} = \frac{m_1 - q}{pqr}.$$

Therefore in this case we have $\chi(m_1 - q) = 1$. Thus by (5.27) $a_k(pqr) \leq \chi(m'-q-r) \leq 1$.

If $y_{n_0} < \tau$ then $y_{n_1} = y_{n_0} - \tau + q \geq q - \tau$ so that $m_1 = m'$. So $x_{m'+q+r} = x_{m_1-q-r} = p - 1 > p/2$ and therefore by Lemma 5.1 we have $\chi(m'-q-r) = 0$. Hence have $-a_k(pqr) \leq \chi(m_0) \leq 1$.

Next assume $m_1 = m_0 - p + 1$. Then by Lemma 5.2, (5.20), (5.21), and (5.22) we have $x_{m_1-q} = x_{m_0-p+1-q} = 0$ and $y_{m_1-q} \equiv y_{m_0-p+1-q} \equiv y_{m_0} - 1 - \tau$. Thus if $y_{m_0} \geq 1 + \tau$ we have,

$$\frac{x_{m_1-q}}{p} + \frac{y_{m_1-q}}{q} = \frac{y_{m_0} - 1 - \tau}{q} \leq \frac{m_0}{pqr} - \frac{1}{q} - \frac{1}{p} + \frac{1}{pq} = \frac{m_0 + r(1-p-q)}{pqr} \leq \frac{m_0 + 1 - p - q}{pqr} = \frac{m_1 - q}{pqr}.$$

Therefore $\chi(m_1 - q) = 1$ and thus by (5.27) $a_k(pqr) \leq \chi(m'-q-r) \leq 1$. If $y_{m_0} < 1 + \tau$ then $y_{m_1-q} = q + y_{m_0} - 1 - \tau$. If $y_{m_0} > 0$ then $y_{m_1} = y_{m_0} - 1 - \tau + q \geq q - \tau$. Thus $m_1 = m'$. So $x_{m'-q-r} = x_{m_1-q-r} = p - 1 > p/2$ and therefore by Lemma 4.1 we have $\chi(m'-q-r) = 0$.

Hence have $-a_k(pqr) \le \chi(m_0) \le 1$. If $y_{m_0} > 0$ then $y_m < q - \tau$ for all $m \in [m_0, m_1]$.

Thus m' does not exists. Hence $-a_k(pqr) \le \chi(m_0) \le 1$.

Lemma 5.13 Assume $r = \kappa pq - 1$ and $q = \tau p - 1$. Then,

(5.35) $x_1 = 1$ $y_1 = q - \tau$

(5.36) $x_p = 0$ $y_p = q - 1$

(5.37) $x_q = p - 1$ $y_q = 0$

(5.38) $x_r = p - 1$ $y_r = \tau$

Proof. These results follow by direct calculation. We have, $1 \equiv_p x_1 qr \equiv_p x_1$. Hence $x_1 = 1$. We have $1 \equiv_q y_1 pr \equiv_p -y_1 p$. This implies $-\tau p y_1 \equiv_q -\tau$. Since $\tau p \equiv_q 1$, we have $y_1 = q - \tau$. We have $0 \equiv_p p \equiv_p x_1 qr \equiv_p x_1$. Hence $x_p = 0$. We have $p \equiv_q y_p pr$, which implies $1 \equiv_q -y_p$. Hence $y_p = q - 1$. We have $q \equiv_p x_q qr$, which implies $1 \equiv_p x_q r \equiv_p -x_q$. Hence $x_q = p - 1$. We have $0 \equiv_q q \equiv_q y_q pr \equiv_q -py_q$, which implies $y_q = 0$. We have $r \equiv_p x_r qr$, which implies $1 \equiv_p x_q q \equiv_p -x_q$. Hence $x_r = p - 1$. We have $r \equiv_q y_r pr$, which implies $1 \equiv_q y_r p$. Thus we have $\tau \equiv_q y_r \tau p$. Since $\tau p \equiv_q 1$, we have $y_r = \tau$.

Lemma 5.14 Assume $r = \kappa pq + 1$ and $q = \tau p - 1$. If $m \le \frac{\varphi(pqr)}{2}$ and $\chi(m) = 1$ then,

(5.39) $\chi(m+q)=1 \qquad [x_m > 0],$

(5.40) $\chi(m-r)=1 \qquad [y_m \geq \tau],$

(5.41) $\chi(m+r)=1 \qquad [x_m > 0].$

Proof. Assume $\chi(m)=1$. By Lemma 5.1 we must have $x_m < \frac{p}{2}$ and $y_m < \frac{q}{2}$. Note that since $q = \tau p - 1$ we have $-\frac{1}{p}+\frac{\tau}{q}=\frac{r}{pqr}$.

If $x_m > 0$ by (5.37) and Lemma 4.2 we have $x_{m+q} = x_m - 1$ and $y_{m+q} = y_m$. Thus,

$$\frac{x_{m+q}}{p}+\frac{y_{m+q}}{q}=\frac{x_m}{p}+\frac{y_m}{q}-\frac{1}{p}\leq\frac{m}{pqr}-\frac{1}{p}\leq\frac{m+q}{pqr}.$$

Therefore $\chi(m+q)=1$. This establishes (5.39).

If $y_m \geq \tau$ by (5.38) and Lemma 5.2 we have $y_{m-r} = y_m - \tau$. Since $x_m < \frac{p}{2}$ by (5.38) and Lemma 5.2 we have $x_{m-r} = x_m + 1$. Thus,

$$\frac{x_{m-r}}{p}+\frac{y_{m-r}}{q}=\frac{x_m}{p}+\frac{y_m}{q}+\frac{1}{p}-\frac{\tau}{q}\leq\frac{m-r}{pqr}.$$

Therefore $\chi(m-r)=1$. This establishes (5.40).

If $x_m > 0$ by (5.38) and Lemma 5.2 we have $x_{m+r} = x_m - 1$. We must have $\tau < \frac{q}{2}$ because $\tau \geq \frac{q}{2}$ implies $q = \tau p + 1 \geq \frac{qp}{2} + 1 > q$, which is a contradiction. Since $y_m < \frac{q}{2}$ and $\tau < \frac{q}{2}$ we have $y_{m+r} = y_m + \tau$. Therefore,

$$\frac{x_{m+r}}{p} + \frac{y_{m+r}}{q} = \frac{x_m}{p} + \frac{y_m}{q} - \frac{1}{p} + \frac{\tau}{q} \leq \frac{m+r}{pqr}.$$

Therefore $\chi(m+r) = 1$. This establishes (5.41).

We introduce two functions on the nonnegative integers,

(5.42) $$F(m) = \chi(m) - \chi(m+q) - \chi(m-r) + \chi(m+q-r);$$

(5.43) $$G(m) = \chi(m) - \chi(m+q) - \chi(m+r) + \chi(m+q+r).$$

Lemma 5.15 For $m \leq \frac{\varphi(pqr)}{2}$, we have

(5.44) $$F(m) \leq 1 \qquad [x_m = 0],$$

(5.45) $$F(m) \leq 0 \qquad [x_m > 0].$$

Proof. If $x_m = 0$ by Lemma 5.2, (5.37), and (5.38) we have $x_{m+q-r} = x_m$ and $y_{m+q-r} \equiv y_m - \tau$. Assume $y_m < \tau$. Then $y_{m+q-r} > \frac{q}{2}$ and therefore by Lemma 5.1, we have

$\chi(m+q-r)=0$. Now (5.45) follows immediately while (5.46) follows from (5.39). Next assume that $y_m \geq \tau$. Then (5.40) gives $\chi(m-r) \geq \chi(m)$. From this (5.45) follows. Moreover, if $x_m > 0$ then by Lemma 5.2, (5.37), and (5.38) so is x_{m-q+r}. Thus we may apply (5.41) with m replaced by $m+q-r$. This gives $\chi(m+q) \geq \chi(m+q-r)$. From this (5.46) follows.

Lemma 5.16 For $m \leq \frac{\varphi(pqr)}{2}$ satisfying $x_m > 1$ and $y_m < q-\tau$ we have,

(5.46) $$G(m) \leq 0.$$

Furthermore if $\chi(m)=0$ we have,

(5.47) $$G(m) \leq -\chi(m+r).$$

Proof. Assume $x_m > 1$ and $y_m < q-\tau$. By (4.41) we have $\chi(m+r) \geq \chi(m)$. Hence both (5.46) and (5.47) follow from the inequality,

(5.48) $$\chi(m+q) \geq \chi(m+q+r).$$

To establish (5.48) note that by assumption on y_m we have $y_{m+q+r} = y_m + \tau \geq \tau$. Thus we may apply (5.40) with m replaced by $m+q+r$. This gives (5.48).

Lemma 5.17 $\Phi_{pqr}(z)$ is flat if $r \equiv -1 \bmod pq$ and $q \equiv -1 \bmod p$.

Proof. By (2.5) and (5.42) we have $-a_k(pqr) = \sum_{k-q-p<m\le k-q} F(m)$. Now by Lemma 5.2 and (5.35) as m runs through the interval $[k-q-p+1, k-q]$ x_m takes on the value 0 exactly once. Thus $-a_k(pqr) \le 1$ follows from Lemma 5.15. Now we establish the upperbound

By (2.5) and (5.43) we have $a_k(pqr) = \sum_{c<m\le d} G(m)$, where $c = k-r-q-p+1$ and $d = k-r-q$. For $i \in \{0,1\}$ let $m_i \in [c,d]$ be such that $x_{m_i} = i$. By Lemma 5.2 and (5.35) there can be at one $m \in [c,d]$ such that $y_m \ge q-\tau$. If there is such an m let it be denoted by m'.

We claim that

(5.49) $$a_k(pqr) \le \chi(m_0) + \chi(m_1) - \chi(m_1+q) - \chi(m_1+r) + \chi(m'+q+r).$$

To establish this claim note that by Lemma 5.11 we have $a_k(pqr) \le S(m_0) + S(m_1) + S(m')$. Now by Lemma 5.1 we have $\chi(m') = 0$ since $y_{m'} > q/2$. By Lemma 5.2, (5.37), and (5.38) we have $x_{m_0+q+r} = p-2 > p/2$ and $x_{m_1+q+r} = p-1 > p/2$. Hence by Lemma 5.1 we have $\chi(m_0-q-r) = \chi(m_1-q-r) = 0$. Thus (5.49) follows.

Now assume $\chi(m_1) \ge \chi(m_0)$. Then (5.39) and (5.41) give $a_k(pqr) \le \chi(m'+q+r) \le 1$. Alternatively assume $\chi(m_0) = 1$ and $\chi(m_1) = 0$. By Lemma 5.2 and (5.35) there are two possibilities, either $m_1 = m_0 + 1$ or $m_1 = m_0 - p + 1$. First assume $m_1 = m_0 + 1$. Then by

Lemma 5.2, (5.35), and (5.36) we have $x_{m_1+q} = x_{m_0+1+q} = 0$ and $y_{m_1+q} \equiv y_{m_0+1+q} \equiv y_{m_0} + 1 - \tau$.

If $y_{m_0} \geq \tau - 1$ we have,

$$\frac{x_{m_1+q}}{p} + \frac{y_{m_1+q}}{q} = \frac{y_{m_0}}{q} + \frac{1}{q} - \frac{\tau}{q} = \frac{m_0}{pqr} + \frac{1}{q} - \frac{1}{p} - \frac{1}{pq} = \frac{m_0 + pq - pr - r}{pqr} < \frac{m_1 + q}{pqr}.$$

Therefore in this case we have $\chi(m_1 + q) = 1$ and thus $a_k(pqr) \leq \chi(m' - q - r) \leq 1$. If $y_{m_0} < \tau$ then $y_{m_1} = y_{m_0} - \tau + q \geq q - \tau$ so that $m_1 = m'$. So $x_{m'-q-r} = x_{m_1-q-r} = p - 1 > p/2$ and therefore by Lemma 5.1 we have $\chi(m' - q - r) = 0$. Hence have $-a_k(pqr) \leq \chi(m_0) \leq 1$.

Next assume $m_1 = m_0 - p + 1$. Then by Lemma 5.2, (5.35), (5.36), and (5.37) we have $x_{m_1+q} = x_{m_0-p+1+q} = 0$ and $y_{m_1+q} \equiv y_{m_0-p+1+q} \equiv y_{m_0} + 1 - \tau$. Thus if $y_{m_0} \geq \tau - 1$ we have,

$$\frac{x_{m_1+q}}{p} + \frac{y_{m_1+q}}{q} = \frac{y_{m_0} - 1 - \tau}{q} \leq \frac{m_0}{pqr} - \frac{1}{q} - \frac{1}{p} - \frac{1}{pq} \leq \frac{m_0}{pqr} - \frac{1}{p} + \frac{1}{pq} = \frac{m_0 - qr(1 - 1/q)}{pqr} \leq \frac{m_0 - q(1 - 1/q)}{pqr} = \frac{m_1 -}{pq}$$

Therefore $\chi(m_1 + q) = 1$ and thus $a_k(pqr) \leq \chi(m' - q - r) \leq 1$.

If $y_{m_0} < \tau - 1$ then $y_{m_0} = q + \tau - 1$. Then $y_{m_1} = q - 1 \geq q - \tau$. Thus $m_1 = m'$. So $x_{m'-q-r} = x_{m_1-q-r} = p - 1 > p/2$ and therefore by Lemma 5.1 we have $\chi(m' - q - r) = 0$.

Hence have $-a_k(pqr) \leq \chi(m_0) \leq 1$. Hence $-a_k(pqr) \leq \chi(m_0) \leq 1$.

Theorem 3. Let p, q, and r be primes with $5 < p < q < r$. If $r \equiv \pm 1 \bmod pq$ and $q \equiv \pm 1 \bmod p$, then $\Phi_{pqr}(z)$ is flat.

Proof. This follows from Bachman's Theorem, Lemma 5.7, Lemma 5.12, and Lemma 5.17.

REFERENCES

1. G. Bachman, 'Flat Cyclotomic Polynomials of Order Three', *Bull. London Math. Soc.* 38 (2005) 1-8

2. G. Bachman, 'Ternary Cyclotomic Polynomials with an Optimally Large Set of Coefficients', *Pro. Amer. Math. Soc.* 132 (2004) 1943-1950.

3. P. T. Bateman, C. Pomerance and R. C. Vaughan, 'On the Size of the Coefficients of the Cyclotomic Polynomial', *Topics in classical number theory I, II* ed. G. Halasz, Coll. Math. Soc. Janos Boyai 34 (North-Holland, Amsterdam, 1984) 171-202.

4. R. C. Vaughan, 'Bounds for the Coefficients of Cyclotomic Polynomials', *Michigan Math. J.* 21, iss. 4 (1975), 289-295.

5. Weisstein, Eric W, 'Cyclotomic Polynomial,' From *Mathword*—A Wolfram Web Resource. http://mathworld.wolfram.com/CyclotomicPolynomial.html

6. H. Davenport, *Multiplicative Number Theory,* 2nd ed (Springer, New York, 1980)

VITA

Graduate College
University of Nevada, Las Vegas

Thomas Joseph Flanagan

Local Address:
8384 Pearl Beach Court
Las Vegas, NV 89139

Degree:
Bachelor of Science, Mathematics, 2001
State University of New York at Stony Brook

Thesis Title: On the Coefficients of Cyclotomic Polynomials

Thesis Committee:
Chairman, Dr. Gennady Bachman, Ph. D.
Committee Member, Dr. Ebrahim Salehi, Ph. D.
Committee Member, Dr. Derrick DeBose, Ph. D.
Graduate Faculty Representative, Dr. Ashok Singh, Ph. D