Max-Planck-Institut für Mathematik
Bonn

The maximal coefficient of ternary cyclotomic polynomials with one free prime

by

Dominik Duda

Max-Planck-Institut für Mathematik
Preprint Series 2013 (4)

The maximal coefficient of ternary cyclotomic polynomials with one free prime

Dominik Duda

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Hollerbornstr. 3a
65197 Wiesbaden
Germany

MPIM 13-4

The maximal coefficient of ternary cyclotomic polynomials with one free prime

Dominik Duda

Abstract

A cyclotomic polynomial $\Phi_n(x)$ is said to be *ternary* if $n = pqr$, with p, q and r distinct odd primes. Let $M(p, q)$ be the maximum (in absolute value) coefficient appearing in the polynomial family $\Phi_{pqr}(x)$ with $p < q < r$, p and q fixed. Here a stronger version of the main conjecture of Gallot, Moree and Wilms [3] regarding $M(p, q)$ is established. Furthermore it is shown that there is an algorithm to compute $M(p) := \max\{M(p, q) : q > p\}$. Our methods are the most geometric used so far in the study of ternary cyclotomic polynomials.

1 Introduction

Let Φ_n denote the nth cyclotomic polynomial. Let $\omega(n)$ denote the number of distinct prime factors of n. If n is odd and $\omega(n) = 3$, then Φ_n is said to be *ternary*.

Let p, q, r be pairwise coprime positive integers. We define, following Bachman [1], the ternary *inclusion-exclusion* polynomial

$$\Phi_{p,q,r}(x) = \frac{(x^{pqr}-1)(x^p-1)(x^q-1)(x^r-1)}{(x-1)(x^{pq}-1)(x^{pr}-1)(x^{qr}-1)} = \sum_{k=0}^{\infty} a_{p,q,r}(k)x^k.$$

It is not difficult to show that $\Phi_{p,q,r}(x)$ is a polynomial of degree $(p-1)(q-1)(r-1)$ with integer coefficients. Note that the above definition generalizes the notion of ternary cyclotomic polynomials because it coincides with the usual definition of the cyclotomic polynomial Φ_{pqr} in the case where p, q and r denote different primes. This is a consequence of the identity

$$\Phi_n(x) = \prod_{d|n}(x^d-1)^{\mu(\frac{n}{d})},$$

where μ denotes the Möbius function. Every previous result regarding the coefficients of ternary cyclotomic polynomials which is used in this article also applies to inclusion-exclusion polynomials, since the condition that p, q, r are prime is not needed in the proofs of these results.

The *height* $A(p, q, r)$ of $\Phi_{p,q,r}$ is defined by $A(p, q, r) = \max\{|a_{p,q,r}(k)| : k \geq 0\}$. Furthermore, set

$$M(p, q) = \max\{A(p, q, r) : r > 0\} \text{ and } M(p) = \max\{A(p, q, r) : q > 0, r > 0\}.$$

Using Lemma 1 below it is easy to see that $M(p, q) \leq M(p) \leq p$. It has been pointed out by Gallot, Moree and Wilms [3] that for p, q different primes

$$M(p, q) = \max\{A(p, q, r) : r > \max(p, q) \text{ and } r \text{ is prime}\}$$

and for p prime

$$M(p) = \max\{A(p, q, r) : p < q < r \text{ primes}\},$$

so the expressions $M(p)$ and $M(p, q)$ generalize the usual definition of these expressions in the literature about maximal coefficients of ternary cyclotomic polynomials.

Let us introduce the notion

$$M_{q'}(p) = \max\{M(p, q) : q \equiv q' (\text{mod } p) \text{ and } q > 0\},$$

where p denotes a positive integer and q' denotes any integer coprime to p. We will prove the following theorems, the first two of which confirm what Gallot, Moree and Wilms state to be their main conjecture concerning $M(p, q)$ (Conjecture 8 of [3]).

Theorem 1 *Given coprime positive integers p and q', there exists a $q_0 \equiv q' (\text{mod } p)$ with the property that for every integer $q \geq q_0$ satisfying $q \equiv q' (\text{mod } p)$, we have $M(p, q) = M_{q'}(p)$.*

We will also show the following theorem:

Theorem 2 *For every positive integer p and integer q' coprime to p we have $M_{-q'}(p) = M_{q'}(p)$.*

Then, we will describe a finite procedure to determine $M_q(p)$, establishing the following theorem:

Theorem 3 *For each positive integer p and integer q coprime to p there exists a deterministic algorithm to determine the value of $M_q(p)$.*

Since $M(p) = \max\{M_q(p) : 0 < q < p\}$, we only have to apply that procedure for $M_q(p)$ a finite number of times to find the value of $M(p)$, yielding:

Corollary 1 *For each positive integer p, there exists a deterministic algorithm to determine the value of $M(p)$.*

Inspired by our technique to prove Theorem 3 we will finally be able to prove an upper bound for the q_0 defined in Theorem 1:

Theorem 4 *If p and q are positive integers such that*

$$q > 14p^{10}, \tag{1}$$

then $M(p, q) = M_q(p)$.

Remark: This yields another method to calculate $M(p)$: Simply choose for each $q' \in \mathbb{Z}/(p\mathbb{Z})$ the least $q \equiv q' \bmod p$ satisfying (1), calculate $M(p, q)$ for these values (this is possible in finitely many steps, see [3]) and determine the maximum over these values. The procedure described in the proof of Theorem 3 could yield a much more efficient algorithm, if implemented in an elegant manner.

2 Preliminaries: Kaplan's lemma revisited

Recall that p and q are coprime positive integers. Let $0 \le [i]_p < q$ and $0 \le [i]_q < p$ be such that $[i]_p \equiv ip^{-1} (\text{mod } q)$ and $[i]_q \equiv iq^{-1} (\text{mod } p)$. Note that for $0 \le i < pq$ we have $[i]_p p + [i]_q q = i$ or otherwise $[i]_p p + [i]_q q = i + pq$ depending on whether $[i]_p p + [i]_q q$ is greater or smaller than pq. Especially, $[1]_p p + [1]_q q = 1 + pq$. We will use Kaplan's lemma [5] in the following form:

Lemma 1 *Let p, q, r be pairwise coprime positive integers and $k \ge 0$ be an integer. Furthermore, we put*

$$b_i = \begin{cases} 1 & \text{if } [i]_p < [1]_p, [i]_q < [1]_q \text{ and } [i]_p p + [i]_q q \le k/r; \\ -1 & \text{if } [i]_p \ge [1]_p, [i]_q \ge [1]_q \text{ and } [i]_p p + [i]_q q - pq \le k/r; \\ 0 & \text{otherwise.} \end{cases}$$

We have

$$a_{p,q,r}(k) = \sum_{m=0}^{p-1} (b_{f(m)} - b_{f(m+q)}), \tag{2}$$

where $f(m)$ is the unique integer such that $f(m) \equiv r^{-1}(k - m) (\text{mod } pq)$ and $0 \le f(m) < pq$.

We introduce $0 \le a, b < pq$ with $a \equiv -r^{-1} (\text{mod } pq)$ and $b \equiv kr^{-1} (\text{mod } pq)$, implying $f(m) \equiv am + b (\text{mod } pq)$. Let s be an irrational integer with $\lfloor k/r \rfloor < pqs < \lfloor k/r \rfloor + 1$. Note that

$$[i]_p p + [i]_q q \le \frac{k}{r} \text{ and } [i]_p p + [i]_q q - pq \le \frac{k}{r}$$

are equivalent to

$$\frac{[i]_p}{q} + \frac{[i]_q}{p} < s \text{ and } \frac{[i]_p}{q} + \frac{[i]_q}{p} < s + 1,$$

respectively.

Since $M(p, q) = \max\{|a_{p,q,r}(k)| : r \ge 1,\ k \ge 0,\ (pq, r) = 1\}$, we now regard p, q as fixed and k, r as varying. We can remove k and r from the conditions of the lemma and formulate the conditions in the lemma only using p, q, a, b and s. On the other hand, given any triple a, b, s where $a \in (\mathbb{Z}/pq\mathbb{Z})^*$, $b \in \mathbb{Z}/pq\mathbb{Z}$ and s is a positive irrational number, we can easily find k, r such that $a \equiv -r^{-1} (\text{mod } pq)$, $b \equiv kr^{-1} (\text{mod } pq)$ and $\lfloor k/r \rfloor < pqs < \lfloor k/r \rfloor + 1$ (simply choose $r > pq$, $(r, pq) = 1$, with $r \equiv -a^{-1} (\text{mod } pq)$ and take a $k \in (\lfloor pqs \rfloor r, \lfloor pqs \rfloor r + r)$ with $k \equiv br (\text{mod } pq)$, which is possible since the length of this interval is greater than pq). Therefore from Lemma 1 and the above argument we infer the following result regarding $M(p, q)$.

Lemma 2 *Let p, q be coprime positive integers, $a \in (\mathbb{Z}/pq\mathbb{Z})^*$, $b \in \mathbb{Z}/pq\mathbb{Z}$ and $s \in \mathbb{R}^+ \setminus \mathbb{Q}$ and $0 \le f(m) < pq$ with $f(m) \equiv am + b (\text{mod } pq)$. Let*

$$b_i = \begin{cases} 1 & \text{if } [i]_p < [1]_p, [i]_q < [1]_q \text{ and } \frac{[i]_p}{q} + \frac{[i]_q}{p} < s; \\ -1 & \text{if } [i]_p \ge [1]_p, [i]_q \ge [1]_q \text{ and } \frac{[i]_p}{q} + \frac{[i]_q}{p} < s + 1; \\ 0 & \text{otherwise.} \end{cases}$$

Then $\sum_{m=0}^{p-1}(b_{f(m)} - b_{f(m+q)})$ is the value of $a_{p,q,r}(k)$ for appropriately chosen k and r. We have

$$M(p,q) = \max\{\big|\sum_{m=0}^{p-1}(b_{f(m)} - b_{f(m+q)})\big| : a \in (\mathbb{Z}/pq\mathbb{Z})^*, b \in \mathbb{Z}/pq\mathbb{Z}, s \in \mathbb{R}^+ \setminus \mathbb{Q}\}.$$

3 Proof of Theorem 1

In the following paragraph we fix coprime positive integers p, q' and choose a $q \equiv q' (\mathrm{mod}\ p)$. For notational convenience we put $\rho = [1]_p$ and $\sigma = [1]_q$.

Let $T_q : \mathbb{Z}/pq\mathbb{Z} \to [0,1)^2$ denote the map into the unit square given by

$$T_q(i) = (t_x(i), t_y(i)) := \left(\frac{[i]_p}{q}, \frac{[i]_q}{p}\right).$$

For ease of formulation we will say "i lies in..." instead of "$T_q(i)$ lies in...". By the Chinese remainder theorem the image of T_q equals

$$\Gamma := \{(x,y) \in [0,1)^2 : qx, py \in \mathbb{Z}\}.$$

Put

$$\mathrm{diag} = \{(x,y) \in \mathbb{R}^2 : x + y = 1\},$$

i.e. diag is the diagonal through the upper left and lower right vertex of the unit square. Since $\rho p + \sigma q = 1 + pq$ we have $t_x(1) + t_y(1) = \rho/q + \sigma/p = 1 + 1/pq$. Note that $T_q(1)$ is the element of Γ above diag with the least distance to diag (since any other i lying above diag satisfies $t_x(i) + t_y(i) = 1 + i/pq > 1 + 1/pq$). Define $Z = (1 - \sigma/p, \sigma/p)$. Observe that Z does not belong to Γ and is the intersection point of the lines $l := \{(x, \sigma/p) \in \mathbb{R}^2\}$ and diag.

There is no element of Γ between Z and $T_q(1)$, because such a point would have a smaller distance to diag than $T_q(1)$. Therefore the "left neighbor" of $T_q(1)$ in Γ (i.e., the point with coordinates $(t_x(1) - 1/q, t_y(1)))$ lies left of Z, which implies $(\rho - 1)/q < 1 - \sigma/p < \rho/q$. Let h be the vertical line passing through Z. Observe that the coordinate equation of h is given by $x = 1 - \sigma/p$, so no point of Γ lies on h. The conditions $[i]_p < \rho, [i]_q < \sigma$ and $[i]_p \geq \rho, [i]_q \geq \sigma$ appearing in Lemma 1 are equivalent to "i lies beneath l and left of h" and "i lies above or on l and right of h", respectively. Define

$$s_+ = \{(x,y) \in \mathbb{R}^2 : x + y < s\} \text{ and } s_- = \{(x,y) \in \mathbb{R}^2 : x + y < s + 1\}.$$

Let

$$G_+ = \{(x,y) \in [0,1)^2 : x + y < s,\ x < 1 - \frac{\sigma}{p},\ y < \frac{\sigma}{p}\}$$

and

$$G_- = \{(x,y) \in [0,1)^2 : x + y < s + 1,\ x > 1 - \frac{\sigma}{p},\ y \geq \frac{\sigma}{p}\}$$

be the polygons which are bounded by the lines $x = 0, y = 0, h, l, s_+$, respectively $x = 1, y = 1, h, l, s_-$. Their definitions depend only on p, q' and s, but not on q itself as long as $q \equiv q' (\mathrm{mod}\ p)$ because $\sigma = [1]_q \equiv q^{-1} \equiv q'^{-1} (\mathrm{mod}\ p)$ depends only on p and q'. We will call the pair $G = (G_+, G_-)$ a *polygon pair.*

With these definitions we can alternatively write b_i as

$$b_i = \begin{cases} 1 & \text{if } i \text{ lies in } G_+; \\ -1 & \text{if } i \text{ lies in } G_-; \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

We will now describe the behavior of $T_q(f(m))$. From now on we will regard $[0,1)^2$ as $(\mathbb{R}/\mathbb{Z})^2$, then T_q is a linear map and, since $f(0), f(1), \ldots, f(p-1)$ is an arithmetic progression,

$$S_+ := (T_q(f(0)), T_q(f(1)), \ldots, T_q(f(p-1)))$$

is also an arithmetic progression on $(\mathbb{R}/\mathbb{Z})^2$, starting at an arbitrary $T_q(b) \in \Gamma$ and being continued by a vector $\vec{T_q}(a) = ([a]_p/q, [a]_q/p)^t$ which is only subject to the condition that $[a]_p$ and $[a]_q$ are coprime to q and p, respectively. Furthermore,

$$[f(m+q)]_p \equiv (am + aq + b)p^{-1} \equiv (am+b)p^{-1} \equiv [f(m)]_p (\text{mod } q)$$

and

$$[f(m+q)]_q \equiv (f(m) + aq)q^{-1} \equiv [f(m)]_q + q[a]_q (\text{mod } p).$$

This means that we obtain the points of the arithmetic progression

$$S_- := (T_q(f(q)), T_q(f(q+1)), \ldots, T_q(f(q+p-1)))$$

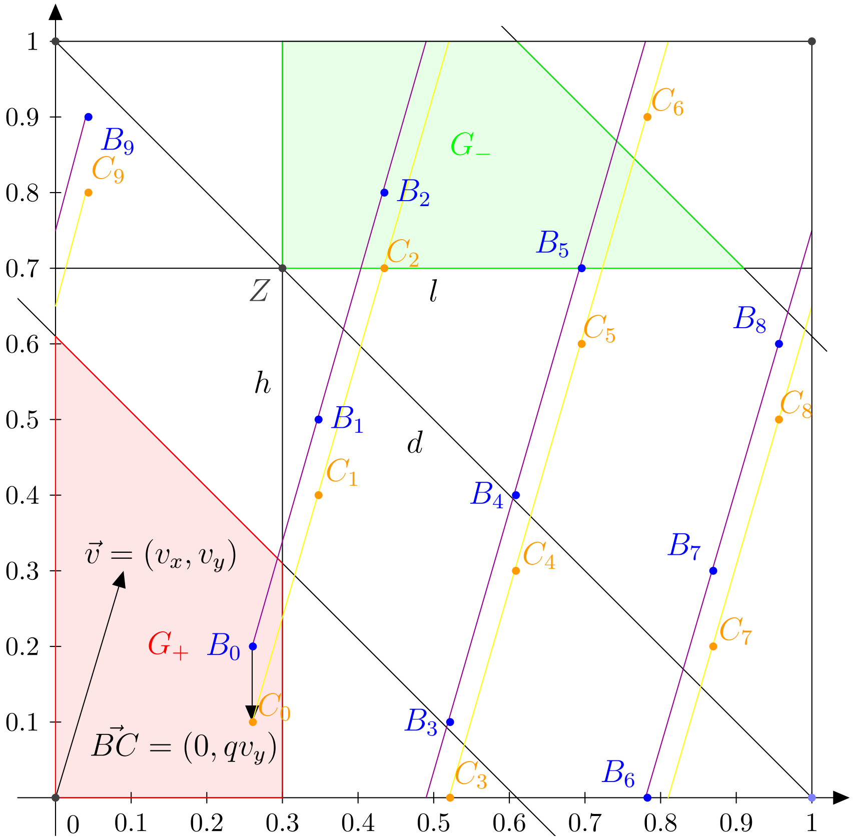
by translating the points S_+ by the vector $(0, q[a]_q/p)^t$. By combining (2) and (3) and using the introduced notation, we obtain:

$$a_{p,q,r}(k) = |G_+ \cap S_+| + |G_- \cap S_-| - |G_+ \cap S_-| - |G_- \cap S_+|. \tag{4}$$

Especially,

$$M(p,q) = \max\{||G_+ \cap S_+| + |G_- \cap S_-| - |G_+ \cap S_-| - |G_- \cap S_+||\},$$

where a, b and s range over their whole domains, which means that (S_+, S_-) ranges over every pair of arithmetic sequences $(B, B+\vec{v}, B+2\vec{v}, \ldots, B+(p-1)\vec{v}) \in \Gamma^p$ and $(C, C+\vec{v}, C+2\vec{v}, \ldots, C+(p-1)\vec{v}) \in \Gamma^p$ subject to the constraints that its generating vector $\vec{v} = (v_x, v_y)^t$ fulfills $\gcd(qv_x, q) = 1$, $\gcd(pv_y, p) = 1$ and that $C = B + (0, qv_y)$. We will call such a pair of sequences a *q-legal sequence*.



Define $\Omega = \{(x, y) \in [0, 1)^2 : x \in \mathbb{Q} \setminus \{1 - \sigma/p\},\ py \in \mathbb{Z}\}$. Note that the definition of Ω (and $G_\pm$ as we have seen before) depends only on p and q', but not on q as long as $q \equiv q'(\text{mod } p)$. We will now consider the pairs of sequences $S_+ = (B, B+\vec{v}, B+2\vec{v}, \ldots, B+(p-1)\vec{v}) \in \Omega^p$ and $S_-(C, C+\vec{v}, C+2\vec{v}, \ldots, C+(p-1)\vec{v}) \in \Omega^p$ such that $\vec{v} = (v_x, v_y)^t$ fulfills $\gcd(pv_y, p) = 1$ and $C = B + (0, qv_y)$ (since $qv_y \equiv q'v_y(\text{mod } p)$ this definition does also depend only on p and q'). Those pairs of sequences are called *legal sequences*. For every polygon pair $G = (G_+, G_-)$ and legal or q-legal sequence $S = (S_+, S_-)$ let $\chi_G(S)$ denote the value $|G_+ \cap S_+| + |G_- \cap S_-| - |G_+ \cap S_-| - |G_- \cap S_+|$ (we will call this value the *characteristic* of S). We define $m_q(p)$ to be the absolute maximum of $\chi_G(S)$ where S ranges over the legal sequences and G ranges over all polygon pairs. This is another definition which depends only on p and q' so that we can equivalently write $m_{q'}(p)$. We will see at the end of this proof that $m_q(p) = M_q(p)$.

Obviously, $\Gamma \subset \Omega$ and any q-legal sequence is legal. This means that:

$$\begin{aligned} M(p,q) &= \max\{|\chi_G(S)| : S \text{ is } q\text{-legal}, G \text{ is a polygon pair}\} \\ &\leq \max\{|\chi_G(S)| : S \text{ is legal}, G \text{ is a polygon pair}\} = m_{q'}(p). \end{aligned} \tag{5}$$

Now we will show that, on the other hand, $M(p, q) \geq m_{q'}(p)$ for any large enough q with $q \equiv q'(\text{mod } p)$. Let (S, G) be a pair, consisting of a legal sequence S and a polygon pair G, such that $|\chi_G(S)|$ is maximal (i. e. $= m_q(p)$).

For each $F \in \Omega$ we will call the unique set $H(F) \in \{G_+, G_-, \Omega \setminus (G_+ \cup G_-)\}$ in which F is contained, the *home* of F. First, we show that there is an $\epsilon > 0$ such that for each $F = (f_x, f_y) \in S$ all the points of $N_F = \Omega \cap \{(f_x + \mu, f_y) : 0 \leq \mu < \epsilon\}$, the "right neighborhood" of F, lie in the home of F.

This follows from the fact that the only points not having a right neighborhood lying in their home are those on the right boundary of the unit square, G^+ or G^-. But these right boundaries consist solely of the lines s_+, s_-, h and $x = 1$, which contain no point of Ω because the equations $x + y = s$ and $x + y = s + 1$ which describe s_+ and s_- have no rational solution (note that we defined s to be irrational) and the line h given by $x = 1 - \sigma/p$ as well as the right boundary of the unit square contain no point of Ω by the definition of Ω. So each $F \in \Omega$ has a right boundary of the form $N_F = \Omega \cap \{(f_x + \mu, f_y) : 0 \leq \mu < \epsilon_F\}$ for some ϵ_F, and $\epsilon := \min_{F \in S}\{\epsilon_F\}$ fulfills the required property.

The Jacobsthal-function of an integer n, is the least positive integer such that among any $j(n)$ consecutive integers, there is at least one integer coprime to n. Kanold [4] showed that $j(n) \leq 2^{\omega(n)}$, where $\omega(n)$ denotes the number of distinct prime divisors of n. Note that

$$\frac{j(n)^2}{n} \leq \frac{4^{\omega(n)}}{n} \leq \prod_{p|n} \frac{4}{p} \leq \frac{4}{2} \cdot \frac{4}{3} < 3. \tag{6}$$

It follows from this that $j(n) = O(\sqrt{n})$ and hence we can choose a $q_0 \equiv q' (\mathrm{mod}\ p)$ with $j(q)/q < \epsilon/p$ for all $q \geq q_0$ with $q \equiv q' (\mathrm{mod}\ p)$. We will now consider such a q.

Let $B = (b_x, b_y)$ be the first point in the arithmetic progression S_+. There is an integer in the interval $[qb_x, qb_x + 1)$, say w. Note that $B' := (w/q, b_y)$ is contained in Γ and lies less than ϵ/p to the right of B, since $1/q < j(q)/q$ and, by assumption, $j(q)/q < \epsilon/p$. Let $\vec{v} = (v_x, v_y)^t$ be the generating vector of $S_+ = (B, B + \vec{v}, \ldots, B + (p-1)\vec{v})$. There is an integer ν coprime to q in the interval $[qv_x, qv_x + j(q))$ since it contains at least $j(q)$ different integers. Set $\vec{v}' := (\nu/q, v_y)^t$ which deviates from $\vec{v}$ by a vector $\vec{\delta}$ pointing straight along the x-axis in positive direction and having length smaller than ϵ/p, since by assumption $j(q)/q < \epsilon/p$.

Note that $\vec{v}'$ is a permitted vector for a q-legal sequence since $\gcd(\nu, q) = 1$ by the definition of ν and $\gcd(pv_y, p) = 1$ since by assumption S is a legal sequence. Especially every point $B' + k\vec{v}'$ in $S'_+ := (B', B' + \vec{v}', ..., B' + (p-1)\vec{v}')$ with $0 \leq k \leq p - 1$ belongs to Γ, because the components of the vector $\vec{v}'$ are integral multiples of $1/q$ and $1/p$ respectively, implying that the translation by $\vec{v}'$ maps points of Γ to points of Γ.

Furthermore, every point $B' + k\vec{v}'$ in $S'_+ = (B', B' + \vec{v}', \ldots, B' + (p-1)\vec{v}')$ with $0 \leq k \leq p - 1$ is obtained from its corresponding $B + k\vec{v} \in S_+$ by a translation to the right with absolute value equal to $|B' - B| + k|\vec{\delta}| < (k+1)\epsilon/p \leq p\epsilon/p = \epsilon$ which means that $B' + k\vec{v}'$ lies in $N_{B+k\vec{v}}$. If we define S'_- as the image of S'_+ under the translation with vector $(0, q'v_y)^t$ (this is the vector which maps S_+ to S_-), then each point $F' \in S'_-$ lies also in N_F, where F appears at the same position in the tuple S_- as F' does in S'_-. Thus, every $F' \in S'$ lies in the home of its corresponding F and thus, contributes in the same way to the values $|G_+ \cap S'_+|, |G_- \cap S'_-|, |G_+ \cap S'_-|$ and $|G_- \cap S'_+|$ as F contributes to $|G_+ \cap S_+|, |G_- \cap S_-|, |G_+ \cap S_-|$ and $|G_- \cap S_+|$, respectively. As a consequence we have that

$$\begin{aligned}\chi_G(S') &= |G_+ \cap S'_+| + |G_- \cap S'_-| - |G_+ \cap S'_-| - |G_- \cap S'_+| \\ &= |G_+ \cap S_+| + |G_- \cap S_-| - |G_+ \cap S_-| - |G_- \cap S_+| = \chi_G(S)\end{aligned}$$

for every G.

But since the components of the vector mapping S_+ onto S_- are integral multiples of $1/q$ and $1/p$, we deduce that this vector maps Γ onto Γ so that all points in S' lie in Γ and, since v' fulfills also the coprimality condition, S' is q-legal.

So, finally

$$\begin{aligned}M(p,q) &= \max\{|\chi_G(S^*)| : S^* \text{ is } q\text{-legal}, G^* \text{ is a polygon pair}\} \\ &\geq |\chi_G(S')| = |\chi_G(S)| = m_{q'}(p) \qquad (7)\end{aligned}$$

Together with (5), this implies $m_{q'}(p) = M(p,q)$ for q large enough, and shows that $m_{q'}(p)$ is the maximum of $M(p,q)$, where q ranges over all the positive integers in the residue class of $q'(\text{mod } p)$. So $m_{q'}(p) = M_{q'}(p)$ and the theorem follows. □

4 Proof of Theorem 2

Elder [2] established the following lemma (generalizing an earlier lemma of Kaplan [5]).

Lemma 3 *Let a, b, c be positive coprime integers and $d > a + b - 1$ with $d \equiv \pm c(\text{mod } ab)$. Then $|A(a,b,c)| \leq |A(a,b,d)|$.*

Proof of Theorem 2. Choose a $q \equiv q'(\text{mod } p)$ with $M(p,q) = M_{q'}(p)$ and let r be a positive integer with $|A(p,q,r)| = M(p,q) = M_{q'}(p)$. Choose some $s \equiv -q(\text{mod } pr)$ with $s > p + r - 1$. Then $M_{q'}(p) = |A(p,q,r)| \leq |A(p,s,r)| \leq M(p,s) \leq M_s(p) = M_{-q'}(p)$. So for every $q' \in \mathbb{Z}$ coprime to p, we have $M_{q'}(p) \leq M_{-q'}(p)$. But the same line of thought, applied to $-q'$ instead of q', leads to $M_{-q'}(p) \leq M_{q'}(p)$, immediately yielding the theorem. □

5 Proof of Theorem 3

In Section 3 it was observed that $M_q(p)$ is the absolute maximum of the characteristic of a legal sequence on Ω. We will now describe a procedure which could be transformed into an algorithm to determine this value.

First, fix the y-coordinates of the first element $B = (b_x, b_y)$ of $S_+ = (B, B + \vec{v}, \ldots, B + (p-1)\vec{v})$ and the y-coordinate of the generating vector $\vec{v} = (v_x, v_y)^t$, where we assume w.l.o.g. that v_x and v_y lie in $[0,1)$ (note that by the definitions of Ω and legal sequences, there are p possibilities for the first choice and $\phi(p)$ for the second, so we can apply the following procedure for all these $p\phi(p)$ cases separately).

Now we consider the three continuous degrees of freedom b_x, v_x and s. They determine $\chi_G(S)$ uniquely. Forget for a moment the constraints on b_x, v_x, s which are:

$$\begin{aligned}
&b_x, v_x \in \mathbb{Q}\\
&s \in \mathbb{R}^+ \setminus \mathbb{Q} \text{ and}\\
&b_x + kv_x \not\equiv 1 - \frac{\sigma}{p} (\text{mod } 1),\ \ k = 0, 1, \ldots, p-1.
\end{aligned} \tag{8}$$

Assume that b_x, v_x and s are arbitrary real numbers in $[0, 1)$ and imagine the unit cube $(\mathbb{R}/\mathbb{Z})^3$ to be their domain. Define

$$S_+ =: (B_0, B_1, \ldots, B_{p-1}) \text{ and } S_- =: (B_p, B_{p+2} \ldots, B_{2p-1}).$$

For each $0 \le k \le 2p - 1$, regard B_k as a linear function in b_x, v_x, namely the one which assigns the position of B_k to a given pair (b_x, v_x). Now define

$$P_+(k) = \{(b_x, v_x, s) : B_k(b_x, v_x) \in G_+\} \text{ and } P_-(k) = \{(b_x, v_x, s) : B_k(b_x, v_x) \in G_-\}.$$

Since, for $k < p$, $B_k = (b_x + kv_x, b_y + kv_y)$ lies in G_+ exactly if

- $b_x + kv_x + b_y + kv_y < s$;
- $0 < b_x + kv_x < 1 - \sigma/p$;
- $0 < b_y + kv_y < \sigma/p$

(where the conditions have to be interpreted modulo 1) and we have analogous conditions for $k \ge p$, we see that $P_+(k)$ is described entirely by linear inequalities with rational coefficients in (b_x, v_x, s) and thus is a set which can be described as a union of polyhedra in the unit cube. The same result applies also to $P_-(k)$. Now define the function

$$\chi(b_x, v_x, s) = |\{k < p : (b_x, v_x, s) \in P_+(k)\}| + |\{k \ge p : (b_x, v_x, s) \in P_-(k)\}|$$

$$-|\{k < p : (b_x, v_x, s) \in P_-(k)\}| - |\{k \ge p : (b_x, v_x, s) \in P_+(k)\}|,$$

which is obviously the characteristic of the sequence with these particular values of (b_x, v_x, s). With this terminology $M_q(p)$ is the maximum absolute value of χ, where b_x, v_x, s *are* subject to the constraints mentioned before. We can now apply an algorithm to determine the finitely many different parts of the cube which we obtain when we dissect it at the boundaries of the polyhedra $P_+(k)$ and $P_-(k)$. For each of these parts, we can check easily in which of these polyhedra it is contained and thereby calculate its characteristic (more precisely, the common characteristic of all the points it contains). Now we show that $M_q(p)$ is the maximum of the absolute value of the characteristic taken over all parts of the cube with positive volume (this latter restriction excludes the exceptional parts of the dissection with dimension < 3 which occur e.g. when some polyhedra only share a face, edge or vertex), a value which we can directly read off from our previous computations.

It suffices to show that in each component with positive volume there is a point satisfying the restrictions stated in (8), thus representing a legal sequence and that, conversely, any point satisfying these restrictions lies in a part of this dissection with positive volume. The former is trivial because the set of triples satisfying the restriction is dense in $[0, 1)^3$.

The latter can be deduced from the observation which we made in the proof of Theorem 1 that for each legal sequence there is a small $\epsilon > 0$ with the property that we can increase v_x and b_x by arbitrary values not greater than ϵ, such that no point of the legal sequence leaves its home.

This implies that, for each point $P = (b_x, v_x, s)$ in the dissected cube satisfying the restriction (8), all the points (b_x+w_1, v_x+w_2, s) with arbitrary $0 \leq w_1, w_2 \leq \epsilon$ lie in the same part of the dissection as P. Now consider the minimum d of the distance from a point in the legal sequence represented by P to one of the lines s_+, s_- (which were defined by $x + y = s$ and $x + y = s + 1$, respectively). Then d is positive as no point of a legal sequence lies on s_+ or s_-. Assume w.l.o.g. that $\epsilon < d/(p+1)$. If we increase b_x, v_x by $w_1, w_2 \leq \epsilon$ each point of the sequence is translated by a vector with modulus $\leq w_1 + (p-1)w_2 < p\epsilon$. By the triangle inequality, the distance of any of these points to s_+ or s_- does not decrease to less than $d - p\epsilon > (p+1)\epsilon - p\epsilon = \epsilon$ and we are able to increase the value of s by any value $0 < w_3 < \epsilon$ without letting s_+ or s_- cross any point of the sequence. This implies that the whole cube

$$V := \{(b_x + w_1, v_x + w_2, s + w_3) : 0 \leq w_1, w_2, w_3 \leq \epsilon\}$$

lies in the same part of the dissection as P which proves the claim made above and therefore shows that we can compute $M_q(p)$ algorithmically in the previously described way, completing the proof of Theorem 3 and yielding Corollary 1. □

6 Proof of Theorem 4

Recall that, in the definition of the dissection of the unit cube in the previous section, the planes dissecting the cube were given by equations of the form:

$$b_x + kv_x + \varpi s = m/p \tag{9}$$

Here $0 \leq k < p$ is an integer, $\varpi \in \{-1; 0\}$ and $m/p \equiv \alpha \bmod 1$ with $\alpha \in \{0, -\sigma/p, b_y + kv_y\}$, so m is also an integer. In addition, the boundary of the cube is described by the equations $b_x = 0, b_x = 1, v_x = 0, v_x = 1, s = 0$ and $s = 1$. If a point $V(b_x, v_x, s)$ is the point of intersection of three such planes of the form (9), then it is obtained as the unique solution of the linear system of equations:

$$\begin{pmatrix} 1 & k_1 & \varpi_1 \\ 1 & k_2 & \varpi_2 \\ 1 & k_3 & \varpi_3 \end{pmatrix} \begin{pmatrix} b_x \\ v_x \\ s \end{pmatrix} = \begin{pmatrix} m_1/p \\ m_2/p \\ m_3/p \end{pmatrix} \tag{10}$$

By applying Cramer's Rule, we obtain:

$$b_x = \frac{\begin{vmatrix} m_1/p & k_1 & \varpi_1 \\ m_2/p & k_2 & \varpi_2 \\ m_3/p & k_3 & \varpi_3 \end{vmatrix}}{\begin{vmatrix} 1 & k_1 & \varpi_1 \\ 1 & k_2 & \varpi_2 \\ 1 & k_3 & \varpi_3 \end{vmatrix}} = \frac{\begin{vmatrix} m_1 & k_1 & \varpi_1 \\ m_2 & k_2 & \varpi_2 \\ m_3 & k_3 & \varpi_3 \end{vmatrix}}{p\begin{vmatrix} 1 & k_1 & \varpi_1 \\ 1 & k_2 & \varpi_2 \\ 1 & k_3 & \varpi_3 \end{vmatrix}}$$

as well as:

$$v_x = \frac{\begin{vmatrix} 1 & m_1 & \varpi_1 \\ 1 & m_2 & \varpi_2 \\ 1 & m_3 & \varpi_3 \end{vmatrix}}{p\begin{vmatrix} 1 & k_1 & \varpi_1 \\ 1 & k_2 & \varpi_2 \\ 1 & k_3 & \varpi_3 \end{vmatrix}}$$

Observe that, the numerators in both fractional expressions are determinants of matrices with integral entries and therefore integers, while the denominators are both of the form $p\varrho$ where ϱ is an integer between 0 and $p-1$. This can be deduced from the fact that for all values ϖ_i equal, the determinant would be zero, violating the assumption that the three planes intersect in a single point, and, whenever one or two of the values $\varpi_1, \varpi_2, \varpi_3$ are nonzero, then the determinant is given by $\varrho = k_i - k_j$ for $i, j \in \{1, 2, 3\}$. It is easy to see that b_x, v_x are still rationals with denominator $p\varrho$ when one or more of the three planes are replaced by faces of the cube.

Let $\mathcal{P}$ be a polyhedron of the dissection associated to $M_q(p)$. Since it is a nondegenerate convex polyhedron with positive volume, its boundary contains at least 4 vertices, which are denoted (together with their respective coordinates) $A(A_1, A_2, A_3), B(A_1, A_2, A_3), C(C_1, C_2, C_3)$ and $D(D_1, D_2, D_3)$. Each of these points is the intersection of three planes of the dissection (including the faces of the unit cube). Hence we can write $A_i = \frac{a_i}{p\alpha}$, $B_i = \frac{b_i}{p\beta}$, $C_i = \frac{c_i}{p\gamma}$ and $D_i = \frac{d_i}{p\delta}$ for $i = 1, 2$ with $a_i, b_i, c_i, d_i, \alpha, \beta, \gamma, \delta$ integers such that $0 < \alpha, \beta, \gamma, \delta < p$.

Let π be the projection $(b_x, v_x, s) \mapsto (b_x, v_x)$. This projection maps $\mathcal{P}$ to a convex polygon $\mathcal{P}'$ with positive volume. Define A', B', C', D' as the projections of A, B, C, D. We assume that A, B, C have been chosen in such a way that A', B', C' are not collinear (this is possible because, otherwise, all vertices of $\mathcal{P}'$ would lie on the same line, forcing $\mathcal{P}'$ to have zero area). The area F of the triangle $A'B'C'$ is given by the formula:

$$\begin{aligned} F &= \frac{1}{2}|A_1B_2 + B_1C_2 + C_1A_2 - A_1C_2 - C_1B_2 - B_1A_2| \\ &= \frac{1}{2}\left|\frac{a_1b_2}{p^2\alpha\beta} + \frac{b_1c_2}{p^2\beta\gamma} + \frac{c_1a_2}{p^2\gamma\alpha} - \frac{a_1c_2}{p^2\alpha\gamma} - \frac{c_1b_2}{p^2\gamma\beta} - \frac{b_1a_2}{p^2\beta\alpha}\right| \\ &= \frac{l}{2p^2\alpha\beta\gamma} \end{aligned} \tag{11}$$

Here l denotes a positive integer. Thus, $l \geq 1$, which yields, together with $\alpha, \beta, \gamma < p$, the estimate:

$$F > \frac{1}{2p^5} \tag{12}$$

On the other hand, the circumference U of the triangle cannot be greater than $3\sqrt{2}$ because every side of the triangle is a line segment inside the unit square and cannot be longer than $\sqrt{2}$, the length of its diagonal. By means of the well-known formula $2F = rU$, this gives us a lower estimate for r, the radius of its incircle:

$$r = \frac{2F}{U} > \frac{1}{3\sqrt{2}p^5} \tag{13}$$

Now for any q satisfying the required inequality (1) we have:

$$\frac{\sqrt{1+j(q)^2}}{q} \leq \frac{\sqrt{3q}}{q} = \sqrt{\frac{3}{q}} < \frac{2}{3\sqrt{2}p^5} < 2r,$$

where we used that (6) implies that $j(q)^2 + 1 \leq 3q$. Observe that the left side equals the length of the diagonal of a rectangle with sides of length $1/q$ and $j(q)/q$, while the right side equals the diameter of the circle. Since a diagonal of a rectangle is a diameter of its respective circumcircle, every rectangle can be embedded in a circle with diameter greater than that diagonal. In particular, it is possible to place a rectangle with sides of length $1/q$ and $j(q)/q$ parallel to the b_x- and v_x-coordinate axes, respectively, inside the incircle of the triangle.

By the definition of $j(q)$, this rectangle contains a point $\mathfrak{p}'$ with coordinates $(\mathfrak{b}/q, \mathfrak{v}/q)$, where $\mathfrak{b}, \mathfrak{v}$ denote integers in $]0, q[$ with $\mathfrak{v}$ coprime to q. Since $\mathfrak{p}'$ lies in $\mathcal{P}'$, there is a point $\mathfrak{p} = (\mathfrak{b}/q, \mathfrak{v}/q, s) \in \mathcal{P}$ with $\pi(\mathfrak{p}) = \mathfrak{p}'$. Now observe that this point $\mathfrak{p}$ together with the choice of b_y and v_y, which was made a priori (see the beginning of the proof of Theorem 3), specifies a q-legal sequence S whose characteristic value equals $M_q(p)$ because of the choice of the polygon $\mathcal{P}$.

This implies that $M(p,q) \geq \chi(S) = M_q(p)$ and therefore $M(p,q) = M_q(p)$, as desired. □

Acknowledgment. Most of this paper was written during a month long internship at the Max-Planck-Institut für Mathematik in Bonn. I would like to thank the MPIM for offering me this unique opportunity to conduct active mathematical research before taking up my studies. I wish to thank Robert Wilms for introducing me to the subject and calling my attention to several errors in the early version of the manuscript. I am very grateful to my advisor, Pieter Moree for his helpful suggestions and for improving significantly the comprehensibility and layout of this article. I would like to thank Alexander Weisse for his help with the creation of the illustration used in this paper. Finally, I would like to thank Frederik Benzing and Jakob Schneider, the two other interns engaged in the investigation of cyclotomic polynomials, for useful comments on early versions of my proofs.

References

[1] G. Bachman, On ternary inclusion-exclusion polynomials, *Integers* **10** (2010), A48, 623-638.

[2] S. Elder, Flat cyclotomic polynomials: a new approach, arXiv:1207.5811.

[3] Y. Gallot, P. Moree and R. Wilms, The family of ternary cyclotomic polynomials with one free prime, *Involve* **4** (2011), 317–341.

[4] H.-J. Kanold, Über eine zahlentheoretische Funktion von Jacobsthal, *Math. Ann.* **170** (1967), 314–326.

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

Dominik Duda, Hollerbornstr. 3a, 65197 Wiesbaden, Germany
Email-address: dominik.du@gmail.com