Max-Planck-Institut für Mathematik
Bonn

A proof of the corrected Sister Beiter cyclotomic coefficient conjecture inspired by Zhao and Zhang

by

Branko Juran
Pieter Moree
Adrian Riekert
David Schmitz
Julian Völlmecke

Max-Planck-Institut für Mathematik
Preprint Series 2023 (33)

Date of submission: December 21, 2023

A proof of the corrected Sister Beiter cyclotomic coefficient conjecture inspired by Zhao and Zhang

by

Branko Juran
Pieter Moree
Adrian Riekert
David Schmitz
Julian Völlmecke

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

Applied Mathematics
Institute for Analysis and Numerics
University of Münster
Orleans-Ring 10
48149 Münster
Germany

Department of Mathematical Sciences
University of Copenhagen
Universitetsparken 5
2100 Copenhagen
Denmark

Fachbereich Mathematik
Technische Universität Darmstadt
Schlossgartenstr. 7
64289 Darmstadt
Germany

Rheinische Friedrich-Wilhelms-
Universität Bonn
Regina-Pacis-Weg 3
53113 Bonn
Germany

MPIM 23-33

A PROOF OF THE CORRECTED SISTER BEITER CYCLOTOMIC COEFFICIENT CONJECTURE INSPIRED BY ZHAO AND ZHANG

B. JURAN, P. MOREE, A. RIEKERT, D. SCHMITZ, AND J. VÖLLMECKE

Abstract. The largest coefficient (in absolute value) of a cyclotomic polynomial Φ_n is called its height $A(n)$. In case p is a fixed prime it turns out that as q and r range over all primes satisfying $p < q < r$, the height $A(pqr)$ assumes a maximum $M(p)$. In 1968, Sister Marion Beiter conjectured that $M(p) \leq (p+1)/2$. In 2009, this was disproved for every $p \geq 11$ by Yves Gallot and Pieter Moree. They proposed a Corrected Beiter Conjecture, namely $M(p) \leq 2p/3$. In 2009, Jia Zhao and Xianke Zhang posted on the arXiv what they thought to be a proof of this conjecture. Their work was never accepted for publication in a journal. However, in retrospect it turns out to be essentially correct, but rather sketchy at some points. Here we supply a lot more details.

The bound $M(p) \leq 2p/3$ allows us to improve some bounds of Bzdęga from 2010 for ternary cyclotomic coefficients. It also makes it possible to determine $M(p)$ exactly for three new primes p and study the fine structure of $A(pqr)$ for them in greater detail.

1. Introduction

The n^{th} cyclotomic polynomial $\Phi_n(x)$ is defined by

$$\Phi_n(x) = \prod_{\substack{1\leq j\leq n\\ (j,n)=1}} \left(x - e^{\frac{2\pi i j}{n}}\right) = \sum_{k=0}^{\varphi(n)} a_n(k)x^k,$$

where φ denotes Euler's totient function. This definition implies that

$$x^n - 1 = \prod_{d\mid n} \Phi_d(x). \tag{1}$$

The cyclotomic polynomials have integer coefficients and are irreducible over the rationals. Hence the product (1) gives a factorization of $x^n - 1$ into irreducible polynomials. We define the *height* $A(n)$ of Φ_n as

$$A(n) = \max\{|a_n(k)| : 0 \leq k \leq \varphi(n)\}.$$

As $\Phi_{p^2n}(x) = \Phi_{pn}(x^p)$ for every prime p and therefore $A(p^2n) = A(pn)$ as well as $\Phi_{2n}(x) = \Phi_n(-x)$ for $2 \nmid n$, it follows that $A(n) = A(m)$ where m is the largest odd squarefree factor of n. Further, $A(n) = 1$ whenever n has at most two distinct odd prime factors (see Lemma 2.5) and so the easiest case where we can expect non-trivial behaviour of $A(n)$ is the so-called *ternary* case $n = pqr$, where $3 \leq p < q < r$ are primes. The smallest ternary integer is 105 and one has $A(105) = 2$. In 1895, Bang [3] proved that $A(pqr) \leq p - 1$. This implies the existence of

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

Noticing that $A(105) = 2$, Bang showed that $M(3) = 2$.

The biggest open problem in the theory of ternary cyclotomic polynomials is to find a formula or efficient algorithm for computing $M(p)$ for every prime p. Since the set $\{(q, r) : p < q < r\}$ is infinite, this is non-trivial. Duda [10] gave an algorithm for determining $M(p)$. Unfortunately it requires the evaluation of coefficients of Φ_n with $n = O(p^{21})$, making its running time so bad that we could not use it to even find one new value of $M(p)$.

An easier problem is to give an upper bound for $M(p)$. In 1968, Sister Marion Beiter [4] conjectured that $A(pqr) \leq (p+1)/2$ and proved her conjecture in case $q \equiv \pm 1 \pmod p$ or $r \equiv \pm 1 \pmod p$ (a result obtained independently by Bloom [7]). As a corollary one obtains Bang's result that $M(3) = 2$. In 1978, Sister Beiter [6] went beyond this and investigated when $A(3qr) = 2$. In 1971, Sister Beiter [5] showed that $M(p) \leq p - \lfloor \frac{p+1}{4} \rfloor$. Bloom [7] showed that $M(5) = 3$. Möller [19], building on work by Emma Lehmer [17], proved that $M(p) \geq (p+1)/2$ for all p, so Beiter's conjecture would imply that $M(p) = (p+1)/2$. However, Moree and Gallot [11] disproved the Beiter conjecture for all primes $p \geq 11$. Further they proposed the following weaker conjecture.

Conjecture (Corrected Beiter Conjecture, 2009)**.** We have $M(p) \leq \frac{2}{3}p$.

In 2019, Luca et al. [18], using techniques from analytic number theory, made some partial progress.

Theorem 1.1 (Luca et al. [18])**.** *The relative density of ternary integers pqr for which $A(pqr) \leq 2p/3$ is at least* 0.925*.*

The Corrected Beiter Conjecture implies of course that $A(pqr) \leq 2p/3$ for all ternary integers.

The best general upper bound for ternary cyclotomic coefficients is due to Bzdęga [8] (improving on an earlier upper bound due to Bachman [1]), and will be given in Section 2 (Theorem 2.13). Using this bound, Zhao and Zhang [22] proved that $M(7) = 4$, thus establishing both the Corrected Beiter Conjecture and Beiter's original conjecture for $p = 7$. Up to now, no values of $M(p)$ for $p > 7$ are explicitly known.

In 2009, Lawrence [16] announced a proof of the Correct Beiter Conjecture for all primes $p > 10^6$, but details were never published. In the same year, Zhao and Zhang [23] posted a purported proof of the Corrected Beiter Conjecture on the arXiv. It builds upon and extends the methods they used to show that $M(7) = 4$ in [22], but is rather longer and more involved. Unfortunately, their paper was never published in a journal and the conjecture is still regarded as being open. However, on carefully checking the alleged proof of Zhao and Zhang, we noted that the main ideas were correct. In this paper we will establish the Corrected Beiter Conjecture.

Theorem 1.2. *We have*
$$M(p) \leq \frac{2}{3}p.$$

Corollary 1.3. *We have*
$$\lim_{p \to \infty} \frac{M(p)}{p} = \frac{2}{3}.$$

Proof. This follows on combining Theorem 1.2 and the result of Gallot and Moree [11] that given any $\varepsilon > 0$, the inequality $M(p) > (2/3 - \varepsilon)\, p$ holds for all large enough primes p. $\square$

Corollary 1.4. *We have $M(11) = 7$, $M(13) = 8$ and $M(19) = 12$.*

Proof. That $7, 8$, respectively 12 are upper bounds follows by the theorem, that they are lower bounds follows from the examples given in Table 1. $\square$

TABLE 1

p	$M(p)$	smallest n	smallest k	$a_{pqr}(k)$	source
3	2	$3\cdot 5\cdot 7$	7	-2	Bang [3]
5	3	$5\cdot 7\cdot 11$	119	-3	Bloom [7]
7	4	$7\cdot 17\cdot 23$	875	4	Zhao and Zhang [22]
11	7	$11\cdot 19\cdot 601$	34884	7	this paper
13	8	$13\cdot 73\cdot 307$	89647	8	this paper
19	12	$19\cdot 53\cdot 859$	318742	-12	this paper

For every prime p in the table, the smallest $n = pqr$ is given with $A(n) = M(p)$ (as computed by Yves Gallot). For this value of n the smallest k is given such that $|a_n(k)| = M(p)$ (as computed by Bin Zhang).

The connaisseur of the cyclotomic polynomial literature might find Table 1 look familiar. Indeed, it already appears in Gallot et al. [12] (but without the "smallest k" column). The latter paper, written shortly after the appearance of the preprint by Zhao and Zhang [23], had optimistically assumed their work to be correct. Various results in [12] are thus proved taking the Corrected Beiter Conjecture for granted. There are too many of these results to be listed here. In each case it easily follows from the proofs given whether the conjecture was assumed or not. In any case, all of the results in Gallot et al. [12] can now be regarded as proved.

We conjecture that there is a sharpening of $M(p) \le 2p/3$ possible in the sense that there exists a function $f(p)$ tending to infinity with p such that $M(p) \le 2p/3 - f(p)$ for every prime p. The growth of the function f must be rather modest as Cobeli et al. [9] showed that $M(p) > 2p/3 - 3p^{3/4}\log p$ for all primes p and $M(p) > 2p/3 - c\sqrt{p}$ for infinitely many primes p for some $c > 0$. In particular we make the following conjecture.

Conjecture. Given any real number r there exist only finitely many primes p such that $M(p) > 2p/3 - r$.

For example, if $r = 1$ we believe that the primes p satisfying $M(p) > 2p/3 - 1$ are precisely those listed in Table 1.

It seems that our conjecture cannot be proved using our method of proof of Theorem 1.2.

1.1. **On the frequency of** $A(pqr) = M(p)$**.** It is natural question how often the maximum $M(p)$ is reached. To study this it is helpful to consider the quantity

$$M(p;q) = \max\{A(pqr) : 2 < p < q < r\}, \tag{2}$$

where p and q are fixed and r ranges over the primes $> q$. Gallot et al. [12] were the first to introduce and study $M(p;q)$. They described a rather efficient finite procedure to compute it. Duda [10], using a rather geometric method, showed that if $q > 14p^{10}$, then the value of $M(p;q)$ only depends on the congruence class β of q modulo p. This value we denote by $M_\beta(p)$. Thus

$$M_\beta(p) = M(p;q), \text{ for any } q > 14p^{10} \text{ satisfying } q \equiv \beta \,(\mathrm{mod}\ p). \tag{3}$$

Duda showed further that

$$M_\beta(p) = \max\{M(p;q) : q > p,\ q \equiv \beta\,(\mathrm{mod}\ p)\},$$

and established the symmetry $M_\beta(p) = M_{p-\beta}(p)$. It follows that

$$M(p) = \max\{M_1(p), \dots, M_{\frac{p-1}{2}}(p)\}. \tag{4}$$

This formula in combination with (3) yields a finite procedure to determine $M(p)$, but unfortunately it is very inefficient. The bound $14p^{10}$ is presumably far from optimal, but it is certainly at least $\gg p^2$. This follows from the result of Gallot et al. [12] that

$$M(p;q) = \min\left\{\frac{q-1}{p}+1, \frac{p+1}{2}\right\} \text{ if } q \equiv 1 \,(\mathrm{mod}\; p). \tag{5}$$

We infer that $M_1(p) = M_{p-1}(p) = \frac{p+1}{2}$ (showing the correctness of the $\beta = 1$ column in Table 2). If q/p is small, then frequently $M(p;q) < M_\beta(p)$ and (5) gives an example of this. As mentioned earlier, Sister Beiter [4] and, independently Bloom [7], already proved that $M(p;q) \le \frac{p+1}{2}$ if $q \equiv 1 \,(\mathrm{mod}\; p)$.

It follows from (3) and Dirichlet's theorem on primes in arithmetic progression that the set of primes $q \equiv \beta \,(\mathrm{mod}\; p)$ for which $M(p;q) = M_\beta(p)$ has natural density $\frac{1}{p-1}$. Since $M_\beta(p) = M_{p-\beta}(p)$ we infer that the set of primes q for which $M(p;q) = M(p)$ has a natural density $\delta(p)$ satisfying $\delta(p) \ge \frac{2}{p-1}$.

Conjecture. Let $2 < p \le 19$ be a prime $\neq 17$. Then $M_\beta(p)$ is given in Table 2 (keeping in mind that $M_{p-\beta}(p) = M_\beta(p)$).

TABLE 2: Values of $M_\beta(p)$

$p\backslash\beta$	$M(p)$	1	2	3	4	5	6	7	8	9
3	2	**2**								
5	3	**3**	**3**							
7	4	**4**	**4**	**4**						
11	7	**6**	**6**	**7**	**7**	6				
13	8	**7**	**7**	7	**8**	**8**	7			
19	12	**10**	**10**	10	**12**	11	9	**11**	11	10

In particular, the set of primes q such that $M(p;q) = M(p)$ has density $\delta(p)$ as given in the table below.

p	3	5	7	11	13	19
$\delta(p)$	1	1	1	2/5	1/3	1/9

It follows using the next theorem that these conjectural densities are certainly *lower bounds* for $\delta(p)$, a result that improves Theorem 5 of [12] in case $p = 13$.

We define the auxiliary function

$$m(j) = \min\left\{w(j), \left\lfloor \frac{2}{3}p \right\rfloor\right\}, \text{ with } w(j) = \begin{cases} \frac{p-1}{2} + j & \text{if } j < \frac{p}{4}; \\ p - j & \text{if } \frac{p}{4} < j \le \frac{p-1}{2}; \\ w(p-j) & \text{if } j > \frac{p-1}{2}. \end{cases} \tag{6}$$

Theorem 1.5. *Let v be an entry in the p-row and β-column with $\beta \le \frac{p-1}{2}$ in Table 2. Let β^* denote the inverse of β in the interval $[1, p-1]$. We have*

$$v \le M_\beta(p) \le m(\beta^*),$$

and, moreover, if v is in boldface, then $M_\beta(p) = v$,

The final entries of the rows in Table 2 satisfy $\frac{p+1}{2} \le M_{\frac{p-1}{2}}(p) \le \min\{\frac{p+3}{2}, \lfloor \frac{2}{3}p \rfloor\}$, for example.

Without the bound $M(p) \le \frac{2}{3}p$ at hand only a substantial weaker version of Theorem 1.5 can be proven. Thus Theorem 1.5 can be seen as an application of our main result.

As a further application we generalize in Section 4 some bounds of Bzdęga (Theorem 2.13) and show that $M_\beta(p) \le m(\beta^*)$ for every odd prime p and $1 \le \beta \le p-1$ (Theorem 4.3).

There are of course more aspects to cyclotomic coefficients than discussed in this paper, for a recent survey see Sanna [21].

2. Preliminaries

Definition 2.1. Let

$$\Phi_n(x) = \sum_{k=0}^{\varphi(n)} a_n(k)x^k,$$

with $a_n(k)$ the k^{th} coefficient of the n^{th} cyclotomic polynomial. For $k < 0$ or $k > \varphi(n)$, we define $a_n(k) = 0$.

Definition 2.2. For any two distinct primes p and q let $0 < \overline{p_q} \le q-1$ be the unique integer with $\overline{p_q} \equiv p \pmod q$.

Definition 2.3. For any two distinct primes p and q let $0 < p_q^* \le q-1$ be the inverse of $p \pmod q$, i.e. the unique integer in $[1, q-1]$ with $pp_q^* \equiv 1 \pmod q$. Likewise modulo p we define q_p^* and r_p^*.

Lemma 2.4. *We have $pq + 1 = pp_q^* + qq_p^*$ for any two distinct primes p and q.*

Proof. Note that $1 < qq_p^* + pp_q^* < 2pq$ and that both modulo p and modulo q the integer $qq_p^* + pp_q^*$ equals 1 and hence, by the Chinese Remainder Theorem, also 1 modulo pq. □

The following lemma is well-known, Lam and Leung [15] is an easily accessible reference. It can also be interpreted in terms of numerical semigroups, see, e.g., Moree [20].

Lemma 2.5. *Let $p < q$ be primes. The k^{th} coefficient $a_{pq}(k)$ of Φ_{pq} satisfies*

$$a_{pq}(k) = \begin{cases} 1 & \text{if } k = up + vq \text{ for some } u \in [0,\ p_q^* - 1] \text{ and } v \in [0,\ q_p^* - 1]; \\ -1 & \text{if } k = up + vq - pq \text{ for some } u \in [p_q^*,\ q-1] \text{ and } v \in [q_p^*,\ p-1]; \\ 0 & \text{otherwise.} \end{cases}$$

Since $u \equiv kp_q^* \pmod q$ and $v \equiv kq_p^* \pmod p$, k uniquely determines u and v, so we can denote $u = [k]_p, v = [k]_q$ for every $0 \le k \le pq$. Observe that

$$[k]_p = [k']_p \iff k \equiv k' \pmod q \text{ and } [k]_q = [k']_q \iff k \equiv k' \pmod p.$$

A further result we will make use of is due to Nathan Kaplan.

Lemma 2.6 (Kaplan [14], 2007)**.** *If $p < q < r$, we have*

$$A(pqr) = A(pqs)$$

for every $s > q$ with $s \equiv \pm r \pmod{pq}$.

Corollary 2.7. *If $p < q < r_1$ are primes, there exists a prime $r > q$ such that $A(pqr_1) = A(pqr)$ and $r_p^* = p - (r_1)_p^*$.*

Proof. By Dirichlet's theorem we can choose k such that $r = -r_1 + kpq > q$ is a prime and hence $A(pqr_1) = A(pqr)$ by Lemma 2.6. As $r \equiv -r_1 \pmod p$, we have $r_p^* = p - (r_1)_p^*$. □

This lemma only allows to exchange the largest prime. There is also an generalization that does not have this restriction.

Lemma 2.8 (Bachman and Moree [2], 2011)**.** *If $r \equiv \pm s \bmod pq$ and $r > \max\{p, q\} > s \ge 1$, then $A(pqs) \le A(pqr) \le A(pqs) + 1$.*

The upper bound part we do not need, but we like to point out that it can happen that $A(pqr) = A(pqs) + 1$.

Corollary 2.9. *Let $p < q_1 < r_1$ be primes. Then there exist primes $q < r$ such that $A(pqr) \ge A(pq_1r_1)$, $q_p^* = (r_1)_p^*$ and $r_p^* = (q_1)_p^*$.*

Proof. By Dirichlet's theorem, we can choose $k \geq 1$ such that $r = q_1 + kpr_1$ is a prime. Note that $r > \max\{p, r_1\} > q_1 \geq 1$. Applying Lemma 2.8, we find $A(pq_1r_1) \leq A(prr_1) = A(pr_1r)$. Thus, we can simply take $q = r_1$. □

This corollary immediately implies the next one.

Corollary 2.10. *Let $p < q_1 < r_1$ be primes. Then there exist primes $q < r$ such that $A(pqr) \geq A(pq_1r_1)$ and $q_p^* \leq r_p^*$.*

Applying Corollary 2.9, followed by Corollary 2.7 and then Corollary 2.9 again yields the next corollary.

Corollary 2.11. *Let $p < q_1 < r_1$ be primes. Then there exist primes q, r such that $p < q < r$, $A(pqr) \geq A(pq_1r_1)$ and $r_p^* = (r_1)_p^*$, $q_p^* = p - (q_1)_p^*$.*

Using three of these four corollaries we can prove the following lemma which is crucial for our proof.

Lemma 2.12. *Let $p < q_1 < r_1$ be primes. Then there exist primes q, r such that $A(pqr) \geq A(pq_1r_1)$ and $1 \leq p - q_p^* \leq r_p^* < p - r_p^* \leq q_p^* \leq p - 1$.*

Proof. It is easy to check that the following algorithm will produce the required chain of inequalities.

`Algorithm`

Check if $\min\{q_p^*, p - q_p^*\} \leq \min\{r_p^*, p - r_p^*\}$.

If NO, swap r_p^* with q_p^* using Corollary 2.9.

Check if $q_p^* > (p-1)/2$.

If NO, swap q_p^* with $p - q_p^*$ using Corollary 2.11.

Check if $r_p* \leq (p-1)/2$.

If NO, swap r_p^* and $p - r_p^*$ using Corollary 2.7. □

The following bound plays an important role in the proof of Theorem 1.1 given in Luca et al. [18] and the proof of Theorem 1.2 given in this paper.

Theorem 2.13 (Bzdęga [8], 2009)**.** *Let $p < q < r$ be primes. Let*

$$\alpha = \min\{q_p^*,\ p - q_p^*,\ r_p^*,\ p - r_p^*\}$$

and let $0 < \beta \leq p - 1$ the unique integer with $\alpha\beta qr \equiv 1 \pmod p$. We have

$$a_{pqr}(i) \leq \min\{2\alpha + \beta,\ p - \beta\} \text{ and } -a_{pqr}(i) \leq \min\{p + 2\alpha - \beta,\ \beta\}.$$

We define a function χ that will play a major role in our proof.

Definition 2.14. Let k and m be integers, p, q and r primes satisfying $q > p$. We put

$$\chi_k(m) = \begin{cases} 1 & \text{if there exists } s \in \mathbb{Z} \text{ with } mr + q < k + 1 + spq \leq mr + q + p; \\ -1 & \text{if there exists } s \in \mathbb{Z} \text{ with } mr < k + 1 + spq \leq mr + p; \\ 0 & \text{otherwise.} \end{cases}$$

From the definition it is immediate that $\chi_k(m)$ only depends on the values of k and m modulo pq. Note that in order for $\chi_k(m)$ to be non-zero, the integer $k + 1 + spq$ has to be an element of one of two disjoint strings of p consecutive integers. In order to show that Definition 2.14 is consistent, we have to show that we cannot both have $mr + q < k + 1 + s_1pq \leq mr + q + p$ for some s_1 and $mr < k + 1 + s_2pq \leq mr + p$ for some s_2. Indeed, if both inequalities were to hold simultaneously, then it would follow that $0 < q - p < (s_1 - s_2)pq < p + q < 2q$, which is impossible.

The following theorem expresses the coefficients of Φ_{pqr} using the coefficients of Φ_{pq}, which can be calculated using Lemma 2.5, and our function χ from Definition 2.14.

Theorem 2.15 (Zhao and Zhang [22], 2010)**.** *Let $p < q < r$ be primes. Let m_0 be the smallest integer such that $m_0 r + p + q \geq k + 1 + pq$. Then*

$$a_{pqr}(k) = \sum_{m \geq m_0} a_{pq}(m)\chi_k(m).$$

The proof makes use of the identity

$$\Phi_{pqr}(x)(x^{pq} - 1)(x - 1) = \Phi_{pq}(x^r)(x^p - 1)(x^q - 1),$$

which allows one to relate a ternary coefficient to a sum of binary ones. Note that m_0 in Theorem 2.15 equals $\left\lceil \frac{k+(p-1)(q-1)}{r} \right\rceil$.

Corollary 2.16. *We have*

$$A(pqr) \leq \max_{j,k \in \mathbb{Z}} \left| \sum_{m \geq j} a_{pq}(m)\chi_k(m) \right|.$$

It turns out that the latter inequality is actually an equality [22, Lemma 2.3].

A further result of Zhao and Zhang we need is the following.

Theorem 2.17 (Zhao and Zhang [22], 2010)**.** *We have*

$$\sum_{m \geq 0} a_{pq}(m)\chi_k(m) = 0.$$

A short proof of this theorem can be given using Theorem 2.15 and the observation that the value of $\chi_k(m)$ only depends on the residue class of both k and m modulo pq.

3. Proof of the Corrected Beiter Conjecture

Our proof will mainly use the methods from the unpublished article [23] by Zhao and Zhang. Many of the ideas there are already to be found in their published paper [22] (dealing with the case $p = 7$). Their proof that $M(7) = 4$ can be regarded as a baby version of the proof we are going to present.

We start by giving a glossary of the notation introduced in the course of our proof.

Glossary

$[\cdot]$	Definition 3.1
$C_{1,1}, C_{1,2}, C_{2,1}, C_{2,2}$	Defined just below Lemma 3.2
low integer	Integer in $[0, q_p^* - 1]$
high integer	Integer in $[q_p^*, p - 1]$
I_p	{0 ,. . . , p-1}
S	Special integers (Definition 3.5)
P, P^+, P^-	Plain integers (ibid.)
N	Null integers: $N = I_p \setminus (P \cup S)$
v_0	Largest low special integer
$h(v), h_q(v)$	Definition 3.15
map f	Definition 3.24
S_0	$\{v \in S : f(v) \in P\}$
map g	Definition 3.27

In some clearly identifiable cases the interval notation $[a, b]$ is used to denote the set $\{a, a+1, \ldots, b\}$.

Since $M(2) = 1$, $M(3) = 2$, $M(5) = 3$ and $M(7) = 4$, the conjecture is true for $p \leq 7$. We will argue by contradiction and assume that there exist primes $7 < p < q_1 < r_1$ with $A(pq_1r_1) > \frac{2}{3}p$.

By Lemma 2.12 we can find primes q and r such that $A(pqr) \geq A(pq_1r_1) > \frac{2}{3}p$ and the chain of inequalities

$$1 \leq p - q_p^* \leq r_p^* < p - r_p^* \leq q_p^* \leq p - 1, \tag{7}$$

is satisfied. We will assume $A(pqr) > \frac{2}{3}p$ and arrive at a contradiction.

First, by Theorem 2.15, there have to exist integers i, j such that

$$A(pqr) = |a_{pqr}(i)| = \left| \sum_{m \geq j} a_{pq}(m)\chi_i(m) \right| > \frac{2}{3}p. \tag{8}$$

Our goal is now to show that this is impossible. The integers i, j will be fixed during the whole proof. For brevity we will denote $\chi_i(m)$ by $\chi(m)$.

From (7) it follows by Theorem 2.13 that $\alpha = p - q_p^*$, $\beta = p - r_p^*$ and so $a_{pqr}(n) < r_p^* < p/2$ for any integer n. We infer that $a_{pqr}(i)$ is negative. Therefore Theorem 2.13 yields $p - r_p^* \geq -a_{pqr}(i) > 2p/3$, and thus

$$r_p^* < \frac{p}{3}, \tag{9}$$

an inequality that will play an important role in our proof.

Since $a_{pqr}(i)$ is negative, we get from (8)

$$\sum_{m \geq j} a_{pq}(m)\chi(m) < -\frac{2}{3}p, \tag{10}$$

and from Theorem 2.17

$$\sum_{0 \leq m < j} a_{pq}(m)\chi(m) > \frac{2}{3}p. \tag{11}$$

If $a_{pq}(k)$ is non-zero, then we can write k uniquely as either $up + vq$ or $up + vq - pq$ for some $0 \leq u \leq q - 1$ and $0 \leq v \leq p - 1$ (see Lemma 2.5).

Definition 3.1. (of $[\cdot]$). For any v, let $0 \leq [v] \leq q - 1$ be the unique integer such that there exists an integer s satisfying

$$([v]p + vq)r + q < i + 1 + spq \leq ([v]p + vq)r + p + q.$$

It is not difficult to show that the set

$$\bigcup_{u=0}^{q-1} \{(up + vq)r + 1, \ldots, (up + vq)r + p\}$$

consists of pq distinct numbers and forms a complete residue system modulo pq. From this the existence and uniqueness of $[v]$ follows. Observe that $v \equiv w \pmod{p}$ implies $[v] = [w]$.

Now we point out a helpful connection between v and $v - r_p^*$.

Lemma 3.2. *Suppose that* $0 \leq u \leq q - 1$. *Then*

a) $\chi(up + vq) = 1$ *if and only if* $u = [v]$.
b) $\chi(up + vq) = -1$ *if and only if* $u = [v - r_p^*]$.

Proof.

a) This follows directly from Definitions 2.14 and 3.1.
b) An easy consequence of the congruences

$$\begin{aligned} ([v - r_p^*]p + (v - r_p^*)q)r + q &\equiv ([v - r_p^*]p + (v - r_p^*)q)r + rr_p^*q \\ &\equiv ([v - r_p^*]p + vq)r \pmod{pq}, \end{aligned}$$

that establish a connection between the two intervals occurring in Definition 2.14. ☐

We consider next when $a_{pq}(m)\chi(m)$ is non-zero. This will naturally lead to the consideration of the following four sets:

$$\begin{aligned}
C_{1,1} &= \{0 \le v \le q_p^* - 1 : j \le [v - r_p^*]p + vq \text{ and } [v - r_p^*] \le p_q^* - 1\};\\
C_{1,2} &= \{q_p^* \le v \le p - 1 : j \le [v]p + vq - pq \text{ and } [v] \ge p_q^*\};\\
C_{2,1} &= \{0 \le v \le q_p^* - 1 : [v]p + vq < j \text{ and } [v] \le p_q^* - 1\};\\
C_{2,2} &= \{q_p^* \le v \le p - 1 : [v - r_p^*]p + vq - pq < j \text{ and } [v - r_p^*] \ge p_q^*\}.
\end{aligned}$$

Let us look for example at the terms on the left-hand side of inequality (10) with $m \ge j$ and $a_{pq}(m)\chi(m) = -1$. By Lemma 2.5 we know that m can be written as either $up+vq$ or $up+vq-pq$ with $0 \le v \le p-1$ and $0 \le u \le q-1$. If $\chi(up+vq) \ne 0$ or $\chi(up+vq-pq) \ne 0$, then by Lemma 3.2 either $u = [v]$ or $u = [v - r_p^*]$. Simple considerations in this spirit then lead to the following lemma.

Lemma 3.3.
a) *We have $\chi(m) = -1$, $a_{pq}(m) = 1$ and $m \ge j$ if and only of $m = [v - r_p^*]p + vq$ with $v \in C_{1,1}$.*
b) *We have $\chi(m) = 1$, $a_{pq}(m) = -1$ and $m \ge j$ if and only if $m = [v]p + vq - pq$ with $v \in C_{1,2}$.*
c) *We have $\chi(m) = 1$, $a_{pq}(m) = 1$ and $m < j$ if and only if $m = [v]p + vq$ with $v \in C_{2,1}$.*
d) *We have $\chi(m) = -1$, $a_{pq}(m) = -1$ and $m < j$ if and only if $m = [v - r_p^*]p + vq - pq$ with $v \in C_{2,2}$.*

An important property of the elements in the C-sets is whether they are *low* or *high*.

Notation 3.4. (Low, high). If $0 \le v \le q_p^* - 1$, we will call v a *low* integer. If $q_p^* \le v \le p - 1$ we will call v a *high* integer.

Building on the C-sets we define some further ones.

Definition 3.5. Define

$$\begin{aligned}
S &= (C_{1,1} \cap C_{2,1}) \cup (C_{1,2} \cap C_{2,2}) && \text{(special integers);}\\
P^+ &= \{v \in C_{1,1} : [v] \ge p_q^*\} \cup \{v \in C_{1,2} : [v - r_p^*] \le p_q^*\} &&\\
P^- &= \{v \in C_{2,1} : [v - r_p^*] \ge p_q^*\} \cup \{v \in C_{2,2} : [v] \le p_q^*\} &&\\
P &= P^+ \cup P^- && \text{(plain integers);}\\
N &= \{0, \ldots, p-1\} \setminus (P \cup S) && \text{(null integers).}
\end{aligned}$$

The intersections $C_{1,1} \cap C_{2,1}$ and $C_{1,2} \cap C_{2,2}$ consist only of low, respectively high integers. Note that the sets S, P^+, P^- and N are mutually disjoint.

We will show that a large value of $M(p)$ leads to a large value of $|S| - |N|$ (Lemma 3.8), which we subsequently show to be impossible.

Lemma 3.6. *We have $|S| + |P^+| > \frac{2}{3}p$.*

Proof. Assume $a_{pq}(m)\chi(m) = -1$ for some $m \ge j$. It follows by Lemma 3.3 that m satisfies either $m = [v - r_p^*]p + vq$ with $v \in C_{1,1}$ or $m = [v]p + vq - pq$ with $v \in C_{1,2}$. Assume first $v \in C_{1,1}$. If $[v] \ge p_q^*$, then $v \in P^+$. If $[v] \le p_q^* - 1$ and $[v]p + vq < j$, then $v \in C_{2,1}$ and so $v \in C_{1,1} \cap C_{2,1} \subseteq S$. Hence, $v \notin S \cup P^+$ implies $[v] \le p_q^* - 1$ and $j \le [v]p + vq$ and thus $a_{pq}(m')\chi(m') = 1$ for $m' = [v]p + vq$. It follows that $a_{pq}(m)\chi(m) + a_{pq}(m')\chi(m') = 0$ and so the terms corresponding to m and m' in (10) cancel.

Next assume $m = [v]p + vq - pq$ and $v \in C_{1,2}$. Then, by a similar reasoning, either $v \in S \cup P^+$ or both $p_q^* \le [v - r_p^*]$ and $j \le m'$ with $m' = [v - r_p^*]p + vq - pq$. Again, the terms corresponding to m and m' in (10) cancel.

In order for the sum in (10) to be smaller than $-2p/3$, there must be more than $2p/3$ terms with value -1 which are not canceled like this. As we have just seen, these satisfy $v \in S \cup P^+$. Since S and P^+ are disjoint, the proof is completed. $\square$

Lemma 3.7. *We have* $|S| + |P^-| > \frac{2}{3}p$.

Proof. The proof is similar to the proof of Lemma 3.6. Assume $a_{pq}(m)\chi(m) = 1$ for some $m < j$, then by Lemma 3.3 either $v \in C_{2,1}$ or $v \in C_{2,2}$. If $v \in C_{2,1}$, then $m = [v]p + vq$ and either $v \in S \cup P^-$ or $a_{pq}(m')\chi(m') = -1$ for $m' = [v - r_p^*]p + vq$ with $m' < j$.

Similarly, if $v \in C_{2,2}$, then $m = [v - r_p^*]p + vq - pq$ and either $v \in S \cup P^-$ or $a_{pq}(m')\chi(m') = -1$ for $m' = [v]p + vq - pq$ with $m' < j$.

In both cases, the terms $a_{pq}(m)\chi(m) = 1$ cancel out against the terms $a_{pq}(m')\chi(m') = -1$ if $v \notin S \cup P^-$. By (11) and the disjointness of S and P^- it then follows that $|S| + |P^-| > \frac{2}{3}p$. $\square$

Lemma 3.8. *If* $A(pqr) > \frac{2}{3}p$, *then*

$$|S| - |N| > \frac{p}{3}. \tag{12}$$

Proof. Since by definition each v is in exactly one of the mutually disjoint sets S, P^+, P^- and N, we have

$$|S| + |P^+| + |P^-| + |N| = p. \tag{13}$$

On combining this identity with Lemma 3.6, Lemma 3.7 and (13) the proof is completed. $\square$

Lemma 3.9. *If v is both low and special, then* $[v] < [v - r_p^*] \le p_q^* - 1$.

Proof. By Definition 3.5 (S) we have $v \in C_{1,1} \cap C_{2,1}$ and so $[v - r_p^*] \le p_q^* - 1$ and $[v]p + vq < j \le [v - r_p^*]p + vq$, as desired. $\square$

Lemma 3.10. *If v is both high and special, then* $p_q^* \le [v - r_p^*] < [v]$.

Proof. By Definition 3.5 (S) we have $v \in C_{1,2} \cap C_{2,2}$. It follows that $[v - r_p^*] \ge p_q^*$ and $[v - r_p^*]p + vq - pq < j \le [v]p + vq - pq$, as desired. $\square$

In order to prove Theorem 1.2 we will derive a contradiction to the conclusion of Lemma 3.8. In principle we need to show that there can't be much more special than null integers. First we will prove a lemma which gives some bounds for integers which can be special. Afterwards, we will define an injection f from a subset of S into N and a bijection g between two distinct sets of integers where only one integer can be special. The domain and range from f and g will be disjoint. Therefore, the elements in the domain of f are not important for the difference $|S| - |N|$ and we will get $|S| - |N| \le p/3$ because of the bounds for special integers and the bijection g. First, we bound the low special integers. As there are $p - q_p^*$ integers in $[q_p^*, p - 1]$, by (7), (9) and (12) we find $p - q_p^* \le r_p^* < \frac{p}{3} < |S| - |N| < |S|$, and so there is at least one low special integer.

Notation 3.11. (v_0). Let v_0 denote the largest low special integer.

Lemma 3.12. *If $v \in S \cup P^-$ is a low integer, then $v_1 \notin S \cup P^+$ for every* $0 \le v_1 \le v - p + q_p^*$.

Proof. The assumption on v implies by Definition 3.5 (S) and Definition 3.5 (P^-), that $v \in C_{2,1}$. Hence, $[v] \le p_q^* - 1$ and $[v]p + vq < j$.

Assume for the sake of contradiction that $v_1 \in S \cup P^+$ for some such v_1. As $v_1 \le v - p + q_p^* \le v \le q_p^* - 1$, the integer v_1 is low. By Definition 3.5 (S) and Definition 3.5 (P^+) it now follows that $v_1 \in C_{1,1}$ and hence $[v_1 - r_p^*] \le p_q^* - 1$ and $j \le [v_1 - r_p^*]p + v_1 q$. We conclude that $[v]p + vq < j \le [v_1 - r_p^*]p + v_1 q$. From this it follows that $(v - v_1)q < ([v_1 - r_p^*] - [v])p$, and hence

$$(p - q_p^*)q \le (v - v_1)q < ([v_1 - r_p^*] - [v])p.$$

Using Lemma 2.4 this leads to a contradiction, since we also have

$$([v_1 - r_p^*] - [v])p \le [v_1 - r_p^*]p \le (p_q^* - 1)p = (p - q_p^*)q - p + 1, \tag{14}$$

completing the proof. ☐

Corollary 3.13. *If an integer v is both low and special, then $v_0 - p + q_p^* + 1 \le v \le v_0$.*

From this we deduce that the number of low special integers is at most $p - q_p^* \le r_p^* < \frac{p}{3} < |S|$, so there must exist high special integers.

Lemma 3.14. *If $v \in S \cup P^+$ is a low integer, we have $v_1 \notin S \cup P^-$ for every $v + r_p^* \le v_1 \le q_p^* - 1$.*

Proof. Similar to the proof of Lemma 3.12. The assumption on v implies by Definition 3.5 (S) and Definition 3.5 (P^+) that $v \in C_{1,1}$ and hence $[v - r_p^*] \le p_q^* - 1$ and $j \le [v - r_p^*]p + vq$.

Assume for the sake of contradiction that $v_1 \in S \cup P^-$ for such v_1. Since v_1 is low by assumption, we have $v_1 \in C_{2,1}$ by Definition 3.5 (S) and Definition 3.5 (P^-). Thus $[v_1] \le p_q^* - 1$ and $[v_1]p + v_1 q < j$. We conclude that $[v_1]p + v_1 q < j \le [v - r_p^*]p + vq$. From this it follows that $(v_1 - v)q < ([v - r_p^*] - [v_1])p$, which implies

$$(p - q_p^*)q \le r_p^* q \le (v_1 - v)q < ([v - r_p^*] - [v_1])p.$$

Using Lemma 2.4 this leads to a contradiction, since we also have

$$([v - r_p^*] - [v_1])p \le [v - r_p^*]p \le (p_q^* - 1)p = (p - q_p^*)q + 1 - p,$$

completing the proof. ☐

If $v \in S \cup P$ (recall Definition 3.5) we can relate $[v]$ and $[v - r_p^*]$. Our goal, however, is to obtain a contradiction to the conclusion of Lemma 3.8. This can only be reached with further information about $[v]$ and $[v - r_p^*]$ and their difference. For ease of notation we make the following definition.

Definition 3.15. (of $h(v)$ and $h_q(v)$). We put

$$h(v) = [v] - [v - r_p^*].$$

The unique integer $0 \le \beta < q$ such that $h(v) \equiv \beta \pmod q$ we denote by $h_q(v)$.

We will need a technical lemma.

Lemma 3.16. *Given any integer $0 \le v \le p - 1$, one of the following holds true.*

(a) *There exists some $\overline{q_p} \le k \le p - 1$ such that*

$$([v]p + vq)r + p + q \equiv i + 1 + k \equiv ([v - r_p^*]p + vq)r + p + \overline{q_p} \pmod{pq}, \tag{15}$$

which implies that

$$h(v)\, pr \equiv \overline{q_p} - q \pmod{pq}. \tag{16}$$

(b) *There exists some $0 \le k \le \overline{q_p} - 1$ such that*

$$([v]p + vq)r + p + q \equiv i + 1 + k \equiv ([v - r_p^*]p + vq)r + p + (\overline{q_p} - p) \pmod{pq}, \tag{17}$$

which implies that

$$h(v)\, pr \equiv \overline{q_p} - q - p \pmod{pq}. \tag{18}$$

Proof. By Definition 3.1, we have

$$([v]p + vq)r + p + q \equiv i + 1 + k_1 \pmod{pq} \text{ with } k_1 \in I_p, \tag{19}$$

By the same definition, but this time applied to $v - r_p^*$, we obtain

$$([v - r_p^*]p + vq)r + p \equiv i + 1 + k_2 \pmod{pq} \text{ with } k_2 \in I_p, \tag{20}$$

on noting that $r_p^* rq \equiv q (\operatorname{mod} pq)$. Therefore, we have

$$h(v)\, pr + q \equiv k_1 - k_2 \,(\operatorname{mod} pq). \tag{21}$$

We infer that $q \equiv k_1 - k_2 \,(\operatorname{mod} p)$. Note that $k_1 - k_2 \in [-(p-1),\ p-1]$, an interval of length smaller than $2p$. Therefore either $k_1 - k_2 = \overline{q_p}$ or $k_1 - k_2 = \overline{q_p} - p$. From (19), (20) and the new information for (21) we get (16), respectively (18). In case $k_1 - k_2 = \overline{q_p}$ we have $k_1 \geq \overline{q_p}$. In case $k_1 - k_2 = \overline{q_p} - p$, we have $k_1 \leq \overline{q_p} - 1$. On taking $k = k_1$ the proof is completed. □

Corollary 3.17. *For any integer $0 \leq v \leq p-1$, there are two possible remainders modulo q for the difference $h(v) = [v] - [v - r_p^*]$, that is $|\{h_q(v) : 0 \leq v \leq p-1\}| \leq 2$.*

This is a simple consequence of Lemma 3.16. Either $h(v)$ satisfies the congruence (16) or the congruence (18) and each of these equations has an unique solution $h(v)$ modulo q. Note that the two solutions are distinct.

Since there is at least one low special and one high special integer, the next lemma in combination with Corollary 3.17 shows that

$$|\{h_q(v) : 0 \leq v \leq p-1\}| = 2.$$

Lemma 3.18. *Let v be a low special integer and v' be a high special integer. Then $h_q(v) \neq h_q(v')$.*

Proof. Assume the two terms are congruent. By Lemma 3.9 and Lemma 3.10, $[v] < [v - r_p^*]$ and $[v' - r_p^*] < [v']$. Hence, $0 < [v - r_p^*] + [v'] - [v] - [v' - r_p^*]$, which is divisible by q by assumption and thus at least q. On the other hand, since $v \in C_{1,1}$ and $v' \in C_{2,2}$, we also have

$$h(v') - h(v) = [v - r_p^*] + [v'] - [v] - [v' - r_p^*] \leq (p_q^* - 1) + (q-1) - 0 - p_q^* = q - 2 < q,$$

which is a contradiction. □

Lemma 3.19. *Let v_1, v_2 be two special integers. Then $h(v_1) = h(v_2)$ if and only if v_1 and v_2 are both low or both high integers.*

Proof. The weaker result with identity replaced by being congruent modulo q follows from Lemma 3.18 and Corollary 3.17.

For low special integers v_1 and v_2 we have $-q < h(v_i) < 0$ by Lemma 3.9. Since the two expressions for $i = 1$ and $i = 2$ are congruent mod q, they have to be equal. For high special integers v_1 and v_2 we have $0 < h(v_i) < q$ by Lemma 3.10. Again the two expressions are congruent mod q and thus equal. □

Lemma 3.20. *Suppose that $v' \in S \cup P^-$ is high and $v' - r_p^* \in P$. Let v_1 be a low special integer. Then $v' - r_p^* \in P^+$ and $h_q(v' - r_p^*) \neq h_q(v_1)$.*

Proof. By Definition 3.5 (S) and (P^-), and since v' is high, we have $v' \in C_{2,2}$ and hence $[v' - r_p^*]p + (v' - p)q < j$ and $p_q^* \leq [v' - r_p^*]$. Thus from $v' - r_p^* < p - r_p^* \leq q_p^*$ being a low integer, we infer that $v' - r_p^* \notin P^-$ (since $v' - r_p^* \in P^-$ would imply $v \in C_{2,1}$ contradicting $p_q^* \leq [v' - r_p^*]$). Therefore, $v' - r_p^* \in P^+$ and so $v' - r_p^* \in C_{1,1}$, implying $[v' - 2r_p^*] \leq p_q^* - 1 < [v' - r_p^*]$. Since $0 \leq [v_1] < [v_1 - r_p^*] \leq p_q^* - 1$ by Lemma 3.9, we conclude that $[v_1 - r_p^*] - [v' - 2r_p^*] - [v_1] + [v' - r_p^*] > 0$.

Since $v' - r_p^* \in C_{1,1}$ and $v' \in C_{2,2}$, we have $[v' - r_p^*]p + v'q - pq < j \leq [v' - 2r_p^*]p + (v' - r_p^*)q$, and so $p([v' - r_p^*] - [v' - 2r_p^*]) < (p - r_p^*)q$. Combining the various inequalities, we deduce

$$\begin{aligned} 0 &< ([v_1 - r_p^*] - [v_1] - [v' - 2r_p^*] + [v' - r_p^*])p < (p_q^* - 1)p + (p - r_p^*)q \\ &\leq p(p_q^* - 1) + qq_p^* = pq - p + 1 < pq. \end{aligned}$$

Hence, the numbers $h(v_1)$ and $h(v' - r_p^*)$ cannot be congruent modulo q, as their difference lies in the interval $[1, q-1]$. □

Lemma 3.21. *Suppose that $v' \in S$ is high and $v' - r_p^* \notin N$. Then $v' - r_p^* \in P^+$ and $h(v') = h(v' - r_p^*)$. Moreover, $h_q(v') = h(v')$ and $h_q(v' - r_p^*) = h(v' - r_p^*)$.*

Proof. As $v' - r_p^* < p - r_p^* \leq q_p^*$, we conclude that $v' - r_p^*$ is low.

Assume first that $v' - r_p^* \in S$. By Definition 3.5 (S), $v' - r_p^* \in C_{2,1}$, so $[v' - r_p^*] \leq p_q^* - 1$. Since v' is high and special, $v' \in C_{2,2}$, so $[v' - r_p^*] \geq p_q^*$, a contradiction.

Hence, $v' - r_p^* \notin S$, so $v' - r_p^* \in P$. By Lemma 3.20 and Corollary 3.17, we know $v' - r_p^* \in P^+$ with $h(v' - r_p^*) = h(v') \pmod q$. We now show that these two numbers are equal. We have $h(v') \in [0, q-1]$ by Lemma 3.10. Further, $[v' - 2r_p^*] \leq p_q^* - 1 < [v' - r_p^*]$ by Definition 3.5 (P^+), and so also $h(v' - r_p^*) \in [0, q-1]$. The final statement follows by Definition 3.15. ☐

Lemma 3.22. *Suppose that $v' \in S \cup P^+$ is high, and $v' + r_p^* - p \in P$. Then $v' + r_p^* - p \in P^-$ and $h_q(v' + r_p^* - p) \neq h_q(v_0)$.*

Proof. The proof is similar to that given in Lemma 3.20. Since $v' \in S \cup P^+$ is high, $v' \in C_{1,2}$, so $[v'] \geq p_q^*$ and $[v']p + v'q - pq \geq j$. Since $v' + r_p^* - p \geq v' + p - q_p^* - p \geq 0$ and $v' + r_p^* - p \leq p - 1 + r_p^* - p < q_p^*$, we conclude that $v' + r_p^* - p$ is low.

Assume for a contradiction that $v' + r_p^* - p \in P^+$. Then $v' + r_p^* - p \in C_{1,1}$ by Definition 3.5 (P^+). Thus, $[(v' + r_p^* - p) - r_p^*] = [v' - p] = [v'] \leq p_q^* - 1$, a contradiction. Hence, $v' + r_p^* - p \in P^-$.

By Definition 3.5 (P^-), $v' + r_p^* - p \in C_{2,1}$. Hence, $[v' + r_p^* - p]p + (v' + r_p^* - p)q < j \leq [v']p + v'q - pq$, or, equivalently, $p([v'] - [v' + r_p^* - p]) > r_p^* q$. Since $[v_0] < [v_0 - r_p^*]$ and $[v' + r_p^* - p] \leq p_q^* - 1 < [v']$ by Lemma 3.9, it follows that both $[v_0] - [v_0 - r_p^*]$ and $[v' + r_p^* - p] - [v']$ lie in the interval $[-q+1, -1]$. Thus, if they are congruent modulo q, they have to be equal. However,

$$p([v_0 - r_p^*] - [v_0] + [v' + r_p^* - p] - [v']) < p(p_q^* - 1) - r_p^* q,$$

and the proof is finished on noticing that, by Lemma 2.4 and (7),

$$p(p_q^* - 1) - r_p^* q = pq + 1 - qq_p^* - p - r_p^* q < q(p - q_p^* - r_p^*) \leq 0.$$ ☐

Lemma 3.23. *Assume $r_p^* + q_p^* = p$. If $q_p^* \leq v' \leq p - 1$ and $v' \in P$ with $v' + r_p^* - p \in S$, then $h_q(v_0) = h_q(v')$.*

Proof. As in the previous lemma, $v' + r_p^* - p \leq p - 1 + r_p^* - p < q_p^*$, so $v' + r_p^* - p$ is low. By Definition 3.5 (S), $v' + r_p^* - p \in C_{1,1}$, so $[(v' + r_p^* - p) - r_p^*] = [v' - p] = [v'] \leq p_q^* - 1$. If $v' \in P^+$, then $v' \in C_{1,2}$ by Definition 3.5 (P^+), and hence $[v'] \geq p_q^*$, contradicting the above inequality. Hence, $v' \in P^-$ and $v' \in C_{2,2}$, so $[v' - r_p^*]p + v'q - pq < j$. Since $v' + r_p^* - p \in C_{1,1}$, we have $j \leq [v' - p]p + (v' + r_p^* - p)q = [v']p + (v' + r_p^* - p)q$. Combining these inequalities for j, we deduce $[v' - r_p^*]p + v'q - pq < [v']p + (v' + r_p^* - p)q$, which simplifies to $p\,h(v') > -r_p^* q$. By Definition 3.5 (P^-) and the definition of $C_{2,2}$, $v' \in C_{2,2}$ being high implies that $[v'] \leq p_q^* \leq [v' - r_p^*]$, and so $-q < h(v') \leq 0$.

Let v be a high special integer. If $h_q(v_0) \neq h_q(v')$, then by Corollary 3.17 and Lemma 3.19, we infer that $h_q(v) = h_q(v')$. By Lemma 3.10, $0 < h(v) < q$ and so the only possibility is $h(v) - q = h(v')$. However, then $-r_p^* q < p\,h(v') = p(h(v) - q)$. Since v is high and special, we have $[v - r_p^*] \geq p_q^*$ as $v \in C_{2,2}$, and so $-r_p^* q < p(q - 1 - p_q^* - q)$. Since by assumption $r_p^* + q_p^* = p$, the latter inequality can be rewritten as $-(p - q_p^*)q < p(-1 - p_q^*)$. This on its turn can be rewritten as $qq_p^* + pp_q^* < pq - p$. As the left-hand side equals $1 + pq$ we have obtained a contradiction. ☐

Definition 3.24. (of the map f). Define $f : I_p \to I_p$ by

$$f(v) = \begin{cases} v - r_p^* & \text{if } v \geq r_p^*; \\ v - r_p^* + p & \text{if } v \leq r_p^* - 1. \end{cases}$$

Obviously, f is a bijection.

Lemma 3.25. *If $v \in S$, then $f(v) \notin S$.*

Proof. For a contradiction assume that $f(v)$ is special.

If $f(v)$ and v are both low, then by Corollary 3.13 either both v and $v - r_p^*$ are in the interval $[v_0 - p + q_p^* + 1, v_0]$, or both v and $v - r_p^* - p$ are in this interval. In the first case we must have $r_p^* < p - q_p^*$, and in the second case $p - r_p^* < p - q_p^*$. Both of these inequalities contradict (7).

The integers v and $f(v)$ cannot be both high integers, since then their difference is at most $p - q_p^* - 1$, which by (7) is both smaller than r_p^* and $p - r_p^*$.

If one of v and $f(v)$ is high and the other low, then by Definition 3.5 (S) it would follow that $p_q^* \leq [v - r_p^*] \leq p_q^* - 1$, which is impossible. □

Definition 3.26. (of S_0). Let S_0 be the set of integers $v \in S$ with $f(v) \in P$.

For $v \in S \setminus S_0$ we have $f(v) \notin P$ (by definition) and $f(v) \notin S$ (by Lemma 3.25), and hence $f(v) \in N$.

Now we need pairs of integers from which only one can be in S_0.

Definition 3.27. (of the map g). For any integer $v \in [0, p-1]$, we define the function g by

$$g(v) = 2v_0 + r_p^* - v.$$

Note that a priori we might have $g(v) < 0$, but the corresponding values of v will not play a role in our arguments.

Lemma 3.28. *If $v \in S_0$ and $v \geq q_p^*$, and if also $0 \leq 2v_0 + r_p^* - v \leq v_0$, then $g(v) = 2v_0 + r_p^* - v$ is not in $S \cup P^+$.*

Proof. Assume for a contradiction that $g(v) \in S \cup P^+$. Either (17) or (15) is true for v_0. Assume first (17) holds for v_0. Then,

- $([v_0]p + v_0 q)r + p + q \equiv i + 1 + k_1 \pmod{pq}$ and
- $([v_0 - r_p^*]p + v_0 q)r + \overline{q_p} \equiv i + 1 + k_1 \pmod{pq}$ with $0 \leq k_1 \leq \overline{q_p} - 1$.

In particular,

$$v_0 qr + q \equiv i + 1 + k_1 \pmod{p}. \tag{22}$$

Furthermore, by Definition 3.1 and noting that $r_p^* rq \equiv q \pmod{pq}$,

- $([2v_0 - v]p + (2v_0 + r_p^* - v)q)r + p \equiv i + 1 + k_2 \pmod{pq}$ with $0 \leq k_2 \leq p - 1$.

Since by assumption $v \geq q_p^*$, it follows that $f(v) = v - r_p^*$ as $q_p^* \geq r_p^*$. Since by assumption $v \in S_0$, we infer that $f(v) = v - r_p^* \in P$ by the definition of S_0. As we assumed that (18) holds, it follows by Lemma 3.20 (with $v' = v$ and $v_1 = v_0$) that (16) (and so (15)) holds for $v - r_p^*$, and hence

- $([v - r_p^*]p + (v - r_p^*)q)r + p + q \equiv i + 1 + k_3 \pmod{pq}$ with $\overline{q_p} \leq k_3 \leq p - 1$.

Similarly (15) holds by Lemma 3.19 applied to v (which is high and special), giving

- $([v - r_p^*]p + vq)r + p + \overline{q_p} \equiv i + 1 + k_4 \pmod{pq}$ with $\overline{q_p} \leq k_4 \leq p - 1$.

The last two congruences imply that q divides $k_3 - k_4 + \overline{q_p}$. Clearly $k_3 - k_4 + \overline{q_p} \in (-p, p) \subseteq (-q, q)$, hence $k_3 = k_4 - \overline{q_p}$ and $k_3 \in [\overline{q_p}, p - 1 - \overline{q_p}]$.

From the congruences involving k_2 and k_3 and (22) we get

$$\begin{aligned} 2(i+1) + k_3 + k_2 &\equiv ([v - r_p^*]p + (v - r_p^*)q)r + p + q + ([2v_0 - v]p + (2v_0 + r_p^* - v)q)r + p \\ &\equiv 2v_0 qr + q \equiv 2(i+1) + 2k_1 - \overline{q_p} \pmod{p}, \end{aligned}$$

showing that p divides $k_3 + k_2 - 2k_1 + \overline{q_p}$. Since $k_3 + k_2 - 2k_1 + \overline{q_p} \leq p - \overline{q_p} - 1 + p - 1 + \overline{q_p} < 2p$ and $0 < \overline{q_p} - 2(\overline{q_p} - 1) + \overline{q_p} \leq k_3 + k_2 - 2k_1 + \overline{q_p}$, it follows that

$$k_3 + k_2 - 2k_1 + \overline{q_p} = p.$$

Using this, we conclude that

$$\begin{aligned} &([v-r_p^*]p+(v-r_p^*)q)r+p+q+[2v_0-v]p+(2v_0+r_p^*-v)q)r+p \\ \equiv\ & i+1+k_3+i+1+k_2 \equiv i+1+k_1+p-\overline{q_p}+i+1+k_1 \\ \equiv\ & ([v_0-r_p^*]p+v_0q)r+\overline{q_p}+p-\overline{q_p}+([v_0]p+v_0q)r+p+q \pmod{pq}, \end{aligned}$$

and thus q divides $[v-r_p^*]+[2v_0-v]-[v_0]-[v_0-r_p^*]$. Since, by Definition 3.5 (S), $v_0 \in C_{1,1}$ and $v \in C_{2,2}$, we have $[v_0-r_p^*] < p_q^* \le [v-r_p^*]$. By assumption, $g(v) \in S \cup P^+$ is low, so $2v_0-v+r_p^* \in C_{1,1}$. Hence, on also noting that $v_0 \in C_{2,1}$, we see that $[v_0]p+v_0q < j \le [2v_0-v]p+(2v_0-v+r_p^*)q < [2v_0-v]p+v_0q$ (since $g(v) \le v_0$ implies $v_0 \le v-r_p^*$), so $[v_0] < [2v_0-v]$. Thus q divides the positive number $[v-r_p^*]+[2v_0-v]-[v_0]-[v_0-r_p^*]$, and so this number is $\ge q$. From this we infer that

$$2[v-r_p^*] \ge 2(q+[v_0-r_p^*]+[v_0]-[2v_0-v]) \ge 2(q-p_q^*+1), \tag{23}$$

where the final inequality follows on noting that $[2v_0-v] \le p_q^*-1$ (a consequence of the fact that $2v_0-v+r_p^* \in C_{1,1}$). On the other hand, by applying Lemma 3.21 to v (which is allowed since $v \in S_0$ implies $f(v) \notin N$), we get

$$2[v-r_p^*] = [v]+[v-2r_p^*] \le q-1+p_q^*. \tag{24}$$

On combining (23) and (24), we obtain $2(q-p_q^*+1) \le q-1+p_q^*$, which on multiplying both sides by p gives rise to $pq+3p \le 3pp_q^*$. Since $2p/3 < p-r_p^* \le q_p^*$, it now follows on invoking Lemma 2.4 that $pq+3p \le 3pp_q^* = 3(pq+1-qq_p^*) < pq+3$, which is impossible.

The proof in the case that (16) holds for v_0 is analogous and now the congruences above with a bullet point get replaced, respectively, by

- $([v_0]p+v_0q)r+p+q \equiv i+1+k_1 \pmod{pq}$ and
- $([v_0-r_p^*]p+v_0q)r+p+\overline{q_p} \equiv i+1+k_1 \pmod{pq}$ with $\overline{q_p} \le k_1 \le p-1$,
- $([2v_0-v]p+(2v_0+r_p^*-v)q)r+p \equiv i+1+k_2 \pmod{pq}$ with $0 \le k_2 \le p-1$,
- $([v-r_p^*]p+(v-r_p^*)q)r+p+q \equiv i+1+k_3 \pmod{pq}$ with $0 \le k_3 \le \overline{q_p}-1$,
- $([v-r_p^*]p+vq)r+\overline{q_p} \equiv i+1+k_4 \pmod{pq}$ with $0 \le k_4 \le \overline{q_p}-1$.

Subtracting the latter congruence from the previous, we conclude that q divides $k_3-k_4-p+\overline{q_p}$. Since $k_3-k_4-p+\overline{q_p} \le \overline{q_p}-1-p+\overline{q_p} < 2p-p < q$ and $k_3-k_4-p+\overline{q_p} \ge -\overline{q_p}+1-p+\overline{q_p} > -q$, we infer that $k_3-k_4-p+\overline{q_p} = 0$. As $k_4 = k_3-p+\overline{q_p} \in [0, \overline{q_p}-1]$, it follows that $k_3 \in [p-\overline{q_p}, \overline{q_p}-1]$. Exactly as above, we conclude that p divides $k_3+k_2-2k_1+\overline{q_p}$. Since also

$$-p < p-\overline{q_p}-2(p-1)+\overline{q_p} \le k_3+k_2-2k_1+\overline{q_p} \le \overline{q_p}-1+p-1-2\overline{q_p}+\overline{q_p} < p,$$

we obtain $k_3+k_2-2k_1+\overline{q_p} = 0$. As before, this implies

$$\begin{aligned} &([v-r_p^*]p+(v-r_p^*)q)r+p+q+([2v_0-v]p+(2v_0+r_p^*-v)q)r+p \\ \equiv\ & i+1+k_3+i+1+k_2 \equiv i+1+k_1-\overline{q_p}+i+1+k_1 \\ \equiv\ & ([v_0-r_p^*]p+v_0q)r+p+\overline{q_p}-\overline{q_p}+([v_0]p+v_0q)r+p+q \pmod{pq}, \end{aligned}$$

and thus q divides $[v-r_p^*]+[2v_0-v]-[v_0]-[v_0-r_p^*]$. We conclude in exactly the same way as above. □

We will now finish the proof by distinguishing three cases depending on the value of v_0.

Case 1: $0 \le v_0 \le r_p^*-1$.
In this case, all low special integers lie in the interval $[0, r_p^*-1]$. Additionally, all high special integers lie in the interval $[q_p^*, p-1] \subseteq [p-r_p^*, p-1]$. By Lemma 3.25, for every $v \in [0, r_p^*-1]$ at most one of v and $v-r_p^*+p$ is special. Thus,

$$|S| \le r_p^* < \frac{p}{3}.$$

Case 2: $r_p^* \leq v_0 \leq q_p^* - r_p^* - 1$.
We structure this lengthy case by formulating four claims in the proof.

Claim 3.29. *If $v \in S$ and $v < v_0$, then $g(v) \in [q_p^*, p-1] \setminus S$ or $\{2v_0 - v - r_p^*, 2v_0 - v, 2v_0 - v + r_p^*\}$ shares an element with N.*

Proof. By Corollary 3.13, we know that $v \in [v_0 - p + q_p^* + 1, v_0]$ for any low special v. We will distinguish two ranges of v.

If $v \in [v_0 - p + q_p^* + 1, 2v_0 + r_p^* - q_p^*]$, then $g(v) = 2v_0 - v + r_p^* \in [q_p^*, p-1]$ (where we use the assumption $v_0 \leq q_p^* - r_p^* - 1$). Since $2v_0 + r_p^* - q_p^* < v_0$ by the conditions of Case 2, it follows from Lemma 3.28 that $2v_0 - v + r_p^* \notin S_0$. Applying Lemma 3.28 to $2v_0 + r_p^* - v$, we conclude that $2v_0 + r_p^* - v \notin S_0$. Thus, we have $g(v) = 2v_0 - v + r_p^* \in [q_p^*, p-1] \setminus S$ or $f(2v_0 - v + r_p^*) = 2v_0 - v \in N$ (cf. with the sentence just below Definition 3.26).

If $v \in [2v_0 + r_p^* - q_p^* + 1, v_0 - 1]$, we know that $2v_0 - v \notin S$ because $v_0 + 1 \leq 2v_0 - v \leq q_p^* - r_p^* - 1 < q_p^*$, so $2v_0 - v$ is larger than all low special integers and smaller than all high integers. Furthermore, $2v_0 - v \geq q_p^* - r_p^* - 1 \geq p - 1 - 2r_p^* \geq r_p^*$.

If $2v_0 - v \in N$ there is nothing to prove and, as $2v_0 - v \notin S$, it remains to consider the case where $2v_0 - v \in P$.

- If $2v_0 - v \in P^+$, then $[2v_0 - v] \geq p_q^*$ by Definition 3.5 (P^+). Note that $2v_0 - v + r_p^*$ is low. We have $2v_0 - v + r_p^* \notin P^+$ (as otherwise $2v_0 - v + r_p^* \in C_{1,1}$ by Definition 3.5 (P^+) and hence $[2v_0 - v] < p_q^*$). Since $2v_0 - v \in P^+$ is low, we conclude by Lemma 3.14 with $v_1 = 2v_0 - v + r_p^*$ that $v_1 \notin P^- \cup S$. All in all, $2v_0 - v + r_p^* \in N$.
- If $2v_0 - v \in P^-$, then $[2v_0 - v - r_p^*] \geq p_q^*$ by Definition 3.5 (P^-). Note that $2v_0 - v - r_p^*$ is low. We have $2v_0 - v - r_p^* \notin P^-$ (as otherwise $2v_0 - v - r_p^* \in C_{2,1}$ by Definition 3.5 (P^-) and hence $[2v_0 - v - r_p^*] < p_q^*$). Since $2v_0 - v \in P^-$ is low, we conclude by Lemma 3.12 with $v_1 = 2v_0 - v - r_p^*$ that $v_1 \notin P^+ \cup S$ (note that $0 \leq v_1 \leq 2v_0 - v - p + q_p^*$). All in all, $2v_0 - v - r_p^* \in N$. $\square$

The numbers $2v_0 - v - r_p^*$, $2v_0 - v$ and $2v_0 - v + r_p^*$ with $v \in [v_0 - p + q_p^* + 1, v_0]$ are all different. This is a consequence of this interval having length $p - q_p^* - 1 < r_p^*$ and the distance between any of the three numbers being at least r_p^*. Hence, we have found an injection of $[v_0 - p + q_p^* + 1, v_0 - 1] \cap S$ (every possible low special integer except v_0) into $N \cup [q_p^*, p-1]$. Hence we infer that

$$\frac{p}{3} < |S| - |N| \leq 1 + (p - 1 - q_p^* + 1) \leq 1 + r_p^* < \frac{p}{3} + 1. \tag{25}$$

Since the interval $[\frac{p}{3}, \frac{p}{3} + 1]$ contains exactly one integer, we conclude from these inequalities that $r_p^* = p - q_p^* = \lfloor \frac{p}{3} \rfloor$.

If $p \equiv 2 \pmod 3$, we can strengthen the inequalities from Lemma 3.6 and Lemma 3.7 to

$$|S| + |P^+| \geq \frac{2}{3}(p+1) \text{ and } |S| + |P^-| \geq \frac{2}{3}(p+1),$$

since $\frac{2}{3}(p+1)$ is the smallest integer $\geq \frac{2}{3}p$. Now the conclusion of Lemma 3.8 can be sharpened to $|S| - |N| \geq \frac{p+4}{3}$, which cannot be true by the previous paragraph by (25). Therefore the only possible case left is $p \equiv 1 \pmod 3$, whence

$$p - q_p^* = r_p^* = v_0 = \frac{p-1}{3} \tag{26}$$

by the conditions of Case 2.

Claim 3.30. *For every $v \in [0, v_0 - 1]$, we have either $v \in S$ or $f(v) \in S$. Similarly, either $v \in S$ or $g(v) \in S$.*

Proof. By Lemma 3.25 and since f is an involution at most one of v and $f(v)$ is a special integer. Note that f maps $[0, v_0-1]$ into $[q_p^*, p-1]$. Since we already deduced that $v_0 = r_p^* = (p-1)/3$, the function f is even a bijection. This immediately shows $|S| \leq r_p^*+1$. Since $|S| > \frac{p}{3}$, this inequality must be an equality, so all pairs $(v, f(v))$ must contain a special integer. This means we also need to have $|N| = 0$ and hence $S = S_0$.

Now g is also a bijection between these two intervals and $v \in S(= S_0)$ implies $g(v) \notin S$ by Lemma 3.28. Hence, either v or $g(v)$ is special. □

We get $\overline{q_p} = 3$ from $q_p^* = \frac{2p+1}{3}$. Given any $0 \leq v \leq p-1$, let $k_v \in [0, p-1]$ be the unique integer satisfying $([v]p + vq)r + p + q \equiv i + 1 + k_v \pmod{pq}$ given by Lemma 3.16. By considering k_v modulo p, we infer that $k_v \neq k_{v'}$ if $v \neq v'$. Therefore, (18) is satisfied by exactly three integers v with $0 \leq v \leq p-1$ (as $\overline{q_p} = 3$) and (16) is satisfied by exactly $p - \overline{q_p} = p-3$ integers v with $0 \leq v \leq p-1$. We will show that v_0 satisfies (18) and find three more v for which this is also the case. These four musketeers then will lead us to victory.

Claim 3.31. *For every $v' \in [q_p^*, p-1]$, we have $v' \in S \cup P^-$.*

Proof. Assume otherwise. Since N is empty, it follows that $v' \in P^+$, so by Definition 3.5 (P^+), $v' \in C_{1,2}$ and $[v'] \geq p_q^*$. Observe that $v' + r_p^* - p \leq v_0 - 1$ is low. Since $f(v' + r_p^* - p) = v' \in P$ is not special, by Claim 3.30, we know $v' + r_p^* - p \in S$. By definition, this means $v' + r_p^* - p \in C_{1,1}$ and thus $[(v' + r_p^* - p) - r_p^*] \leq p_q^* - 1$, which contradicts $[v' - p] = [v'] \geq p_q^*$. Hence, such a v' cannot exist. □

Using Claim 3.31, we can apply Lemma 3.20 to every $v \in [q_p^*, p-1]$. This implies $h_q(v) \neq h_q(v_0)$ for any $v \in [v_0+1, q_p^*-1]$. Hence, none of the integers in $[v_0+1, q_p^*-1] = [\frac{p+2}{3}, \frac{2p-2}{3}]$ satisfies $h_q(v) = h_q(v_0)$. Since $p \geq 13$ (as the prime $11 \not\equiv 1 \pmod 3$ is excluded from consideration), this interval contains $\frac{p-1}{3} > 3$ integers. Since the number of v with $h_q(v) = h_q(v_0)$ is either 3 or $p-3$, it follows that there are exactly three integers v with $h_q(v) = h_q(v_0)$. In particular, v_0 satisfies (18).

Claim 3.32. *There is a special integer v_1 with $0 \leq v_1 < v_0$.*

Proof. Assume otherwise, i.e. $v \notin S$ for every $v \in [0, v_0-1]$. By Claim 3.30, this implies $v' \in S$ for every $v' \in [q_p^*, p-1]$.

Since the two values of $h_q(v)$ appear $p-3$, respectively, three times, there must be at least one $\tilde{v} \neq v_0$ with $h_q(\tilde{v}) = h_q(v_0)$. By Lemma 3.18, such a $\tilde{v}$ cannot be in the interval $[q_p^*, p-1]$, since all of those integers are special.

In addition, we can apply Lemma 3.20 to any $v' \in [q_p^*, p-1]$ (since $v' - r_p^* \in P$ follows from $|N| = 0$). Then $h_q(v' - r_p^*) \neq h_q(v_0)$, so $\tilde{v} \notin [q_p^* - r_p^*, p-1-r_p^*] = [v_0+1, q_p^*-1]$.

We can also apply Lemma 3.22 to those v' (since $v' + r_p^* - p \in P$ follows from the assumption that no integer in $[0, v_0-1]$ is special, as $v' \in S$ and so $f(v') = v' + r_p^* - p$ is not in S and hence in P). Then $h_q(v' + r_p^* - p) \neq h_q(v_0)$, and so $\tilde{v} \notin [0, v_0-1]$.

Combining the above, we see that such a $\tilde{v}$ cannot exist. Therefore, a low special integer $v_1 \neq v_0$ must exist. As v_0 is the largest special low integer, we have $v_1 < v_0$. □

Let $v_1 < v_0$ be a low special integer, which exists by Claim 3.32. We get $f(v_1) = v_1 - r_p^* + p \notin S$ (Lemma 3.25). By Lemma 3.30, $v_1 - r_p^* + p \notin S$ implies $g(v_1 - r_p^* + p) \in S$, so $g(v_1 - r_p^* + p) = 2v_0 + 2r_p^* - v_1 - p = r_p^* - 1 - v_1 \in S$.

Since v_0 satisfies (18) and each of v_0, v_1 and $r_p^* - 1 - v_1$ is both low and special, they all satisfy (18) by Lemma 3.19. Using (26) we see that $q_p^* \leq v_1 - r_p^* + p \leq p-1$. As $v_1 - r_p^* + p \notin S$ and N is empty, we conclude that $v_1 - r_p^* + p \in P$. Recalling that $v_1 \in S$, it now follows by Lemma 3.23 that also $v_1 - r_p^* + p$ satisfies (18). We have $\max\{v_1, r_p^* - 1 - v_1\} < v_0 < v_1 - r_p^* + p$, and thus if two of these four integers are equal, then necessarily $v_1 = r_p^* - 1 - v_1$ and so $v_1 = \frac{p-4}{6}$. However, v_1 is not an integer since $p-4$ is odd. Thus we have identified four integers in I_p satisfying (18), giving rise to a contradiction.

Case 3: $q_p^* - r_p^* \leq v_0 \leq q_p^* - 1$.
Let v be any high special integer. If $v \notin S_0$, then $f(v) \in N$, so v does not contribute to the difference $|S| - |N|$ and hence $|S| - |N| \leq |S_0|$. It remains to deal with those v that are in S_0, which we will do by considering two v-ranges separately.

If $q_p^* \leq v \leq v_0 + r_p^*$, then $v_0 - r_p^* + 1 \leq q_p^* - r_p^* \leq v - r_p^* \leq v_0$. Moreover, $v \in S_0$ (by assumption), so $f(v) \in P$ and by Lemma 3.20, we even have $f(v) \in P^+$. Thus, we can restrict f to a smaller domain, giving rise to a map $\tilde{f} : S_0 \cap [q_p^*, v_0 + r_p^*] \to P^+ \cap [v_0 - r_p^* + 1, v_0]$.

If $v_0 + r_p^* + 1 \leq v \leq p - 1$, then $g(v) = 2v_0 + r_p^* - v \in [v_0 - r_p^* + 1, v_0]$ (since $2v_0 + r_p^* - p + 1 \geq v_0 + q_p^* - r_p^* + r_p^* - p + 1 \geq v_0 - r_p^* + 1$) and hence $2v_0 + r_p^* - v \notin S \cup P^+$ by Lemma 3.28. Thus, we have $\tilde{g} : S_0 \cap [v_0 + r_p^* + 1, p - 1] \to [v_0 - r_p^* + 1, v_0]$ with $\mathrm{Im}(\tilde{g})$ and $S \cup P^+$ being disjoint.

Observe that the domains of $\tilde{f}$ and $\tilde{g}$ cover $[q_p^*, p-1] \cap S_0$ and thus they cover every high integer in S_0. Also, the ranges of $\tilde{f}$ and $\tilde{g}$ are distinct, since $\mathrm{Im}(\tilde{f}) \subseteq P^+$, whereas $\tilde{g}(v) \notin P^+$. All low integers in S_0 are contained in $[v_0 - p + q_p^* + 1, v_0] \subseteq [v_0 - r_p^* + 1, v_0]$ by Corollary 3.13. Hence, the map

$$h : S_0 \to [v_0 - r_p^* + 1, v_0], \quad v \mapsto \begin{cases} v & \text{for } v \in [0, q_p^* - 1]; \\ \tilde{f}(v) & \text{for } v \in [q_p^*, v_0 + r_p^*]; \\ \tilde{g}(v) & \text{for } v \in [v_0 + r_p^* + 1, p - 1], \end{cases}$$

is injective, and it follows that $|S| - |N| \leq |S_0| \leq r_p^* < \frac{p}{3}$.

Combining the three cases above we obtain $|S| - |N| < \frac{p}{3}$ for every possible v_0. By Lemma 3.8 it then follows that $A(pqr) \leq \frac{2}{3}p$ and thus the corrected Sister Beiter cyclotomic coefficient conjecture is proven.

3.1. **On the restriction $p \geq 11$.** Note that we really used $p \geq 11$ in Case 2, as for our argument the number of integers in $\left[\frac{p+2}{3}, \frac{2p-2}{3}\right]$ has to exceed 3. This is not true for $p = 7$ (and neither for $p = 11$, but $11 \not\equiv 1 \pmod 3$). Nevertheless, it is possible to finish the proof with very similar arguments for $p = 7$, cf. Zhao and Zhang [22]. For $p \in \{3, 5\}$ it immediately follows from Theorem 2.13 that $M(p) \leq 2p/3$.

3.2. **Establishing the weaker bound $M(p) \leq (2p+1)/3$.** If one is satisfied with proving that $M(p) \leq \frac{2p+1}{3}$, a shorter proof is possible. In Case 2, after establishing that $q_p^* = \frac{2p+1}{3}$, one then merely concludes using Theorem 1.5 that $M(p; q) \leq f(\frac{2p+1}{3}) = f(\frac{p-1}{3}) = \frac{2p+1}{3}$. Further, there is no need to formulate and prove Lemma 3.22 and Lemma 3.23.

4. Improvement of some bounds of Bzdęga

The ternary coefficient bounds of Bzdęga given in Theorem 2.13 are quite useful. Combination of our main result with his, then leads to the following improvement.

Theorem 4.1. *Let $p < q < r$ be primes. Let*

$$\alpha = \min\{q_p^*,\ p - q_p^*,\ r_p^*,\ p - r_p^*\}$$

and let $0 < \beta \leq p - 1$ the unique integer with $\alpha\beta qr \equiv 1 \pmod p$. We have

$$a_{pqr}(i) \leq \min\{2\alpha + \beta,\ p - \beta, 2p/3\} \text{ and } -a_{pqr}(i) \leq \min\{p + 2\alpha - \beta,\ \beta, 2p/3\}.$$

Recall the definition (6) of m and w. Using Bzdęga's bounds the following upper bound for $M(p;q)$ can be derived.

Theorem 4.2 (Gallot et al. [12], 2011)**.** *Let $p<q$ be primes with $q\equiv\beta\,(\mathrm{mod}\,p)$. Then $M(p;q)\le M_\beta(p)\le w(\beta^*)$.*

This in combination with our main result leads to the following sharpening.

Theorem 4.3. *Let $p<q$ be primes with $q\equiv\beta\,(\mathrm{mod}\,p)$. Then $M(p;q)\le M_\beta(p)\le m(\beta^*)$.*

Since $\#\{1\le j\le p-1 : m(j)<w(j)\}$ asymptotically grows as $p/6$, Theorem 4.3 is a true improvement of Theorem 4.2.

5. The proof of Theorem 1.5

Let v be a non-zero entry in the p-row and β-column with $\beta\le\frac{p-1}{2}$ in Table 2. By Theorem 4.3 we have $M_\beta(p)\le m(\beta^*)$. It remains to establish the lower bound $M_\beta(p)\ge v$. Since $M_\beta(p)\ge M(p;q)$ for $q\equiv\beta\,(\mathrm{mod}\,p)$, it is enough for the non-boldface cases to find one example with $M(p;q)=v$ with $q\equiv\beta\,(\mathrm{mod}\,p)$. This also holds for the boldface cases where $v=M(p)$. We will not give explicit examples, but note that the reader can work some out from Table 1. However, more satisfactory than finding one example, is to find a construction which yields $M(p;q)=v$ with $q\equiv\beta\,(\mathrm{mod}\,p)$ for all primes q large enough. Usually the results we quote below rest on constructions given in the indicated references, e.g., in [11] one finds a construction for $M_5(13)\ge 8$. In the preprint of Gallot et al. [13] more details of the construction are in general supplied than in the published version [12].

By [12, Thm. 27] we have $M_1(p)=M_2(p)=\frac{p+1}{2}$, and so we may assume that $\beta\ge 3$.

We finish the proof by discussing the six relevant primes individually.

$p=3$. If $q>3$ is a prime, then $M(3;q)=2$ [12, Thm. 17].

$p=5$. If $q>3$ is a prime, then $M(5;q)=3$ [12, Thm. 28].

$p=7$. If $q>13$ is a prime, then $M(7;q)=4$ [12, Thm. 32].

$p=11$. The result for $p=11$ follows from [12, Thm. 36] (which assumes the Corrected Sister Beiter conjecture to be true).

$p=13$. Theorem 4 of [11] (together with the corresponding Table 1 in that paper) shows that $M_5(13)=8$.

$p=19$. Theorem 4 of [11] (together with the corresponding Table 1 in that paper) shows that $M_8(19)\ge 11$. Lemma 38 of [12] together with $M(19)\le 12$ shows that $M_4(19)=12$ (and hence $M(19)=12$).

Acknowledgment. Work on this paper was started during an internship of the first and third author and finished during an internship of the fourth and fifth author at the Max Planck Institute for Mathematics (MPIM) in Bonn with the second author in September 2015, respectively September 2022. The first and third author made a good start with clarifying the argument of Zhao and Zhang, the fourth and fifth author finished this process. The second author polished the write-up, wrote the introduction, and added the material on applications.

The second author thanks the administration and Christian Blohmann for their support in organizing the internships. The remaining authors like to thank MPIM for hosting them and the hospitality. Thanks are also due for Jia Zhao for supporting this new version of his purported proof with Xianke Zhang. Yves Gallot and Bin Zhang kindly helped with the computations in Table 1. Table 2 is based on a lot of computational work by Robert Wilms and, especially, Yves Gallot. Alessandro Languasco helped with some LaTeX issues we had. Gennady Bachman pointed out the relevance of [2].

References

[1] G. Bachman, On the coefficients of ternary cyclotomic polynomials, *J. Number Theory* **100** (2003), 104–116.
[2] G. Bachman and P. Moree, On a class of ternary inclusion-exclusion polynomials, *Integers* **11** (2011), A8, 14 pp.
[3] A.S. Bang, Om Lingingen $\Phi_n(x) = 0$, *Tidsskr. Math.* **6** (1895), 6–12.
[4] Sister M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial $F_{pqr}(x)$, *Amer. Math. Monthly* **75** (1968), 370–372.
[5] Sister M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial F_{pqr}. II, *Duke Math. J.* **38** (1971), 591–594.
[6] Sister M. Beiter, Coefficients of the cyclotomic polynomial $F_{3qr}(x)$, *Fibonacci Quart.* **16** (1978), 302–306.
[7] D.M. Bloom, On the coefficients of the cyclotomic polynomials, *Amer. Math. Monthly* **75** (1968), 372–377.
[8] B. Bzdęga, Bounds on ternary cyclotomic coefficients, *Acta Arith.* **144** (2010), 5–16.
[9] C. Cobeli, Y. Gallot, P. Moree and A. Zaharescu, Sister Beiter and Kloosterman: a tale of cyclotomic coefficients and modular inverses, *Indag. Math. (N.S.)* **24** (2013), 915–929.
[10] D. Duda, The maximal coefficient of ternary cyclotomic polynomials with one free prime, *Int. J. Number Theory* **10** (2014), 1067–1080.
[11] Y. Gallot and P. Moree, Ternary cyclotomic polynomials having a large coefficient, *J. Reine Angew. Math* **632** (2009), 106–125.
[12] Y. Gallot, P. Moree and R. Wilms, The family of ternary cyclotomic polynomials with one free prime, *Involve* **4** (2011), 317–341.
[13] Ibidem, Preprint 2010-11, Max-Planck-Institut fürr Mathematik, Bonn, 2010, available at `http://www.mpim-bonn.mpg.de/node/263`. A longer version (32 pp.) of [12] with some proofs given in greater detail.
[14] N. Kaplan, Flat cyclotomic polynomials of order three, *J. Number Theory* **127** (2007), 118–126
[15] T.Y. Lam and K.H. Leung, On the cyclotomic polynomial $\Phi_{pq}(X)$, *Amer. Math. Monthly* **103** (1996), 562–564.
[16] B. Lawrence, Bounding the coefficients of $\Phi_{pqr}(x)$, Joint Mathematics Meeting of the AMS/MAA (2009), 1046–11–1150.
[17] E. Lehmer, On the magnitude of the coefficients of the cyclotomic polynomial, *Bull. Amer. Math. Soc.* **42** (1936), 389–392.
[18] F. Luca, P. Moree, R. Osburn, S. Saad Eddin and A. Sedunova, Constrained ternary integers, *Int. J. Number Theory* **15** (2019), 407–431.
[19] H. Möller, Über die Koeffizienten des n-ten Kreisteilungspolynoms, *Math. Z.* **119** (1971), 33–40.
[20] P. Moree, Numerical semigroups, cyclotomic polynomials, and Bernoulli numbers, *Amer. Math. Monthly* **121** (2014), 890–902.
[21] C. Sanna, A survey on coefficients of cyclotomic polynomials, *Expo. Math.* **40** (2022), 469–494.
[22] J. Zhao and X. Zhang, Coefficients of ternary cyclotomic polynomials, *J. Number Theory* **130** (2010), 2223–2237.
[23] J. Zhao and X. Zhang, A proof of the Corrected Beiter conjecture, arXiv:0910.2770 (unpublished).

(B. Juran) Department of Mathematical Sciences, Universitetsparken 5, 2100 København Ø, Denmark
Email address: `bj@math.ku.dk`

(P. Moree) Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany
Email address: `moree@mpim-bonn.mpg.de`

(A. Riekert) Applied Mathematics: Institute for Analysis and Numerics, University of Münster, Orleans-Ring 10, D-48149 Münster, Germany
Email address: `ariekert@uni-muenster.de`

(D. Schmitz) Fachbereich Mathematik, Technische Universität Darmstadt, Schlossgartenstrasse 7, D-64289 Darmstadt, Germany
Email address: `david.schmitz@stud.tu-darmstadt.de`

(J. Völlmecke) Rheinische Friedrich-Wilhelms-Universität Bonn, Regina-Pacis-Weg 3, D-53113 Bonn, Germany
Email address: `julian.voellmecke@uni-bonn.de`