The family of ternary cyclotomic polynomials with one free prime

Yves Gallot, Pieter Moree and Robert Wilms

Abstract

A cyclotomic polynomial $\Phi_n(x)$ is said to be ternary if $n = pqr$ with p, q and r distinct odd primes. Ternary cyclotomic polynomials are the simplest ones for which the behaviour of the coefficients is not completely understood. Here we establish some results and formulate some conjectures regarding the coefficients appearing in the polynomial family $\Phi_{pqr}(x)$ with $p < q < r$, p and q fixed and r a free prime.

1 Introduction

The n-th cyclotomic polynomial $\Phi_n(x)$ is defined by

$$\Phi_n(x) = \prod_{\substack{1\le j\le n\\(j,n)=1}} (x - \zeta_n^j) = \sum_{k=0}^{\infty} a_n(k)x^k,$$

with ζ_n a n-th primitive root of unity (one can take $\zeta_n = e^{2\pi i/n}$). It has degree $\varphi(n)$, with φ Euler's totient function. We write $A(n) = \max\{|a_n(k)| : k \ge 0\}$, and this quantity is called the height of $\Phi_n(x)$. It is easy to see that $A(n) = A(N)$, with $N = \prod_{p|n,\ p>2} p$ the odd squarefree kernel. In deriving this, one uses the observation that if n is odd, then $A(2n) = A(n)$. If n has at most two distinct odd prime factors, then $A(n) = 1$. If $A(n) > 1$, then we necessarily must have that n has at least three distinct odd prime factors. Thus for $n < 105$ we have $A(n) = 1$. It turns out that $A(3 \cdot 5 \cdot 7) = 2$ with $a_{105}(7) = -2$. Thus the easiest case where we can expect non-trivial behaviour of the coefficients of $\Phi_n(x)$ is the ternary case, where $n = pqr$, with $2 < p < q < r$ odd primes. In this paper we are concerned with the family of ternary cyclotomic polynomials

$$\{\Phi_{pqr}(x)|r > q\}, \tag{1}$$

where $2 < p < q$ are fixed primes and r is a 'free prime'. Up to now in the literature the above family was considered, but with also q free. The maximum coefficient (in absolute value) that occurs in that family will be denoted by $M(p)$, thus $M(p) = \max\{A(pqr) : p < q < r\}$, with $p > 2$ fixed. Similarly we define

Mathematics Subject Classification (2000). 11B83, 11C08

$M(p;q)$ to be the maximum coefficient (in absolute value) that occurs in the family (1), thus $M(p;q) = \max\{A(pqr) : r > q\}$, with $2 < p < q$ fixed primes. Example. Bang [5] proved that $M(p) \le p-1$. Since $a_{3\cdot 5\cdot 7}(7) = -2$ we infer that $M(3) = 2$. Using $a_{105}(7) = -2$ and $M(3) = 2$, we infer that $M(3;5) = 2$.

Let $\mathcal{A}(p;q) = \{a_{pqr}(k) | r > q,\ k \ge 0\}$ be the set of coefficients occurring in the polynomial family (1).

Theorem 1 *We have* $\mathcal{A}(p;q) = [-M(p;q), M(p;q)] \cap \mathbb{Z}$.

This shows the relevance of understanding $M(p;q)$. Let us first recall some known results concerning the related function $M(p)$. Here we know thanks to Bachman [1], who very slightly improved on an earlier result in [7], that $M(p) \le 3p/4$. In 1968 it was conjectured by Sister Marion Beiter [6] (see also [7]) that $M(p) \le (p+1)/2$. She proved it for $p \le 5$. The first to show that Beiter's conjecture is false seems to have been Eli Leher (in his PhD thesis), who gave the counter-example $a_{17\cdot 29\cdot 41}(4801) = -10$, showing that $M(17) \ge 10 > 9 = (17+1)/2$. Gallot and Moree [13] provided infinitely many counter-examples for the case $p = 17$ and in fact for every $p \ge 11$. Moreover, they have shown that for every $\epsilon > 0$ and p sufficiently large $M(p) > (\frac{2}{3} - \epsilon)p$. They also proposed the Corrected Beiter Conjecture: $M(p) \le 2p/3$. The implications of their work for $M(p;q)$ are described in Section 4.

Zhao and Zhang [21] showed that $M(7) = 4$, thus establishing the Beiter Conjecture for $p = 7$. In a later paper they eastablished the Corrected Beiter Conjecture:

Theorem 2 Zhao and Zhang [22]. *We have* $M(p) \le 2p/3$.

This result together with some computer computation allows on to extend the list of exactly known values of $M(p)$ (see Table 1). For a given prime p by 'smallest n', we mean the smallest integer n satisfying $A(n) = M(p)$ and with p as its smallest prime divisor.

TABLE 1

p	$M(p)$	smallest n
3	2	$3\cdot 5\cdot 7$
5	3	$5\cdot 7\cdot 11$
7	4	$7\cdot 17\cdot 23$
11	7	$11\cdot 19\cdot 601$
13	8	$13\cdot 73\cdot 307$
19	12	$19\cdot 53\cdot 859$

It is not known whether there is a finite procedure to determine $M(p)$. On the other hand, it is not difficult to see that there is such a procedure for $M(p;q)$.

Theorem 3 *Given primes* $2 < p < q$, *there is a finite procedure to determine* $M(p;q)$.

A further question that arises is how often the maximum value $M(p)$ is assumed. Here we have the following theorem.

Theorem 4 *Given primes $2 < p < q$, there exists a prime q_0 with $q_0 \equiv q (\bmod p)$ and an integer d such that $M(p,q) \leq M(p,q_0) = M(p,q')$ for every prime $q' \geq q_0$ satisfying $q' \equiv q_0 (\bmod d \cdot p)$. In particular the set of primes q with $M(p;q) = M(p)$ has a subset having a positive natural density.*

A weaker result in this direction, namely that for a fixed prime $p \geq 11$, the set of primes q such that $M(p;q) > (p+1)/2$ has a subset of positive natural density, follows from the work of Gallot and Moree [13] (recall that $M(p) > (p+1)/2$ for $p \geq 11$).

Unfortunately, the proof of Theorem 4 gives a lower bound for the density that seems to be far removed from the true value. In this paper we present some constructions that allow one to obtain much better bounds for the density for small p.

Theorem 5 *Let $2 < p \leq 19$ be a prime with $p \neq 17$. Then the set of primes q such that $M(p;q) = M(p)$ has a subset having natural density $\delta(p)$ as given in the table below.*

TABLE 2

p	3	5	7	11	13	19
$\delta(p)$	1	1	1	2/5	1/12	1/9

Numerical experimentation suggests that the set of primes q such that $M(p;q) = M(p)$ has a natural density $\delta(p)$ as given in the above table, except when $p = 13$ in which case numerical experimentation suggests $\delta(13) = 1/3$.

In order to prove Theorem 5, we will use the following theorem dealing with $2 < p \leq 7$.

Theorem 6 *For $2 < p \leq 7$ and $q > p$ we have $M(p;q) = (p+1)/2$, with as only exception $M(7;13) = 3$.*

The fact that $M(7;13) = 3$ can be explained. Indeed, it turns out that if $ap+bq = 1$ for small (in absolute value) integers a and b, then $M(p;q)$ is small. For example, one has the following result.

Theorem 7 *If $p \geq 5$ and $2p-1$ is a prime, then $M(p;2p-1) = 3$.*

This result and similar ones are established in Section 10.

Our main conjecture on $M(p;q)$ is the following one.

Conjecture 1 *Given a prime p, there exists an integer d and a function $g : (\mathbb{Z}/d\mathbb{Z})^* \to \mathbb{Z}_{>0}$ such that for some $q_0 > d$ we have for every prime $q \geq q_0$ that $M(p;q) = g(\overline{q})$, where $1 \leq \overline{q} < d$ satisfies $q \equiv \overline{q} (\bmod d)$. The function g is symmetric, that is we have $g(\alpha) = g(d-\alpha)$.*

The smallest integer d with the above properties, if it exists, we call the *ternary conductor* $\mathfrak{f}_p$. The corresponding smallest choice of q_0 (obtained on setting $d = \mathfrak{f}_p$) we call the *ternary minimal prime.* For $p = 7$ we obtain, e.g., $\mathfrak{f}_7 = 1$ and $q_0 = 17$ (by Theorem 6). Theorem 6 can be used to obtain the following observation concerning the ternary conductor.

Theorem 8 *If $2 < p \leq 7$, then the ternary conductor exists and we have $\mathfrak{f}_p = 1$. If $p \geq 11$ and $\mathfrak{f}_p$ exists, then $p|\mathfrak{f}_p$.*

While Theorem 4 only says that the set of primes q with $M(p;q) = M(p)$ has a subset having a positive natural density, Conjecture 1 implies that the set actually has a natural denisty in $\mathbb{Q}_{>0}$ which can be easily explicitly computed assuming that we know the function g explicitly. In order to establish this implication one can invoke a quantitative form of Dirichlet's prime number theorem to the effect that, for $(a,d) = 1$, we have, as x tends to infinity,

$$\sum_{p \leq x,\ p \equiv a (\mathrm{mod}\ d)} 1 \sim \frac{x}{\varphi(d) \log x}.$$

This result implies that asymptotically the primes are equidistributed over the primitive congruence classes modulo d. (Recall that Dirichlet's prime number theorem, Dirichlet's theorem for short, says that each primitive residue class contains infinitely many primes.)

The main tool in this paper is Kaplan's lemma and is presented in Section 6. The material in that section (except for Lemma 8 which is new), is taken from [14].

The above summary of results makes clear how limited presently our knowledge of $M(p;q)$ is. For the benefit of the interested reader we present a list of open problems in the final section.

2 Proof of Theorem 4

In this section we define for coprime positive not necessary prime integers p, q, r the polynomial

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

Here we do not assume $p < q < r$. Hence we have the symmetry $\Phi'_{p,q,r} = \Phi'_{p,r,q}$. Analogously to $A(pqr)$ and $M(p;q)$ we define the following quantities:

$$A'(p,q,r) = \max\{|a'_{p,q,r}(k)| : k \geq 0\}, M'(p;q) = \max\{A'(p,q,r) : r \geq 1\}$$

$$\text{and } M'(p) = \max\{M'(p;q) : q \geq 1\}$$

We have $\Phi_{pqr} = \Phi'_{p,q,r}$ if p, q, r are primes with $p < q < r$. Hence we have $A(pqr) = A'(p,q,r)$ in this case.

Lemma 1 *We have:*

$$A'(p,q,r_1) \leq A'(p,q,r_2) \textit{ for } r_2 \equiv r_1 (\mathrm{mod}\ pq) \textit{ and } r_1 < r_2$$

$$A'(p,q_1,r) \leq A'(p,q_2,r) \textit{ for } q_2 \equiv q_1 (\mathrm{mod}\ pr) \textit{ and } q_1 < q_2$$

For the proof we merely refer to the first part of the proof of Theorem 2 in [15], because in this part of the proof the assumption that q, r are primes with $r > q$ is not needed.

Lemma 2 *If p is a prime, then $M'(p) = M(p)$. If q is also a prime with $q > p$ then $M'(p;q) = M(p;q)$.*

Proof. Let $p < q$ be primes. Assume $M'(p;q) = A'(p,q,r)$, where r is not necessary a prime. By Dirichlet's theorem we can find a prime r' satisfying $r' \equiv r (\text{mod } pq)$ and $r' > \max(q,r)$. Therefore we have by Lemma 1:

$$M'(p;q) = A'(p,q,r) \leq A'(p,q,r') = A(p,q,r') \leq M(p;q).$$

Since $M(p;q) \leq M'(p;q)$ is trivial, we have $M'(p;q) = M(p;q)$. Now let only p be a prime. Assume $M'(p) = A'(p,q,r)$, where q and r are not necessary primes. Again by Dirichlet's theorem we find a prime q' with $q' \equiv q (\text{mod } pr)$ and $q' > \max(p,q)$. Using Lemma 1 we have:

$$M'(p) = A'(p,q,r) \leq A'(p,q',r) \leq M'(p,q') = M(p,q') \leq M(p).$$

Since $M(p) \leq M'(p)$ is trivial, we have $M'(p) = M(p)$. □

Proof of Theorem 4. We set $q_1 := q$. Let r_i be a positive integer satisfying $M'(p;q_i) = A'(p,q_i,r_i)$. Using Lemma 1 we deduce:

$$M'(p;q_1) = A'(p,q_1,r_1) \leq A'(p,q_2,r_1) \leq A'(p,q_2,r_2) = M'(p,q_2),$$

where $q_2 = q_1 + pr_1$. By the same argument the sequence $q_1, q_2, q_3, \ldots$ with $q_{i+1} = q_i + pr_i$ satisfies:

$$M'(p;q_1) \leq M'(p;q_2) \leq M'(p;q_3) \leq \ldots$$

Since $M'(p;q) \leq M'(p) = M(p)$ and $M(p)$ is finite, as was known already in the 19th century, there are only finitely many different values for $M'(p;q)$. Hence there is an index k such that $M'(p;q_k) = M'(p;q_{k+i})$ for all $i \geq 0$. That means:

$$M'(p;q_k) = A'(p,q_k,r_k) = A'(p,q_{k+1},r_k) = A'(p,q_{k+1},r_{k+1}) = M'(p,q_{k+1}),$$

and by induction $A'(p,q_{k+i},r_k) = A'(p,q_{k+i},r_{k+i})$. Therefore we can assume $r_{k+i} = r_k$ for $i \geq 0$. Then we have $q_{k+i} = q_k + i \cdot pr_k$. We set $q_0 := q_k$ and $d := r_k$. Certainly we have $q_0 \equiv q (\text{mod } p)$. Let $q' \geq q_0$ be a prime with $q' \equiv q_0 (\text{mod } d \cdot p)$. There must be an integer m such that $q' = q_{k+m}$. Since $M'(p;q) = M(p;q)$ by Lemma 2 we have:

$$M(p;q_1) \leq M(p;q_0) = M(p;q').$$

Applying this to $M(p;q_1)$ with $M(p;q_1) = M(p)$, we get infinitely many primes of the form $q_i = q_1 + i \cdot pr_1$ satisfying $M(p;q_i) = M(p)$. □

3 The bounds of Bachman and Bzdęga

Let q^* and r^*, $0 < q^*, r^* < p$ be the inverses of q and r modulo p respectively. Set $a = \min(q^*, r^*, p - q^*, p - r^*)$. Put $b = \max(\min(q^*, p - q^*), \min(r^*, p - r^*))$. In the sequel we will use repeatedly that $b \geq a$. Bachman in 2003 [1] showed that

$$A(pqr) \leq \min(\frac{p-1}{2} + a, p - b). \tag{2}$$

This was more recently improved by Bzdęga [10] who showed that

$$A(pqr) \leq \min(2a+b, p-b). \tag{3}$$

It is not difficult to show that $\min(2a+b,p-b) \leq \min(\frac{p-1}{2}+a,p-b)$ and thus Bzdęga's bound is never worse than Bachman's and in practice often strict inequality holds.

Note that if $q \equiv \pm 1(\text{mod } p)$, then (2) implies that $A(pqr) \leq (p+1)/2$, a result due to Sister Beiter [6] and, independently, Bloom [9].

We like to remark that Bachman and Bzdęga define b as follows:

$$b = \min(b_1, p-b_1),\ ab_1qr \equiv 1(\text{mod } p),\ 0 < b_1 < p.$$

It is an easy exercise to see that our definition is equivalent with this one.

Both (2) and (3) give rise to the same upper bound $f(q^*)$ for $M(p;q)$ as we will show. Write $q^* \equiv j(\text{mod } p)$, $r^* \equiv k(\text{mod } p)$ with $1 \leq j,k \leq p-1$. Thus the right hand side of both (2) and (3) are functions of j and k, which we denote by $GB(j,k)$, respectively $BB(j,k)$.

Lemma 3 *Let* $1 \leq j \leq p-1$. *We have*

$$\max_{1\leq k\leq p-1} GB(j,k) = \max_{1\leq k\leq p-1} BB(j,k) = f(j), \text{ with}$$

$$f(j) = \begin{cases} (p-1)/2+j & \textit{if } j < p/4; \\ p-j & \textit{if } p/4 < j \leq (p-1)/2; \\ f(p-j) & \textit{if } j > (p-1)/2. \end{cases}$$

Proof. Since the problem is symmetric under replacing j by $p-j$, w.l.o.g. we may assume that $j \leq (p-1)/2$. If $j < p/4$, then

$$GB(j,k) \leq \frac{p-1}{2} + a \leq \frac{p-1}{2} + j = GB(j,j) = f(j).$$

If $j > p/4$, then

$$GB(j,k) \leq p-b \leq p-a \leq p-j = GB(j,j) = f(j).$$

Note that

$$f(j) = \begin{cases} BB(j, \frac{p+1}{2}-j) & \text{if } j < p/4; \\ BB(j,j) & \text{if } j > p/4. \end{cases}$$

Since $BB(j,k) \leq GB(j,k) \leq f(j)$ we are done. □

Theorem 9 *Let* $2 < p < q$. *Then* $M(p;q) \leq f(q^*)$.

Proof. By (3) and the definition of $BB(j,k)$ we have

$$M(p;q) \leq \max_{1\leq k\leq p-1} BB(q^*,k) = f(q^*),$$

completing the proof. □

Lemma 3 shows that using either (2) or (3), we cannot improve on the upper bound given in Theorem 9. Note that

$$M(p) \leq \max_{1\leq j\leq p-1} \max_{1\leq k\leq p-1} GB(j,k) = \max_{1\leq j\leq p-1} f(j) < \frac{3}{4}p.$$

4 Earlier work on $M(p;q)$

Implicit in the literature are various results on $M(p;q)$ (although we are the first to explicitly study $M(p;q)$). Most of these are mentioned in the rest of this paper. Here we rewrite the main result of Gallot and Moree [13] in terms of $M(p;q)$ and use it for $p = 11$ and $p = 13$ (to deal with $q \equiv 4(\text{mod } 11)$, respectively $q \equiv 5(\text{mod } 13)$).

Theorem 10 *Let $p \geq 11$ be a prime. Given an $1 \leq \beta \leq p-1$ we let β^* be the unique integer $1 \leq \beta^* \leq p-1$ with $\beta\beta^* \equiv 1(\text{mod } p)$. Let $\mathcal{B}_-(p)$ be the set of integers satisfying*

$$1 \leq \beta \leq \frac{p-3}{2},\ p \leq \beta + 2\beta^* + 1,\ \beta > \beta^*.$$

Let $\mathcal{B}_+(p)$ be the set of integers satisfying

$$1 \leq \beta \leq \frac{p-3}{2},\ \beta + \beta^* \geq p,\ \beta^* \leq 2\beta.$$

The set $\mathcal{B}(p) = \mathcal{B}_-(p) \cup \mathcal{B}_+(p)$ is non-empty (it contains at least $\beta = (p-3)/2$). Let $q \equiv \beta(\text{mod } p)$ be a prime satisfying $q > p$. Suppose that the inequality $q > q_-(p) = p(p-\beta^*)(p-\beta^*-2)/(2\beta)$ holds if $\beta \in \mathcal{B}_-(p)$ and

$$q > q_+(p) = \frac{p(p-1-\beta)}{\gamma(p-1-\beta) - p + 1 + 2\beta},$$

with $\gamma = \min((p-\beta^*)/(p-\beta), (\beta^*-\beta)/\beta^*)$ if $\beta \in \mathcal{B}_+(p)$. Then

$$M(p;q) \geq p - \beta > \frac{p+1}{2}$$

and hence $M(p) \geq p - \min\{\mathcal{B}(p)\}$.

We have $\mathcal{B}(11) = \{4\}, \mathcal{B}(13) = \{5\}, \mathcal{B}(17) = \{7\}$ and $\mathcal{B}(19) = \{8\}$. In general one can show [11] using Kloosterman sum techniques that

$$\left| |\mathcal{B}(p)| - \frac{p}{16} \right| \leq 8\sqrt{p}(\log p + 2)^3.$$

The lower bound for $M(p)$ resulting from this theorem, $p - \min\{\mathcal{B}(p)\}$, never exceeds $2p/3$ and this together with extensive numerical experimentation led Gallot and Moree [13] to propose the corrected Beiter conjecture, now proved by Zhao and Zhang (Theorem 2).

In a rather small subset of cases using Theorem 10 one can exactly compute $M(p;q)$ on combining the latter theorem with Theorem 9.

Theorem 11 *Let $p \geq 13$ with $p \equiv 1(\text{mod } 4)$.be a prime. Let x_0 be the smallest positive integer such that $x_0^2 + 1 \equiv 0(\text{mod } p)$. If $x_0 > p/3$, $q \geq q_+(p)$ (with $\beta = x_0$) and $q \equiv x_0(\text{mod } p)$, then $M(p;q) = p - x_0$. The set of primes p satisfying $p \equiv 1(\text{mod } 4)$ and $x_0 > p/3$ $(13, 29, 53, 73, 89, 173, \cdots)$ has natural density $1/6$.*

Proof. Some easy computations show that if $p-\beta=f(\beta^*)$ and $\beta\in\mathcal{B}(p)$, we must have

$$1\le\beta\le\frac{p-3}{2},\ \beta+\beta^*=p,\ \beta^*\le 2\beta,\ \frac{p-1}{2}<\beta^*<\frac{3}{4}p,\ \beta\in\mathcal{B}_+(p). \qquad (4)$$

Note that $\beta+\beta^*=p$, $p\ge 13$, has a solution with $\beta<p/2$ iff $p\equiv 1(\text{mod }4)$ and $\beta=x_0$ (and hence $\beta^*=p-x_0$) with x_0 the smallest solution of $x_0^2+1\equiv 0(\text{mod }p)$. If $x_0>p/3$, then $\beta=x_0$ satisfies (4). Since by assumption $q\ge q_+(p)$ and $q\equiv x_0(\text{mod }p)$, we have $M(p;q)\ge p-x_0$ by Theorem 10. On the other hand, by Theorem 9, we have $M(p;q)\le f(p-x_0)=f(x_0)=p-x_0$. Duke et al. [12] proved that if f is a quadratic polynomial with complex roots and $0\le\alpha<\gamma\le 1$ are prescribed real numbers, then as x tends to infinity,

$$\#\{(p,v): p\le x,\ f(v)\equiv 0(\text{mod }p),\ \alpha\le\frac{v}{p}<\gamma\}\sim(\gamma-\alpha)\pi(x),$$

using which the result is completed on taking $\gamma=1/2$ and $\alpha=1/3$. □

`Remark`. Note that a priori the estimate $p-\beta>f(\beta^*)$ with $\beta\in\mathcal{B}(p)$ cannot have a solution. A posteriori one checks that indeed it does not have a solution.

5 Computation of $M(3;q)$

Note that for all primes q and r with $1<q<r$, we have $r=(kq+1)/h$, or $r=(kq-1)/h$ with $h\le(q-1)/2$. If $n\equiv 0(\text{mod }3)$ is ternary, then either $A(n)=1$ or $A(n)=2$ as $M(3)=2$. The following result due to Sister Beiter [8] allows one to compute $A(n)$ in this case.

Theorem 12 *Let $n\equiv 0(\text{mod }3)$ be ternary.*
If $h=1$, then $A(n)=1$ iff $k\equiv 0(\text{mod }3)$.
If $h>1$, then $A(n)=1$ iff one of the following conditions holds:
(a) $k\equiv 0(\text{mod }3)$ *and* $h+q\equiv 0(\text{mod }3)$.
(b) $k\equiv 0(\text{mod }3)$ *and* $h+r\equiv 0(\text{mod }3)$.

We have seen that $M(3;5)=2$. The next result extends this.

Theorem 13 *Let $q>3$ be a prime. We have $M(3;q)=2$.*

Proof. In case $q\equiv 1(\text{mod }3)$, then let r be a prime such that $r\equiv 1+q(\text{mod }3q)$. Since $(1+q,3q)=1$, there are in fact infinitely many such primes (by Dirichlet's theorem). In case $q\equiv 2(\text{mod }3)$, then let r be a prime such that $r\equiv 1+2q(\text{mod }3q)$. Since $(1+2q,3q)=1$, there are infinitely many such primes. The prime r was chosen so to ensure that $h=1$ and $3\nmid k$. Using Theorem 12 it then follows that $A(3qr)=2$ and hence $M(3;q)=2$. □

6 Kaplan's lemma reconsidered

Our main tool will be the following recent result due to Kaplan [15], the proof of which uses the identity

$$\Phi_{pqr}(x)=(1+x^{pq}+x^{2pq}+\cdots)(1+x+\cdots+x^{p-1}-x^q-\cdots-x^{q+p-1})\Phi_{pq}(x^r).$$

Lemma 4 (Nathan Kaplan, 2007). *Let $2 < p < q < r$ be primes and $k \geq 0$ be an integer. Put*

$$b_i = \begin{cases} a_{pq}(i) & \textit{if } ri \leq k; \\ 0 & \textit{otherwise.} \end{cases}$$

We have

$$a_{pqr}(k) = \sum_{m=0}^{p-1} (b_{f(m)} - b_{f(m+q)}), \tag{5}$$

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

(If we need to stress the k-dependence of $f(m)$, we will write $f_k(m)$ instead of $f(m)$, see e.g. Lemma 8 and its proof.) This lemma reduces the computation of $a_{pqr}(k)$ to that of $a_{pq}(i)$ for various i. These binary cyclotomic polynomial coefficients are computed in the following lemma. For a proof see e.g. Lam and Leung [16] or Thangadurai [20].

Lemma 5 *Let $p < q$ be odd primes. Let ρ and σ be the (unique) non-negative integers for which $1 + pq = (\rho+1)p + (\sigma+1)q$. Let $0 \leq m < pq$. Then either $m = \alpha_1 p + \beta_1 q$ or $m = \alpha_1 p + \beta_1 q - pq$ with $0 \leq \alpha_1 \leq q-1$ the unique integer such that $\alpha_1 p \equiv m (\operatorname{mod} q)$ and $0 \leq \beta_1 \leq p-1$ the unique integer such that $\beta_1 q \equiv m (\operatorname{mod} p)$. The cyclotomic coefficient $a_{pq}(m)$ equals*

$$\begin{cases} 1 & \textit{if } m = \alpha_1 p + \beta_1 q \textit{ with } 0 \leq \alpha_1 \leq \rho,\ 0 \leq \beta_1 \leq \sigma; \\ -1 & \textit{if } m = \alpha_1 p + \beta_1 q - pq \textit{ with } \rho+1 \leq \alpha_1 \leq q-1,\ \sigma+1 \leq \beta_1 \leq p-1; \\ 0 & \textit{otherwise.} \end{cases}$$

We say that $[m]_p = \alpha_1$ is the *p-part of m* and $[m]_q = \beta_1$ is the *q-part of m*. It is easy to see that

$$m = \begin{cases} [m]_p p + [m]_q q & \text{if } [m]_p \leq \rho \text{ and } [m]_q \leq \sigma; \\ [m]_p p + [m]_q q - pq & \text{if } [m]_p > \rho \text{ and } [m]_q > \sigma; \\ [m]_p p + [m]_q q - \delta_m pq & \text{otherwise,} \end{cases}$$

with $\delta_m \in \{0, 1\}$. Using this observation we find that, for $i < pq$,

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

Thus in order to evaluate $a_{pqr}(n)$ using Kaplan's lemma, it is not necessary to compute $f(m)$ and $f(m+q)$ (as we did in [13]), it suffices to compute $[f(m)]_p$, $[f(m)]_q$, $[f(m+q)]_p$ and $[f(m+q)]_q$ (which is easier). Indeed, as $[f(m)]_p = [f(m+q)]_p$, it suffices to compute $[f(m)]_p$, $[f(m)]_q$, and $[f(m+q)]_q$.

For future reference we provide a version of Kaplan's lemma in which the computation of b_i has been made explicit, and thus is self-contained.

Lemma 6 *Let $2 < p < q < r$ be primes and $k \geq 0$ be an integer. We put $\rho = [(p-1)(q-1)]_p$ and $\sigma = [(p-1)(q-1)]_q$. Furthermore, we put*

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

We have

$$a_{pqr}(k) = \sum_{m=0}^{p-1} (b_{f(m)} - b_{f(m+q)}), \tag{6}$$

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

Note that if i and j have the same p-part, then $b_i b_j \neq -1$, that is b_i and b_j cannot be of opposite sign. From this it follows that $|b_{f(m)} - b_{f(m+q)}| \leq 1$, and thus we infer from Kaplan's lemma that $|a_{pqr}(k)| \leq p$ and hence $M(p) \leq p$.

Using the mutual coprimality of p, q and r we arrive at the following trivial, but useful, lemma.

Lemma 7 *We have $\{[f(m)]_q : 0 \leq m \leq p-1\} = \{0, 1, 2, \ldots, p-1\}$ and $|\{[f(m)]_p : 0 \leq m \leq p-1\}| = p$. The same conclusions hold if we replace $[f(m)]_q$ and $[f(m)]_p$ by $[f(m+q)]_q$, respectively $[f(m+q)]_p$.*

On working with Kaplan's lemma one first computes $a_{pq}(f(m))$ and then $b_{f(m)}$. As a check on the correctness of the computations we note that the following identity should be satisfied.

Lemma 8 *We have*

$$\sum_{m=0}^{p-1} a_{pq}(f_k(m)) = \sum_{m=0}^{p-1} a_{pq}(f_k(m+q)).$$

Proof. Choose an integer $k_1 \equiv k (\text{mod } pq)$ such that $k_1 > pqr$. Then $a_{pqr}(k_1) = 0$. By Lemma 4 we find that

$$0 = a_{pqr}(k_1) = \sum_{m=0}^{p-1} [a_{pq}(f_{k_1}(m)) - a_{pq}(f_{k_1}(m+q))].$$

Since $f_k(m)$ only depends on the congruence class of k modulo pq, $f_{k_1}(m) = f_k(m)$ and the result follows. □

6.1 Working with Kaplan's lemma: examples

In this section we carry out four sample computations using Kaplan's lemma. As an application we are able to determine $M(5; q)$ (Theorem 15). For more involved examples the reader is referred to [13].

We remark that the result that $a_n(k) = (p+1)/2$ in Lemma 9 is due to Herbert Möller [18]. The reproof we give is rather different. The foundation for Möller's result is due to Emma Lehmer [17], who already in 1936 had shown that $a_n(\frac{1}{2}(p-3)(qr+1)) = (p-1)/2$ with p, q, r and n satisfying the conditions of Lemma 9.

Lemma 9 *Let $p < q < r$ be primes satisfying*

$$p > 3,\ q \equiv 2(\text{mod } p),\ r \equiv \frac{p-1}{2}(\text{mod } p),\ r \equiv \frac{q-1}{2}(\text{mod } q).$$

For $k = (p-1)(qr+1)/2$ we have $a_{pqr}(k) = (p+1)/2$.

Proof (taken from [14].) Using that $q \equiv 2(\text{mod } p)$, we infer from $1+pq = (\rho+1)p+(\sigma+1)q$ that $\sigma = \frac{p-1}{2}$ and $(\rho+1)p = 1+(\frac{p-1}{2})q$ (and hence $\rho = (p-1)(q-2)/(2p)$). On invoking the Chinese remainder theorem one checks that

$$-r^{-1} \equiv 2 \equiv -(\frac{q-2}{p})p + q(\text{mod } pq). \tag{7}$$

Furthermore, writing $f(0)$ as a linear combination of p and q we see that

$$f(0) \equiv \frac{k}{r} \equiv (\frac{p-1}{2})q + \frac{p-1}{2r} \equiv (\frac{p-1}{2})q + 1 - p \equiv \rho p(\text{mod } pq). \tag{8}$$

From (7) and (8) we infer that, for $0 \le m \le (p-1)/2$, we have $[f(m)]_p = \rho - m(q-2)/p \le \rho$ and $[f(m)]_q = m \le \sigma$. On noting that $[f(m)]_p p + [f(m)]_q q = \rho p + 2m \le \rho p + p - 1 = [k/r]$, we infer that $a_{pq}(f(m)) = b_{f(m)} = 1$ in this range (see also Table 3).

TABLE 3

m	$[f(m)]_p$	$[f(m)]_q$	$f(m)$	$a_{pq}(f(m))$	$b_{f(m)}$
0	ρ	0	ρp	1	1
1	$\rho - (q-2)/p$	1	$\rho p + 2$	1	1
$\dots$	$\dots$	$\dots$	$\dots$	1	1
j	$\rho - j(q-2)/p$	j	$\rho p + 2j$	1	1
$\dots$	$\dots$	$\dots$	$\dots$	1	1
$(p-1)/2$	0	$(p-1)/2$	$(p-1)q/2$	1	1

Note that $f(m) \equiv f(0) - m/r \equiv \rho p + 2m(\text{mod } pq)$, from which one easily infers that $f(m) = \rho p + 2m$ for $0 \le m \le p-1$ (as $\rho p + 2m \le \rho p + 2(p-1) < pq$). In the range $\frac{p+1}{2} \le m \le p-1$ we have $f(m) \ge \rho p + p + 1 = (p-1)q/2 + 2 > k/r$, and hence $b_{f(m)} = 0$.

On noting that $f(m+q) \equiv f(m) - q/r \equiv f(m) + 2q \equiv \rho p + 2m + 2q(\text{mod } pq)$, one easily finds, for $0 \le m \le p-1$, that $f(m+q) = \rho p + 2m + 2q > k/r$ and hence $b_{f(m+q)} = 0$.

On invoking Kaplan's lemma one finds

$$a_{pqr}(k) = \sum_{m=0}^{p-1} b_{f(m)} - \sum_{m=0}^{p-1} b_{f(m+q)} = \frac{p+1}{2} - 0 = \frac{p+1}{2}.$$

This concludes the proof. □

Lemma 10 *Let $3 < p < q < r$ be primes satisfying*

$$q \equiv -2(\text{mod } p),\ r^{-1} \equiv p-2(\text{mod } pq)\ \textit{and}\ q > \frac{p^2}{2}.$$

For $k = \frac{p+1}{2}(1 + r(2-p+q)) + r + q - rq$ we have $a_{pqr}(k) = -(p+1)/2$.

Remark. Numerical experimentation suggests that with this choice of k, a condition of the form $q > p^2 c_1$, with c_1 some absolute positive constant, is unavoidable.

Proof of Lemma 10. Using $q \equiv -2(\text{mod } p)$ it follows from $1 + pq = (\rho+1)p + (\sigma+1)q$ that

$$\sigma = \frac{p-3}{2} \text{ and } \rho = \frac{1+q\frac{p+1}{2}}{p} - 1.$$

For k we have the congruences:

$$k \equiv -3(\text{mod } p),\ k \equiv r(\text{mod } q),\ k \equiv q + \frac{p+1}{2}(\text{mod } r).$$

These help us to compute $[f(m)]_q$, $[f(m+q)]_q$ and $[f(m)]_p = [f(m+q)]_p$:

$$[f(m)]_q \equiv q^{-1}r^{-1}(k-m) \equiv (-2)^{-1}\cdot(-2)\cdot(-3-m) \equiv -3-m(\text{mod } p)$$

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

$$[f(m)]_p \equiv [f(m+q)]_p \equiv p^{-1}r^{-1}(k-m) \equiv (\rho+1)r^{-1}r - p^{-1}(p-2)m$$

$$\equiv (\rho+1) - m + 2(\rho+1)m \equiv (\rho+1) + m\Big(\frac{2+q}{p} - 1\Big)(\text{mod } q)$$

Recalling that $0 \le [i]_q < p$ and $0 \le [i]_p < q$, we find:

$$[f(m)]_q = \begin{cases} p-3-m & \text{for } 0 \le m \le p-3 \\ 2p-3-m & \text{for } p-2 \le m \le p-1 \end{cases} \tag{9}$$

$$[f(m+q)]_q = p-1-m \tag{10}$$

$$[f(m)]_p = \begin{cases} (\rho+1) + m(\frac{2+q}{p} - 1) & \text{for } 0 \le m \le \frac{p-1}{2} \\ (\rho+1) + m(\frac{2+q}{p} - 1) - q & \text{for } \frac{p+1}{2} \le m \le p-1, \end{cases} \tag{11}$$

where (9) and (10) are obvious. For (11) one has to do some work, and here the assumption $q > \frac{p^2}{2}$ will be needed. Now it is easy to see, that:

$$[f(m)]_q \begin{cases} \le \sigma & \text{for } \frac{p-3}{2} \le m \le p-3 \\ > \sigma & \text{for } 0 \le m \le \frac{p-5}{2} \text{ or } p-2 \le m \le p-1 \end{cases}$$

$$[f(m+q)]_q \begin{cases} \le \sigma & \text{for } \frac{p+1}{2} \le m \le p-1 \\ > \sigma & \text{for } 0 \le m \le \frac{p-1}{2} \end{cases}$$

$$[f(m)]_p = [f(m+q)]_p \begin{cases} \le \rho & \text{for } \frac{p+1}{2} \le m \le p-1 \\ > \rho & \text{for } 0 \le m \le \frac{p-1}{2} \end{cases}$$

Using Kaplan's Lemma it remains to compute $[f(m)]_p p + [f(m)]_q q$, respectively $[f(m+q)]_p p + [f(m+q)]_q q$ and to compare it with k/r.

- Case 1: $[f(m)]_q \le \sigma$, $[f(m)]_p \le \rho$. We have $\frac{p+1}{2} \le m \le p-3$.

$$[f(m)]_p p + [f(m)]_q q = \Big(\rho + 1 + m(\frac{2+q}{p} - 1) - q\Big)p + (p-3-m)q$$

$$= \frac{p+1}{2}q + m(2-p) - 3q + 1 < \frac{p+1}{2}(2-p+q) - q + 1 + \frac{\frac{p+1}{2}+q}{r} = \frac{k}{r}$$

- Case 2: $[f(m)]_q > \sigma$, $[f(m)]_p > \rho$. We have $0 \leq m \leq \frac{p-5}{2}$.

$$[f(m)]_p p + [f(m)]_q q - pq = \Big(\rho + 1 + m(\frac{2+q}{p} - 1)\Big)p + (p-3-m)q - pq$$

$$= \frac{p+1}{2}q + m(2-p) - 3q + 1 < \frac{p+1}{2}(2-p+q) - q + 1 + \frac{\frac{p+1}{2}+q}{r} = \frac{k}{r}$$

- Case 3: $[f(m+q)]_q \leq \sigma$, $[f(m+q)]_p \leq \rho$. We have $\frac{p+1}{2} \leq m \leq p-1$.

$$[f(m+q)]_p p + [f(m+q)]_q q = \Big(\rho + 1 + m(\frac{2+q}{p} - 1) - q\Big)p + (p-1-m)q$$

$$= \frac{p+1}{2}q + m(2-p) - q + 1 < \frac{p+1}{2}(2-p+q) - q + 1 + \frac{\frac{p+1}{2}+q}{r} = \frac{k}{r}$$

- Case 4: $[f(m+q)]_q > \sigma$, $[f(m+q)]_p > \rho$. We have $0 \leq m \leq \frac{p-1}{2}$.

$$[f(m)]_p p + [f(m)]_q q - pq = \Big(\rho + 1 + m(\frac{2+q}{p} - 1)\Big)p + (p-1-m)q - pq$$

$$= \frac{p+1}{2}q + m(2-p) - q + 1 > \frac{p+1}{2}(2-p+q) - q + 1 + \frac{\frac{p+1}{2}+q}{r} = \frac{k}{r}$$

Now we can compute $a_{pqr}(k)$ by Kaplan's Lemma:

$$a_{pqr}(k) = \left(\frac{p-5}{2} - \frac{p-3}{2}\right) - \left(\frac{p-1}{2} - 0\right) = -\frac{(p+1)}{2}.$$

Lemma 11 *Let $3 < p < q < r$ be primes satisfying*

$$q \equiv 1 (\text{mod } p), \;\; r^{-1} \equiv \frac{p+q}{2} (\text{mod } pq).$$

For $k = (p-1)qr/2 - pr + 2$ we have $a_{pqr}(k) = -\min(\frac{q-1}{p} + 1, \frac{p+1}{2})$.

Proof. Let $0 \leq m \leq p-1$. We have:

$$\rho = \frac{1 + q(p-1)}{p} - 1 \text{ and } \sigma = 0,$$

$$k \equiv 1 (\text{mod } p), \;\; k \equiv 0 (\text{mod } q), \;\; k \equiv 2 (\text{mod } r),$$

so that we can compute:

$$[f(m)]_q \equiv q^{-1}r^{-1}(k-m) \equiv (1-m)/2 (\text{mod } p)$$

$$[f(m+q)]_q \equiv q^{-1}r^{-1}(k-m-q) \equiv -m/2 (\text{mod } p)$$

$$[f(m)]_p = [f(m+q)]_p \equiv p^{-1}r^{-1}(k-m) \equiv -m/2 (\text{mod } q)$$

This leads to:

$$[f(m)]_q = \begin{cases} (p+1-m)/2 & \text{for } m \text{ even} \\ (2p+1-m)/2 & \text{for } m \text{ odd and } m \neq 1 \\ 0 & \text{for } m = 1 \end{cases}$$

$$[f(m+q)]_q = \begin{cases} (p-m)/2 & \text{for } m \text{ odd} \\ (2p-m)/2 & \text{for } m \text{ even and } m \neq 0 \\ 0 & \text{for } m = 0 \end{cases}$$

$$[f(m)]_p = [f(m+q)]_p = \begin{cases} (q-m)/2 & \text{for } m \text{ odd} \\ (2q-m)/2 & \text{for } m \text{ even and } m \neq 0 \\ 0 & \text{for } m = 0 \end{cases}$$

We consider the following four cases:

- Case 1: $[f(m)]_q = \sigma = 0$, $[f(m)]_p \leq \rho = \frac{1+q(p-1)}{p} - 1$. In this case $m = 1$. Therefore:
$$[f(m)]_p p + [f(m)]_q q = \frac{p(q-1)}{2} > \frac{k}{r}$$

- Case 2: $[f(m)]_q > \sigma = 0$, $[f(m)]_p > \rho = \frac{1+q(p-1)}{p} - 1$. This is the case, only if m is even and $m \geq 2$. We have:
$$[f(m)]_p p + [f(m)]_q q - pq = \frac{2q-m}{2}p + \frac{p+1-m}{2}q - pq$$
$$= \frac{q(p+1-m) - mp}{2} \leq \frac{q(p-1)}{2} - p + \frac{2}{r} = \frac{k}{r}$$
But in general this is not the case for all such values of m, since we have $\frac{2q-m}{2} > \frac{1+q(p-1)}{p} - 1$. That means $\frac{m}{2} < \frac{q-1}{p} + 1$ and by $0 < \frac{m}{2} \leq \frac{p-1}{2}$ we have exactly $\min(\frac{q-1}{p}, \frac{p-1}{2})$ different values of m in this case.

- Case 3: $[f(m+q)]_q = \sigma = 0$, $[f(m+q)]_p \leq \rho = \frac{1+q(p-1)}{p} - 1$. In this case we have $m = 0$. Therefore:
$$[f(m+q)]_p p + [f(m+q)]_q q = 0 \leq \frac{k}{r}$$

- Case 4: $[f(m+q)]_q > \sigma = 0$, $[f(m+q)]_p > \rho = \frac{1+q(p-1)}{p} - 1$. This is the case, only if m is even and $m \geq 2$. We find:
$$[f(m+q)]_p p + [f(m+q)]_q q - pq = \frac{2q-m}{2}p + \frac{2p-m}{2}q - pq > \frac{k}{r}$$

Now we can compute $a_{pqr}(k)$ by Kaplan's Lemma:

$$a_{pqr}(k) = \left(0 - \min\left(\frac{q-1}{p}, \frac{p-1}{2}\right)\right) - (1-0) = -\min\left(\frac{q-1}{p} + 1, \frac{p+1}{2}\right).$$

Lemma 12 *Let $3 < p < q < r$ be primes satisfying*

$$q \equiv -1 (\text{mod } p), \ r^{-1} \equiv \frac{p+q}{2} (\text{mod } pq) \text{ and } q \geq p^2 - 2p.$$

For $k = p(q-1)r/2 - rq + p - 1$ we have $a_{pqr}(k) = -(p+1)/2$.

Proof. We have

$$\sigma = p-2 \text{ and } \rho = \frac{q+1}{p} - 1.$$

$$k \equiv p-3 (\text{mod } p),\ k \equiv p-2 (\text{mod } q),\ k \equiv p-1 (\text{mod } r),$$

so that we can compute $[f(m)]_q$, $[f(m+q)]_q$ and $[f(m)]_p = [f(m+q)]_p$:

$$[f(m)]_q \equiv q^{-1}r^{-1}(k-m) \equiv (p-3-m)/2 (\text{mod } p)$$

$$[f(m+q)]_q \equiv q^{-1}r^{-1}(k-m-q) \equiv (p-2-m)/2 (\text{mod } p)$$

$$[f(m)]_p \equiv [f(m+q)]_p \equiv p^{-1}r^{-1}(k-m) \equiv (p-2-m)/2 (\text{mod } q)$$

That leads to:

$$[f(m)]_q = \begin{cases} (p-3-m)/2 & \text{for } m \text{ even and } m \neq p-1 \\ (2p-3-m)/2 & \text{for } m \text{ odd} \\ p-1 & \text{for } m = p-1 \end{cases}$$

$$[f(m+q)]_q = \begin{cases} (p-2-m)/2 & \text{for } m \text{ odd} \\ (2p-2-m)/2 & \text{for } m \text{ even} \end{cases}$$

$$[f(m)]_p = [f(m+q)]_p = \begin{cases} (p-2-m)/2 & \text{for } m \text{ odd} \\ (q+p-2-m)/2 & \text{for } m \text{ even.} \end{cases}$$

We have to distinguish four cases:

- Case 1: $[f(m)]_q \leq \sigma = p-2$, $[f(m)]_p \leq \rho = \frac{q+1}{p} - 1$. In this case m must be odd, but then we have:

$$[f(m)]_p p + [f(m)]_q q = \frac{(p-2-m)}{2}p + \frac{(2p-3-m)}{2}q$$

$$\geq \frac{p}{2} + \frac{pq}{2} > \frac{p(q-1)}{2} - q + \frac{p-1}{r} = \frac{k}{r}$$

- Case 2: $[f(m)]_q > \sigma = p-2$, $[f(m)]_p > \rho = \frac{q+1}{p} - 1$. This is the case, if and only if $m = p-1$. Therefore we have:

$$[f(m)]_p p + [f(m)]_q q - pq = \frac{(q+p-2-(p-1))}{2}p + (p-1)q - pq$$

$$= \frac{p(q-1)}{2} - q < \frac{p(q-1)}{2} - q + \frac{p-1}{r} = \frac{k}{r}$$

- Case 3: $[f(m+q)]_q \leq \sigma = p-2$, $[f(m+q)]_p \leq \rho = \frac{q+1}{p} - 1$. By assumption $q \geq p^2 - 2p$ and hence $q \geq p(p-1)/2 - 1$ this is the case if and only if m is odd. Then we have:

$$[f(m+q)]_p p + [f(m+q)]_q q = \frac{p-2-m}{2}p + \frac{p-2-m}{2}q$$

$$\leq (\frac{p-3}{2})(p+q) \leq \frac{p(q-1)-2q}{2} < \frac{k}{r},$$

where we used that $q \geq p^2 - 2p$ in order to derive the latter inequality.

- Case 4: $[f(m+q)]_q > \sigma = p-2$, $[f(m+q)]_p > \rho = \frac{q+1}{p} - 1$. In this case we must have $m = 0$ and hence

$$[f(m+q)]_p p + [f(m+q)]_q q - pq = \frac{(q+p-2)}{2} p + (p-1)q - pq$$

$$= \frac{p(q+p-2)}{2} - q > \frac{p(q-1)}{2} - q + \frac{p-1}{r} = \frac{k}{r}$$

Now we can compute $a_{pqr}(k)$ by Kaplan's lemma:

$$a_{pqr}(k) = (0-1) - \left(\frac{p-1}{2} - 0\right) = -\frac{(p+1)}{2},$$

and the proof is completed. □

The results from this section together with those from Section 3 allow one to establish the following theorem.

Theorem 14 *Let $2 < p < q$ be primes.*
(a) *If $q \equiv 2 (\text{mod } p)$, then $M(p;q) = (p+1)/2$.*
(b) *If $q \equiv -2 (\text{mod } p)$ and $q > p^2/2$, then $M(p;q) = (p+1)/2$.*
(c) *If $q \equiv 1 (\text{mod } p)$ and $q \geq (p-1)p/2 + 1$, then $M(p;q) = (p+1)/2$.*
(d) *If $q \equiv -1 (\text{mod } p)$ and $q \geq p^2 - 2p$, then $M(p;q) = (p+1)/2$.*

Proof. By Theorem 13 we have $M(3;q) = 2 = (3+1)/2$, so assume $p > 3$.
(a) We have $M(p;q) \geq (p+1)/2$ by Lemma 9, and $M(p;q) \leq f(2^*) = f((p+1)/2) = (p+1)/2$ by Theorem 9.
(b)+(c)+(d) Similar to that of part (a). Note that $f((-2)^*) = f((p-1)/2) = (p+1)/2$ and $f(1) = f(p-1) = (p+1)/2$. □

In Section 10 we will discuss the sharpness of the lower bounds for q in the latter theorem.

Using Theorem 14 it is easy to establish the following result.

Theorem 15 *Let $q > 5$ be a prime. Then $M(5;q) = 3$.*

Proof. The proof is most compactly given by Table 4.

TABLE 4

$\overline{q}$	q_0	$M(5;q)$	result
1	31	3	Theorem 14 (c)
2	7	3	Theorem 14 (a)
3	13	3	Theorem 14 (b)
4	29	3	Theorem 14 (d)

The table should be read as follows. From, e.g. the third row we read that for $q \equiv 3(\text{mod } 5)$, $q \geq 13$, we have that $M(5;q) = 3$ by Theorem 14 (b). Since $M(5;11) = M(5;19) = 3$ (the only cases not covered by Table 4), the proof is then completed. □

7 Computation of $M(7;q)$

Theorem 14 in addition with the following two lemmas allows one to compute $M(7;q)$. These lemmas concern the computation of $M(p;q)$ with $q \equiv (p \pm 1)/2 (\text{mod } p)$.

Lemma 13 *Let $p \geq 5$ be a prime. Let $q \geq \max(3p, p(p+1)/4)$ be a prime satisfying $q \equiv \frac{p-1}{2} (\text{mod } p)$. Let $r > q$ be a prime satisfying*

$$r^{-1} \equiv \frac{p+1}{2} (\text{mod } p),\ r^{-1} \equiv p (\text{mod } q).$$

For $k = p - 1 + r(1 + q(p-1)/2 - p(p+1)/2)$ we have $a_{pqr}(k) = (p+1)/2$.

Proof. We have

$$\sigma = p - 3 \text{ and } \rho = \frac{2q+1}{p} - 1,$$

$$k \equiv \frac{p+3}{2} (\text{mod } p),\ k \equiv \frac{p-3}{2} + \frac{2q+1}{p} (\text{mod } q),\ k \equiv p - 1 (\text{mod } r),$$

so that we can compute $[f(m)]_q$, $[f(m+q)]_q$ and $[f(m)]_p = [f(m+q)]_p$:

$$[f(m)]_q \equiv q^{-1} r^{-1} (k - m) \equiv m - \frac{p+3}{2} (\text{mod } p)$$

$$[f(m+q)]_q \equiv q^{-1} r^{-1} (k - m - q) \equiv m - 2 (\text{mod } p)$$

$$[f(m)]_p \equiv [f(m+q)]_p \equiv p^{-1} r^{-1} (k - m) \equiv \frac{p-3}{2} + \frac{2q+1}{p} - m (\text{mod } q)$$

That leads to:

$$[f(m)]_q = \begin{cases} m + \frac{p-3}{2} & \text{for } 0 \leq m \leq \frac{p+1}{2} \\ m - \frac{p+3}{2} & \text{for } \frac{p+3}{2} \leq m \leq p-1 \end{cases}$$

$$[f(m+q)]_q = \begin{cases} p - 2 + m & \text{for } 0 \leq m \leq 1 \\ m - 2 & \text{for } 2 \leq m \leq p-1 \end{cases}$$

and, by the assumption $q \geq p(p+1)/4$,:

$$[f(m)]_p = [f(m+q)]_p = \frac{p-3}{2} + \frac{2q+1}{p} - m$$

We have to distinguish four cases:

- Case 1: $[f(m)]_q \leq \sigma = p - 3$, $[f(m)]_p \leq \rho = \frac{2q+1}{p} - 1$. This is the case if and only if $\frac{p+3}{2} \leq m \leq p - 1$. Therefore we have:

$$[f(m)]_q q + [f(m)]_p p = \left(m - \frac{p-1}{2}\right) q - \left(m - \frac{p-3}{2}\right) p + 1 \leq \frac{k}{r}$$

- Case 2: $[f(m)]_q > \sigma = p - 3$, $[f(m)]_p > \rho = \frac{2q+1}{p} - 1$. There is no value of m satisfying these conditions.

- Case 3: $[f(m+q)]_q \le \sigma = p-3$, $[f(m+q)]_p \le \rho = \frac{2q+1}{p} - 1$. In this case we have $\frac{p-1}{2} \le m \le p-1$, but then we have:

$$[f(m+q)]_q q + [f(m+q)]_p p = mq - \left(m - \frac{p-3}{2}\right) p + 1 > \frac{k}{r}$$

- Case 4: $[f(m+q)]_q > \sigma = p-3$, $[f(m+q)]_p > \rho = \frac{2q+1}{p} - 1$. This is the case if and only if $0 \le m \le 1$. Therefore we have, by the assumption $q \ge 3p$,:

$$[f(m+q)]_q q + [f(m+q)]_p p - pq = mq + \left(\frac{p-3}{2} - m\right) p + 1 \le \frac{k}{r}$$

Now we can compute $a_{pqr}(k)$ by Kaplan's lemma:

$$a_{pqr}(k) = \left(\frac{p-3}{2} - 0\right) - (0-2) = \frac{p+1}{2}.$$

Lemma 14 *Let $p \ge 5$ be a prime. Let $q \ge \max(3p, p(p-1)/4+1)$ be a prime satisfying $q \equiv \frac{p+1}{2} (\text{mod } p)$. Let $r > q$ be a prime satisfying*

$$r^{-1} \equiv \frac{p-1}{2} (\text{mod } p),\ r^{-1} \equiv p (\text{mod } q).$$

For $k = q+p-1+r(q(p-1)/2 - p(p+1)/2)$ we have $a_{pqr}(k) = (p+1)/2$.

Proof. We have

$$\sigma = 1 \text{ and } \rho = \frac{q(p-2)+1}{p} - 1.$$

$$k \equiv 0 (\text{mod } p),\ k \equiv \frac{p-3}{2} (\text{mod } q),\ k \equiv q+p-1 (\text{mod } r),$$

so that we can compute $[f(m)]_q$, $[f(m+q)]_q$ and $[f(m)]_p = [f(m+q)]_p$:

$$[f(m)]_q \equiv q^{-1} r^{-1} (k-m) \equiv m (\text{mod } p)$$

$$[f(m+q)]_q \equiv q^{-1} r^{-1} (k-m-q) \equiv m + \frac{p+1}{2} (\text{mod } p)$$

$$[f(m)]_p \equiv [f(m+q)]_p \equiv p^{-1} r^{-1} (k-m) \equiv \frac{p-3}{2} - m (\text{mod } q)$$

That leads to:

$$[f(m)]_q = m$$

$$[f(m+q)]_q = \begin{cases} m + \frac{p+1}{2} & \text{for } 0 \le m \le \frac{p-3}{2} \\ m - \frac{p-1}{2} & \text{for } \frac{p-1}{2} \le m \le p-1 \end{cases}$$

$$[f(m)]_p = [f(m+q)]_p = \begin{cases} \frac{p-3}{2} - m & \text{for } 0 \le m \le \frac{p-3}{2} \\ q + \frac{p-3}{2} - m & \text{for } \frac{p-1}{2} \le m \le p-1 \end{cases}$$

We have to distinguish four cases:

- Case 1: $[f(m)]_q \leq \sigma = 1$, $[f(m)]_p \leq \rho = \frac{q(p-2)+1}{p} - 1$. This is the case if and only if $0 \leq m \leq 1$. Therefore we have by assumption $q \geq 3p$:

$$[f(m)]_q q + [f(m)]_p p = mq + \left(\frac{p-3}{2} - m\right) p \leq \frac{k}{r}$$

- Case 2: $[f(m)]_q > \sigma = 1$, $[f(m)]_p > \rho = \frac{q(p-2)+1}{p} - 1$. In this case we have $\frac{p-1}{2} \leq m \leq p-1$, but then we have:

$$[f(m)]_q q + [f(m)]_p p - pq = mq - \left(m - \frac{p-3}{2}\right) p > \frac{k}{r}$$

- Case 3: $[f(m+q)]_q \leq \sigma = 1$, $[f(m+q)]_p \leq \rho = \frac{q(p-2)+1}{p} - 1$. There is no value of m satisfying these conditions.

- Case 4: $[f(m+q)]_q > \sigma = 1$, $[f(m+q)]_p > \rho = \frac{q(p-2)+1}{p} - 1$. By the assumption $q \geq \frac{p(p-1)}{4} + 1$ this is the case if and only if $\frac{p+3}{2} \leq m \leq p-1$. Therefore we have:

$$[f(m+q)]_q q + [f(m+q)]_p p - pq = \left(m - \frac{p-1}{2}\right) q - \left(m - \frac{p-3}{2}\right) p \leq \frac{k}{r}$$

Now we can compute $a_{pqr}(k)$ by Kaplan's lemma:

$$a_{pqr}(k) = (2-0) - \left(0 - \frac{p-3}{2}\right) = \frac{p+1}{2},$$

concluding the proof. □

Theorem 16
(a) *Let* $q \geq \max(3p, p(p+1)/4)$ *be a prime satisfying* $q \equiv \frac{p-1}{2} (\mathrm{mod}\ p)$, *then* $(p+1)/2 \leq M(p;q) \leq (p+3)/2$.
(b) *Let* $q \geq \max(3p, p(p-1)/4+1)$ *be a prime satisfying* $q \equiv \frac{p+1}{2} (\mathrm{mod}\ p)$, *then* $(p+1)/2 \leq M(p;q) \leq (p+3)/2$.

Proof. Follows on combining Lemmas 13 and 14 with Theorem 9. □

Theorem 17 *We have* $M(7;11) = 4$, $M(7;13) = 3$ *and for* $q \geq 17$ *a prime,* $M(7;q) = 4$.

Proof. The proof is most compactly given by a table (Table 5). Recall that Zhao and Zhang [21] proved that $M(7) \leq 4$.

TABLE 5

$\overline{q}$	q_0	$M(7;q)$	result
1	29	4	Theorem 14 (c)
2	23	4	Theorem 14 (a)
3	31	4	Theorem 16 (a) $+M(7) \leq 4$
4	53	4	Theorem 16 (b) $+M(7) \leq 4$
5	47	4	Theorem 14 (b)
6	41	4	Theorem14 (d)

Since $M(7;11) = M(7;17) = M(7;19) = 4$ and $M(7;13) = 3$ (the only cases not covered in Table 5), the proof is completed. □

8 Computation of $M(11;q)$

We have $M(11;q) \leq M(11) = 7$. From [13] we recall the following result.

Theorem 18 *Let $q < r$ be primes such that $q \equiv 4(\text{mod } 11)$ and $r \equiv -3(\text{mod } 11)$. Let $1 \leq \alpha \leq q-1$ be the unique integer such that $11r\alpha \equiv 1(\text{mod } q)$. Suppose that $q/33 < \alpha \leq (3q-1)/77$, then $a_{11qr}(10 + (6q - 77\alpha)r) = -7$.*

Lemma 15 *Let q be a prime such that $q \equiv 4(\text{mod } 11)$. Then $M(11;37) = 6$ and, for $q > 37$, $M(11;q) = 7$.*

Proof. By computation one finds that $M(11;37) = 6$. Now assume $q > 37$. Notice that it is enough to show that $M(11;q) \geq 7$. For $q \geq 367$ the interval $I(q) := (q/33, (3q-1)/77]$ has length exceeding 1 and so contains at least one integer α_1. Then by the Chinese remainder theorem and Dirichlet's theorem we can find a prime r_1 such that both $r_1 \equiv -3(\text{mod } 11)$ and $11r_1\alpha_1 \equiv 1(\text{mod } q)$. Then we invoke Theorem 18 with $r = r_1$ and $\alpha = \alpha_1$. It remains to deal with the primes 59 and 191. One checks that the interval $I(59)$ and $I(191)$ both contain an integer and so we can proceed as in the case $q \geq 367$ to conclude the proof. □

Lemma 16 *Let $p = 11$.*
(a) *For $q > 113$, $q \equiv 3(\text{mod } 11)$, $r^{-1} \equiv \frac{q-19}{2}(\text{mod } pq)$ and $k = q + 7r\frac{(q-19)}{2}$ we have $a_{pqr}(k) = 7$.*
(b) *For $q \equiv 7(\text{mod } 11)$, $r^{-1} \equiv \frac{q+7}{2}(\text{mod } pq)$ and $k = 6qr + 4$ we have $a_{pqr}(k) = 7$.*
(c) *For $q \equiv 8(\text{mod } 11)$, $r^{-1} \equiv \frac{q-3}{2}(\text{mod } pq)$ and $k = 6qr + 4$ we have $a_{pqr}(k) = 7$.*

Proof.

(a) We have

$$\sigma = 3 \text{ and } \rho = \frac{7q-10}{11}$$

$$k \equiv 10(\text{mod } p),\ k \equiv 7(\text{mod } q),\ k \equiv q(\text{mod } r),$$

so that we can compute $[f(m)]_q$, $[f(m+q)]_q$ and $[f(m)]_p = [f(m+q)]_p$:

$$[f(m)]_q \equiv q^{-1}r^{-1}(k-m) \equiv 10 - m(\text{mod } p)$$

$$[f(m+q)]_q \equiv q^{-1}r^{-1}(k-m-q) \equiv 7-m (\mathrm{mod}\ p)$$

$$[f(m)]_p \equiv [f(m+q)]_p \equiv p^{-1}r^{-1}(k-m) \equiv \frac{19+q}{22}(m-7)(\mathrm{mod}\ q)$$

That leads to:

$$[f(m)]_q = 10-m$$

$$[f(m+q)]_q = \begin{cases} 7-m & \text{for } 0 \leq m \leq 7 \\ 18-m & \text{for } 8 \leq m \leq 10 \end{cases}$$

$$[f(m)]_p = [f(m+q)]_p = \begin{cases} q + \frac{19+q}{22}(m-7) & \text{for } 0 \leq m \leq 6 \\ \frac{19+q}{22}(m-7) & \text{for } 7 \leq m \leq 10 \end{cases}$$

We have to distinguish four cases:

- Case 1: $[f(m)]_q \leq \sigma = 3$, $[f(m)]_p \leq \rho = \frac{7q-10}{11}$. This is the case if and only if $7 \leq m \leq 10$. By the assumption $q > 113$ we have:

$$[f(m)]_q q + [f(m)]_p p = \frac{(13-m)q + 19(m-7)}{2} \leq \frac{k}{r}$$

- Case 2: $[f(m)]_q > \sigma = 3$, $[f(m)]_p > \rho = \frac{7q-10}{11}$. In this case we have $0 \leq m \leq 6$, but then we have:

$$[f(m)]_q q + [f(m)]_p p - pq = \frac{(13-m)q + 19(m-7)}{2} > \frac{k}{r}$$

- Case 3: $[f(m+q)]_q \leq \sigma = 3$, $[f(m+q)]_p \leq \rho = \frac{7q-10}{11}$. This is the case if and only if $m = 7$. Therefore we have:

$$[f(m+q)]_q q + [f(m+q)]_p p = 0 \leq \frac{k}{r}$$

- Case 4: $[f(m+q)]_q > \sigma = 3$, $[f(m+q)]_p > \rho = \frac{7q-10}{11}$. By the assumption $q > 113$ this is the case if and only if $0 \leq m \leq 3$. Therefore we have:

$$[f(m+q)]_q q + [f(m+q)]_p p - pq = \frac{(7-m)q - 19(7-m)}{2} \leq \frac{k}{r}$$

Now we can compute $a_{pqr}(k)$ by Kaplan's lemma:

$$a_{pqr}(k) = (4-0) - (1-4) = 7.$$

(b) We have

$$\sigma = 7 \text{ and } \rho = \frac{3q-10}{11}$$

$$k \equiv 10 (\mathrm{mod}\ p),\ k \equiv 4 (\mathrm{mod}\ q),\ k \equiv 4 (\mathrm{mod}\ r),$$

so that we can compute $[f(m)]_q$, $[f(m+q)]_q$ and $[f(m)]_p = [f(m+q)]_p$:

$$[f(m)]_q \equiv q^{-1}r^{-1}(k-m) \equiv 10-m (\mathrm{mod}\ p)$$

$$[f(m+q)]_q \equiv q^{-1}r^{-1}(k-m-q) \equiv 3-m(\text{mod } p)$$

$$[f(m)]_p \equiv [f(m+q)]_p \equiv p^{-1}r^{-1}(k-m) \equiv \frac{q-7}{22}(m-4)(\text{mod } q)$$

That leads to:

$$[f(m)]_q = 10-m$$

$$[f(m+q)]_q = \begin{cases} 3-m & \text{for } 0 \leq m \leq 3 \\ 14-m & \text{for } 4 \leq m \leq 10 \end{cases}$$

$$[f(m)]_p = [f(m+q)]_p = \begin{cases} q+\frac{q-7}{22}(m-4) & \text{for } 0 \leq m \leq 3 \\ \frac{q-7}{22}(m-4) & \text{for } 4 \leq m \leq 10 \end{cases}$$

We have to distinguish four cases:

- Case 1: $[f(m)]_q \leq \sigma = 7$, $[f(m)]_p \leq \rho = \frac{3q-10}{11}$. This is the case if and only if $4 \leq m \leq 10$. Therefore we have:

$$[f(m)]_q q + [f(m)]_p p = \frac{(16-m)q - 7(m-4)}{2} \leq \frac{k}{r}$$

- Case 2: $[f(m)]_q > \sigma = 7$, $[f(m)]_p > \rho = \frac{3q-10}{11}$. In this case we have $0 \leq m \leq 2$, but then we have:

$$[f(m)]_q q + [f(m)]_p p - pq = \frac{(16-m)q + 7(4-m)}{2} > \frac{k}{r}$$

- Case 3: $[f(m+q)]_q \leq \sigma = 7$, $[f(m+q)]_p \leq \rho = \frac{3q-10}{11}$. In this case we have $7 \leq m \leq 10$. By $q \equiv 7(\text{mod } 11)$ we have $q \geq 29$. It follows:

$$[f(m+q)]_q q + [f(m+q)]_p p = \frac{(24-m)q - 7(m-4)}{2} > \frac{k}{r}$$

- Case 4: $[f(m+q)]_q > \sigma = 7$, $[f(m+q)]_p > \rho = \frac{3q-10}{11}$. There is no value of m satisfying these conditions.

Now we can compute $a_{pqr}(k)$ by Kaplan's lemma:

$$a_{pqr}(k) = (7-0) - (0-0) = 7.$$

(c) We have

$$\sigma = 6 \text{ and } \rho = \frac{4q-10}{11}$$

$$k \equiv 10(\text{mod } p), \ k \equiv 4(\text{mod } q), \ k \equiv 4(\text{mod } r),$$

so that we can compute $[f(m)]_q$, $[f(m+q)]_q$ and $[f(m)]_p = [f(m+q)]_p$:

$$[f(m)]_q \equiv q^{-1}r^{-1}(k-m) \equiv 10-m(\text{mod } p)$$

$$[f(m+q)]_q \equiv q^{-1}r^{-1}(k-m-q) \equiv 2-m(\text{mod } p)$$

$$[f(m)]_p \equiv [f(m+q)]_p \equiv p^{-1}r^{-1}(k-m) \equiv \frac{q+3}{22}(m-4)(\text{mod } q)$$

That leads to:

$$[f(m)]_q = 10 - m$$

$$[f(m+q)]_q = \begin{cases} 2-m & \text{for } 0 \le m \le 2 \\ 13-m & \text{for } 3 \le m \le 10 \end{cases}$$

$$[f(m)]_p = [f(m+q)]_p = \begin{cases} q + \frac{q+3}{22}(m-4) & \text{for } 0 \le m \le 3 \\ \frac{q+3}{22}(m-4) & \text{for } 4 \le m \le 10 \end{cases}$$

We have to distinguish four cases:

- Case 1: $[f(m)]_q \le \sigma = 6$, $[f(m)]_p \le \rho = \frac{4q-10}{11}$. This is the case if and only if $4 \le m \le 10$. Therefore we have:
$$[f(m)]_q q + [f(m)]_p p = \frac{(16-m)q + 3(m-4)}{2} \le \frac{k}{r}$$
- Case 2: $[f(m)]_q > \sigma = 6$, $[f(m)]_p > \rho = \frac{4q-10}{11}$. In this case we have $0 \le m \le 3$, but then we have:
$$[f(m)]_q q + [f(m)]_p p - pq = \frac{(16-m)q + 3(m-4)}{2} > \frac{k}{r}$$
- Case 3: $[f(m+q)]_q \le \sigma = 6$, $[f(m+q)]_p \le \rho = \frac{4q-10}{11}$. In this case we have $7 \le m \le 10$, but then we have:
$$[f(m+q)]_q q + [f(m+q)]_p p = \frac{(22-m)q + 3(m-4)}{2} > \frac{k}{r}$$
- Case 4: $[f(m+q)]_q > \sigma = 6$, $[f(m+q)]_p > \rho = \frac{4q-10}{11}$. This is the case if and only if $m = 3$. Therefore we have:
$$[f(m+q)]_q q + [f(m+q)]_p p - pq = 10q - \frac{q+3}{2} > \frac{k}{r}$$

Now we can compute $a_{pqr}(k)$ by Kaplan's lemma:

$$a_{pqr}(k) = (7-0) - (0-0) = 7.$$

Theorem 19 *For $q \ge 13$ we have*

$q(\text{mod } 11)$	1	2	3	4	5	6	7	8	9	10
$M(11;q)$	6	6	7	7	6,7	6,7	7	7	6	6

with as only exceptions $M(11;17) = 5$, $M(11;23) = 3$, $M(11;37) = 6$, $M(11;43) = 5$ and $M(11;47) = 6$.

Remark 1. If $q \equiv \pm 5(\text{mod } 11)$ and $q \ge 61$, then $M(p,q) \in \{6,7\}$. We believe that $M(p;q) = 6$.
Remark 2. By Corollary 1 and 2 below, one infers that $M(11;17) \le 5$, $M(11;23) \le 3$ and $M(11;43) \le 5$.

Proof of Theorem 19. Is most compactly given in Table 6:

TABLE 6

$\overline{q}$	q_0	$M(11;q)$	result
1	67	6	Theorem 14 (c)
2	13	6	Theorem 14 (a)
3	157	7	Lemma 16 (a) $+M(11) \le 7$
4	59	7	Lemma 15
5	71	6,7	Theorem 16 (a) $+M(11) \le 7$
6	61	6,7	Theorem 16 (b) $+M(11) \le 7$
7	29	7	Lemma 16 (b) $+M(11) \le 7$
8	19	7	Lemma 16 (c) $+M(11) \le 7$
9	97	6	Theorem 14 (b)
10	109	6	Theorem 14 (d)

On directly computing the values of $M(p;q)$ not covered by the table, the proof is completed. □

9 Computation for $p = 19$

By Theorem 2 we have $M(19) \le 2 \cdot 19/3$ and hence $M(19) \le 12$. By Theorem 10 we find that $M(19;q) \ge 11$ for every $q \equiv 8(\text{mod } 19)$ and $q \ge 179$ and hence $M(19) \ge 11$. On computing $A(n)$ for the consecutive ternary n having 19 as a smallest prime factor, it is seen that $19 \cdot 53 \cdot 859$ is the smallest ternary n with $19|n$ such that $A(n) = 12$. It follows that $M(19) = 12$. The next result even shows that $M(19;q) = M(19) = 12$ for a positive fraction of all primes q.

Theorem 20 *We have $M(19) = 12$. Moreover, $M(19,q) = 12$ if $q \equiv \pm 4(\text{mod } 19)$, with $q \ge 29$. Furthermore, $M(19;23) = 11$.*

The proof makes use of the following lemmata.

Lemma 17 *Put $p = 19$ and let $q \equiv 15(\text{mod } 19)$ be a prime. Suppose there exists an integer a satysifying*

$$qa \equiv -1(\text{mod } 3) \text{ and } \frac{q}{6p} < a \le \frac{5q-18}{6p}.$$

Let $r > q$ be a prime satisfying $r(q-ap) \equiv 3(\text{mod } pq)$. Then $a_{pqr}(7qr+q) = -12$.

Proof. We have $\sigma = 13$ and $\rho = \frac{5q-18}{19}$. Note that

$$-\frac{1}{r} \equiv \frac{ap-q}{3} \equiv \frac{(q+a)}{3}p + q\frac{(p-1)}{3}(\text{mod } pq),$$

with $(q+a)/3$ and $(p-1)/3 = 6$ integers. We leave it to the reader to check the correctness of Table 7. Application of Kaplan's lemma then gives

$$a_{pqr}(7qr+q) = -5-7 = -12,$$

completing the proof. □

Table 7: Computation of $a_{19qr}(k)$ with $q \equiv 15 (\mathrm{mod}\ 19)$, $k = 7qr + q$

$\overline{m}$	m	$[f(m)]_p$	$[f(m)]_q$		$c_{f(m)}$	$b_{f(m)}$	$c_{f(m+q)}$	$b_{f(m+q)}$
0	0	0	12	7	1	0	1	1
	3	a	11	6	1	0	1	1
	6	$2a$	10	5	1	0	1	1
	9	$3a$	9	4	1	0	1	1
	12	$4a$	8	3	1	0	1	1
	15	$5a$	7	2	1	0	1	1
	18	$6a$	6	1	1	0	1	1
1	1	$(q+a)/3$	18	13	-1	-1	0	0
	4	$(q+a)/3+a$	17	12	-1	-1	0	0
	7	$(q+a)/3+2a$	16	11	-1	-1	0	0
	10	$(q+a)/3+3a$	15	10	-1	-1	0	0
	13	$(q+a)/3+4a$	14	9	-1	-1	0	0
	16	$(q+a)/3+5a$	13	8	0	0	0	0
2	2	$2(q+a)/3$	5	0	0	0	0	0
	5	$2(q+a)/3+a$	4	18	0	0	-1	0
	8	$2(q+a)/3+2a$	3	17	0	0	-1	0
	11	$2(q+a)/3+3a$	2	16	0	0	-1	0
	14	$2(q+a)/3+4a$	1	15	0	0	-1	0
	17	$2(q+a)/3+5a$	0	0	14	0	-1	0

For reasons of space the fifth column could not be given an header. It has header $[f(m+q)]_q$. Also for reasons of space we have written $c_{f(m)} = a_{pq}(f(m))$. Note that $[f(m+q)]_p = [f(m)]_p$.Thus the final 4 columns can be computed from columns 3-5. The same remarks apply to Table 8.

Lemma 18 *Put $p = 19$ and let $q \equiv 4 (\mathrm{mod}\ 19)$ be a prime. Suppose there exists an integer a satysifying*

$$qa \equiv -1 (\mathrm{mod}\ 3) \text{ and } \frac{q}{6p} < a < \frac{5q-1}{6p}.$$

Let $r > q$ be a prime satisfying $r(q - ap) \equiv 3 (\mathrm{mod}\ pq)$. Then we have $a_{19qr}(7qr + r) = -12$.

Proof. We have $\sigma = 4$ and $\rho = \frac{14q-18}{19}$. Note that

$$-\frac{1}{r} \equiv \frac{ap-q}{3} \equiv \frac{(q+a)}{3}p + q\frac{(p-1)}{3} (\mathrm{mod}\ pq),$$

with $(q + a)/3$ and $(p - 1)/3 = 6$ integers. Put $k = 7qr + r$. Note that $\frac{k}{r} = 7q + 1 \equiv (\rho + 1)p + (8 + \sigma)q (\mathrm{mod}\ pq)$. We leave it to the reader to check the correctness of the rest of Table 8, from which the result is established on invoking Kaplan's lemma. □

Table 8: `Computation of` $a_{19qr}(k)$ `with` $q \equiv 4(\text{mod } 19)$, $k = 7qr + r$

$\overline{m}$	m	$[f(m)]_p$	$[f(m)]_q$		$c_{f(m)}$	$b_{f(m)}$	$c_{f(m+q)}$	$b_{f(m+q)}$
0	0	$\rho+1$	12	17	-1	-1	-1	0
	3	$\rho+1+a$	11	16	-1	-1	-1	0
	6	$\rho+1+2a$	10	15	-1	-1	-1	0
	9	$\rho+1+3a$	9	14	-1	-1	-1	0
	12	$\rho+1+4a$	8	13	-1	-1	-1	0
	15	$\rho+1+5a$	7	12	-1	-1	-1	0
	18	$\rho+1+6a$	6	11	-1	-1	-1	0
1	1	$\rho+1+(q+a)/3-q$	18	4	0	0	1	1
	4	$\rho+1+a+(q+a)/3-q$	17	3	0	0	1	1
	7	$\rho+1+2a+(q+a)/3-q$	16	2	0	0	1	1
	10	$\rho+1+3a+(q+a)/3-q$	15	1	0	0	1	1
	13	$\rho+1+4a+(q+a)/3-q$	14	0	0	0	1	1
	16	$\rho+1+5a+(q+a)/3-q$	13	18	0	0	0	0
2	2	$\rho+1+2(q+a)/3-q$	5	10	0	0	0	0
	5	$\rho+1+a+2(q+a)/3-q$	4	9	1	0	0	0
	8	$\rho+1+2a+2(q+a)/3-q$	3	8	1	0	0	0
	11	$\rho+1+3a+2(q+a)/3-q$	2	7	1	0	0	0
	14	$\rho+1+4a+2(q+a)/3-q$	1	6	1	0	0	0
	17	$\rho+1+5a+2(q+a)/3-q$	0	5	1	0	0	0

10 When q is close to p

Typically if $M(p;q)$ is constant for all q large enough with $q \equiv a(\text{mod } d)$, then $M(p;q)$ assumes a smaller value for some small q in this progression. A (partial) explanation of this phenomenon is provided in this section. The idea is that if $ap + bq = 1$ with a and b small in absolute value, then $M(p;q)$ is small. Thus the caption of this section is a bit imprecise (but short !)

Theorem 21 *Let ρ and σ be the (unique) non-negative integers for which $1 + pq = (\rho+1)p + (\sigma+1)q$. Then*

$$M(p;q) \leq \begin{cases} p+\rho-\sigma & \text{if } \rho \leq \sigma; \\ q+\sigma-\rho & \text{if } \rho > \sigma. \end{cases}$$

Corollary 1 *Let $k \geq 2$ be an integer and $q = (kp-1)/h$ a prime. If $p \geq k+h$, then $M(p;q) \leq k+h$.*

Corollary 2 *Let $k \geq 2$ be an integer and $q = (kp+1)/h$ a prime. If $p > h$ and $q > k+h$, then $M(p;q) \leq k+h$.*

Proof of Theorem 21. Let us assume that $\rho \leq \sigma$, the other case being similar. Using Lemma 7 and Lemma 5 we infer that the number of $0 \leq m \leq p-1$ with $b_{f(m)} = 1$ is at most $\rho+1$. Likewise the number of m with $b_{f(m+q)} = -1$ is at most

$p-1-\sigma$. By Kaplan's lemma it then follows that $a_{pqr}(k) \le \rho+1+(p-1-\sigma) = p+\rho-\sigma$. Since the number of $0 \le m \le p-1$ with $b_{f(m)} = -1$ is at most $p-1-\sigma$ and the number of m with $b_{f(m+q)} = 1$ is at most $\rho+1$, we infer that $a_{pqr}(k) \ge -(p+\rho-\sigma)$ and hence the result is proved. □

Theorem 22 *Let $q \equiv 1 (\text{mod } p)$. Them*

$$M(p;q) = \min\Big(\frac{q-1}{p}+1, \frac{p+1}{2}\Big).$$

Proof. For $p=3$ the result follows by Theorem 13, so assume $p \ge 5$. Sister Beiter [6], and independently Bloom [9], proved that $M(p;q) \le (p+1)/2$ if $q \equiv \pm 1 (\text{mod } p)$ (alternatively we invoke Theorem 9). By Corollary 2 we have $M(p;q) \le (q-1)/p+1$. By Lemma 11 the proof is then completed. □

Numerical experimentation suggests that in part b of Theorem 14 perhaps the condition $q > p^2/2$ can be dropped. By Theorem 22 the condition $q \ge (p-1)p/2+1$ in part c is optimal. In part d we need $q \ge (p-1)p/2-1$, for otherwise $M(p;q) < (p+1)/2$ by Corollary 1.

Lemma 19 *Let $p \ge 7$ be a prime such that $q = 2p-1$ is also a prime. Let $r > q$ be a prime such that $(p+q)r \equiv -2 (\text{mod } pq)$. Put $k = rq(p-1)/2+2p-pq$. Then $a_{pqr}(k) = 3$.*

Proof. Since $2p-q=1$, we have $\rho = 1$ and $\sigma = p-2$. Note that

$$\frac{2}{r} \equiv -(p+q) \equiv -p = -(\frac{q+1}{2}) \equiv \frac{q-1}{2} \ (\text{mod } q).$$

We infer that

$$f(0) \equiv \frac{k}{r} \equiv q(\frac{p-1}{2}) + \frac{2p}{r} \equiv q(\frac{p-1}{2}) + (\frac{q-1}{2})p \ (\text{mod } pq).$$

Since

$$-\frac{1}{r} \equiv (\frac{q+1}{2})p + (\frac{p+1}{2})q \ (\text{mod } pq),$$

we find that $f(1) \equiv f(0) - 1/r \equiv 0 (\text{mod } pq)$ and $f(2j+1) \equiv f(1) - 2j/r \equiv j(p+q) \ (\text{mod } pq)$. Note that $f(q+j) \equiv f(j) - q/r \equiv f(j) + (\frac{p-1}{2})q (\text{mod } pq)$. Using this information we arrive at Table 9, however without the columns headed $b_{f(m)}$ and $b_{f(m+q)}$. To establish the correctness of these columns it is enough, using that $f(0) < f(3)$ and $f(q+3) > f(q+1)$, to show that
(a) $f(q) \le k/r$;
(b) $f(q+1) > k/r$;
(c) $f(3) \le k/r$;
(d) $f(p-1) > k/r$.
(a) We have

$$f(q) = (\frac{q-1}{2})p + (p-1)q - pq = (\frac{q-1}{2})p - q.$$

Since

$$(\frac{q-1}{2})p - q < q(\frac{p-1}{2}) - \frac{q}{2} < q(\frac{p-1}{2}) - \frac{pq}{r} < \frac{k}{r},$$

it follows that $f(q) \leq k/r$.
(b) We have $f(q+1) = q(p-1)/2 > k/r$.
The inequalities c and d are left to the reader.

Using Table 9 and Kaplan's lemma we find that

$$a_{pqr}(k) = \sum_{m=0}^{p-1} (b_{f(m)} - b_{f(m+q)}) = 2 - -1 = 3,$$

finishing the proof. □

Table 9: A large coefficient for $q = 2p - 1$

$\overline{m}$	m	$[f(m)]_p$	$[f(m)]_q$	$[f(m+q)]_q$	$a_{f(m)}$	$b_{f(m)}$	$a_{f(m+q)}$	$b_{f(m+q)}$
0	0	$(q-1)/2$	$(p-1)/2$	$p-1$	0	0	-1	-1
	$\ldots$	$\ldots$	$\ldots$	$\ldots$	0	0	0	0
	$2j$	$(q-1)/2+j$	$(p-1)/2+j$	$j-1$	0	0	0	0
	$\ldots$	$\ldots$	$\ldots$	$\ldots$	0	0	0	0
	$p-1$	$3(q-1)/4$	$p-1$	$(p-3)/2$	-1	0	0	0
1	1	0	0	$(p-1)/2$	1	1	1	0
	3	1	1	$(p+1)/2$	1	1	1	0
	5	2	2	$(p+3)/2$	0	0	0	0
	$\ldots$	$\ldots$	$\ldots$	$\ldots$	0	0	0	0
	$2j+1$	j	j	$(p-1)/2+j$	0	0	0	0
	$\ldots$	$\ldots$	$\ldots$	$\ldots$	0	0	0	0
	$p-2$	$(p-3)/2$	$(p-3)/2$	$p-2$	0	0	0	0

In the $\overline{m} = 0$ part of the table, we have $1 \leq j \leq (p-3)/2$. In the $\overline{m} = 1$ part of the table, we have $3 \leq j \leq (p-5)/2$ if $p > 7$. If $p = 7$ there are only the $1, 3, 5$ rows and no further ones.

On combining the latter lemma with Corollary 1, one deduces that $M(p; 2p-1) = 3$ if $p \geq 5$ and $2p-1$ is a prime (that is we established Theorem 7).

11 Proofs of results announced in introduction

Proof of Theorem 1. By the definiton of $M(p;q)$ we have

$$\mathcal{A}(p;q) \subseteq [-M(p;q), M(p;q)] \cap \mathbb{Z}.$$

Let $r > q$ be a prime such that $A(pqr) = M(p;q)$ and suppose w.l.o.g. that $a_{pqr}(k) = M(p;q)$. Gallot and Moree [14] showed that we have $|a_n(k) - a_n(k-1)| \leq 1$ for ternary n (see Bachman [4] and Bzdęga [10] for alternative proofs). Since $a_{pqr}(k) = 0$ for every k large enough, it then follows that $0, 1, \ldots, M(p;q)$ are in $\mathcal{A}(p;q)$. By a result of Kaplan [15] (see Zhao and Zhang [21] for a reproof), we can find a prime $s \equiv -r (\mathrm{mod}\, pq)$ and an integer k_1 such that $a_{pqs}(k_1) = -M(p;q)$. By a similar arguments as above one then infers that $-M(p;q), -M(p;q)+1, \ldots, -1, 0$ are all in $\mathcal{A}(p;q)$. □

Proof of Theorem 2. See Zhao and Zhang [22].

Proof of Theorem 3. Let $\mathcal{R}_{pq}$ be a set of primes, all exceeding q such that every primitive residue class modulo pq is represented. By [15, Theorem 2] we have $A(pqr) = A(pqs)$ if $s \equiv r(\text{mod } pq)$ with s, r both primes exceeding q and hence

$$M(p;q) = \max\{A(pqr) : r \in \mathcal{R}_{pq}\}.$$

Since the computation of $\mathcal{R}_{pq}$ and $A(pqr)$ is a finite one, the computation of $M(p;q)$ is also finite. □

Proof of Theorem 4. See Section 2.

Proof of Theorem 6. Follows on combining Theorems 13, 15 and 17. □

Proof of Theorem 5. By Theorem 10 and Dirichlet's theorem the claim follows for $p = 13$. Using Lemmas 15 and 16 the result follows for $p = 11$. On invoking Theorems 6 and 20, the proof is then completed. □

Proof of Theorem 7. See the last sentence of Section 10.

Proof of Theorem 8. The first assertion follows by Theorem 6, so assume $p \geq 11$. Suppose that $p \nmid \mathfrak{f}_p$. Let $\beta \in \mathcal{B}(p)$. By the Chinese remainder theorem and Dirichlet's theorem there are infinitely many primes q_1 such that

$$q_1 \equiv 2(\text{mod } p) \text{ and } q_1 \equiv 1(\text{mod } \mathfrak{f}_p).$$

Further, there are infinitely many primes q_2 such that

$$q_2 \equiv \beta(\text{mod } p) \text{ and } q_2 \equiv 1(\text{mod } \mathfrak{f}_p).$$

By Lemma 9 we have $M(p;q_1) = (p+1)/2$. By Theorem 10, we have $M(p;q_2) > (p+1)/2$ for all q_2 large enough. By the definition of $\mathfrak{f}_p$ we must have $M(p;q_1) = M(p;q_2)$ for all q_i large enough. Contradiction. □

12 Conjectures, questions, problems

The open problem that we think is the most interesting is Conjecture 1. Note that if one could prove Conjecture 1 and getting an effective upper bound for the ternary conductor $\mathfrak{f}_p$ (say $16p$) and an effective upper bound for the minimal ternary prime (say p^3), then one has a finite procedure to compute $M(p)$.

Problem 1 *Bachman* [4] *introduced inclusion-exclusion polynomials. The inclusion-exclusion ternary polynomials generalize the ternary cyclotomic polynomials. Study $M(p;q)$ in this setting (here p and q can be any coprime natural numbers).*

Problem 2 *The analogue of $M(p;q)$ for inverse cyclotomic polynomials, see* [19], *can be defined. Study it.*

Question 1 *Can one compute the average value of $M(p;q)$, that is does the limit*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p<q\le x} M(p;q)$$

exist and if yes, what is its value ?

Question 2 *Is Theorem* 5 *still true if we put $\delta(13) = 1/3$ and cross out the words 'a subset having' ?*

Question 3 *If $q > p$ is prime and $q \equiv -2 (\mathrm{mod}\ p)$, then $M(p;q) = (p+1)/2$?*

Question 4 *Suppose that $p > 11$ is a prime.*
If $6p-1$ is prime, then $M(p, 6p-1) = 7$?
If $(5p-1)/2$ is prime, then $M(p, (5p-1)/2) = 7$?
If $(5p+1)/2$ is prime then $M(p, (5p+1)/2) = 7$?
Find more similar results.

Question 5 *Given an integer $k \ge 1$, does there exist $p_0(k)$ and a function $g_k(p)$ such that if $q \equiv 2/(2k+1)(\mathrm{mod}\ p)$, then $M(p;q) = (p+2k+1)/2$?*

Question 6 *Is it true that $M(11;q) = 6$ for all large enough q satisfying $q \equiv \pm 5(\mathrm{mod}\ 6)$? If so one can finish the computation of $M(11;q)$.*

Question 7 *Is it true that for q sufficiently large the values of $M(13;q)$, $M(17;q)$, $M(19;q)$ and $M(23;q)$ are given by the following tables ?*

$q(\mathrm{mod}\ 13)$	1	2	3	4	5	6	7	8	9	10	11	12
$M(13;q)$	7	7	7	8	8	7	7	8	8	7	7	7

$q(\mathrm{mod}\ 17)$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$M(17;q)$	9	9	9	10	10	9	10	9	9	10	9	10	10	9	9	9

$q(\mathrm{mod}\ 19)$	1	2	3	4	5	6	7	8	9
$M(19;q)$	10	10	10	12	11	9	11	11	10

$q(\mathrm{mod}\ 19)$	10	11	12	13	14	15	16	17	18
$M(19;q)$	10	11	11	9	11	12	10	10	10

$q(\mathrm{mod}\ 23)$	1	2	3	4	5	6	7	8	9	10	11
$M(23;q)$	12	12	12	14	14	11	13	11	14	13	12

$q(\mathrm{mod}\ 23)$	12	13	14	15	16	17	18	19	20	21	22
$M(23;q)$	12	13	14	11	13	11	14	14	12	12	12

`Acknowledgement`. The second author likes to thank the MPIM interns (in June 2008) N. Baghina, C. Budde, B. Jüttner and D. Sullivan for their (computer) assistance in computing Tables 7 and 8. However, the bulk of the paper was written whilst the third author was during two months in 2010 an intern at MPIM under the guidance of the second author. The third author would like to thank the MPIM for the possibility to do an internship and for the nice research atmosphere. He also thanks the second author for his mentoring and for having a sympathetic ear for any questions.

References

[1] G. Bachman, On the coefficients of ternary cyclotomic polynomials, *J. Number Theory* **100** (2003), 104–116.

[2] G. Bachman, Ternary cyclotomic polynomials with an optimally large set of coefficients, *Proc. Amer. Math. Soc.* **132** (2004), 1943–1950.

[3] G. Bachman, Flat cyclotomic polynomials of order three, *Bull. London Math. Soc.* **38** (2006), 53–60.

[4] G. Bachman, On ternary inclusion-exclusion polynomials, submitted for publication.

[5] A.S. Bang, Om Ligningen $\varphi_n(x) = 0$, *Nyt Tidsskrift for Mathematik (B)* **6** (1895), 6–12.

[6] M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial $F_{pqr}(x)$, *Amer. Math. Monthly* **75** (1968), 370–372.

[7] M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial F_{pqr}. II, *Duke Math. J.* **38** (1971), 591–594.

[8] M. Beiter, Coefficients of the cyclotomic polynomial $F_{3qr}(x)$, *Fibonacci Quart.* **16** (1978), 302–306.

[9] D.M. Bloom, On the coefficients of the cyclotomic polynomials, *Amer. Math. Monthly* **75** (1968), 372–377.

[10] B. Bzdęga, Bounds on ternary cyclotomic coefficients, arXiv:0812.4024, to appear in Acta Arithmetica.

[11] C. Cobeli, Y. Gallot and P. Moree, unpublished manuscript.

[12] W. Duke, J.B. Friedlander and H. Iwaniec, Equidistribution of roots of a quadratic congruence to prime moduli, *Ann. of Math.* (2) **141** (1995), 423–441.

[13] Y. Gallot and P. Moree, Ternary cyclotomic polynomials having a large coefficient, *J. Reine Angew. Math.* **632** (2009), 105–125.

[14] Y. Gallot and P. Moree, Neighboring ternary cyclotomic coefficients differ by at most one, *J. Ramanujan Math. Soc.* **24** (2009), 235–248.

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

[16] T.Y. Lam and K.H. Leung, On the cyclotomic polynomial $\Phi_{pq}(X)$, *Amer. Math. Monthly* **103** (1996), 562–564.

[17] E. Lehmer, On the magnitude of the coefficients of the cyclotomic polynomials, *Bull. Amer. Math. Soc.* **42** (1936), 389–392.

[18] H. Möller, Über die Koeffizienten des n-ten Kreisteilungspolynoms, *Math. Z.* **119** (1971), 33–40.

[19] P. Moree, Inverse cyclotomic polynomials, *J Number Theory* **129** (2009), 667–680.

[20] R. Thangadurai, On the coefficients of cyclotomic polynomials, *Cyclotomic fields and related topics* (Pune, 1999), 311–322, Bhaskaracharya Pratishthana, Pune, 2000.

[21] Jia Zhao and Xianke Zhang, On the coefficients of the cyclotomic polynomials of order three, arXiv:0910.2770.

[22] Jia Zhao and Xianke Zhang, A proof of the Corrected Beiter conjecture, arXiv:0910.2770.

12 bis rue Perrey, 31400 Toulouse, France.
e-mail: galloty@orange.fr

Max-Planck-Institut für Mathematik,
Vivatsgasse 7, D-53111 Bonn, Germany.
e-mail: moree@mpim-bonn.mpg.de

Sterbeckerstrasse 21, 58579 Schalksmühle, Germany
e-mail: Robert.wilms@rub.de