# Counter-examples to Sister Beiter's cyclotomic coefficient conjecture

Yves Gallot and Pieter Moree

**Abstract**

Let $\Phi_n(x)$ denote the $n$th cyclotomic polynomial. In 1968 Sister Marion Beiter conjectured that $a_n(k)$, the coefficient of $x^k$ in $\Phi_n(x)$, satisfies $|a_n(k)| \le (p+1)/2$ in case $n = pqr$ with $p < q < r$ primes. Since then several results towards establishing her conjecture have been proved (for example $|a_n(k)| \le 3p/4$). Here we show that, nevertheless, Beiter's conjecture is false for every $p \ge 11$. We also prove that given any $\epsilon > 0$ there exist infinitely many triples $(p_j, q_j, r_j)$ with $p_1 < p_2 < \ldots$ consecutive primes such that $|a_{p_j q_j r_j}(n_j)| > (2/3 - \epsilon)p_j$ for $j \ge 1$.

## 1 Introduction

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

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

where $\varphi$ is Euler's totient function and $\zeta_n$ a primitive $n$th root of unity. For the $k$ not in the range $[0, \varphi(n)]$ we put $a_n(k) = 0$. The coefficients $a_n(k)$ are known to be integral. The study of the $a_n(k)$ began with the startling observation that for small $n$ we have $|a_n(k)| \le 1$ (it thus seems, as D. Lehmer [10] worded it, that the primitive roots of unity conspire to achieve this smallness). The first counter-example to $|a_n(k)| \le 1$ occurs for $n = 105$: $a_{105}(7) = -2$. Note that 105 is the smallest odd integer having three prime factors. If $\omega_1(n)$ denotes the number of odd prime factors of $n$, then it is well-known that if $\omega_1(n) \le 2$, then $\Phi_n(x)$ is *flat*, that is all its coefficients satisfy $|a_n(k)| \le 1$. Thus $n = 105$ is the first candidate integer for $\Phi_n(x)$ to be non-flat. We see that with respect to the smallness of the coefficients the first non-trivial case arises when $\omega_1(n) = 3$. In this case some authors say that $\Phi_n(x)$ is *ternary*. Then we write $n = pqr$ with $2 < p < q < r$.

We define the *height* of $\Phi_n(x)$ to be $\max\{|a_n(k)| : 0 \le k \le \varphi(n)\}$ and denote it by $A(n)$. In 1968 Sister Marion Beiter [3] put forward the following conjecture (which she repeated in 1971 [4]).

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

**Conjecture 1** (Sister Marion Beiter, 1968). *If* $2 < p < q < r$ *are primes, then* $A(pqr) \le \frac{p+1}{2}$.

Note that $A(2qr) = 1$. In case either $q$ or $r \equiv \pm 1 (\bmod p)$ Beiter proved her conjecture. This result was extended by Bachman [1].

**Theorem 1** (Gennady Bachman, 2003). *If either* $q$ *or* $r$ *is congruent to* $\pm 1$ *or* $\pm 2$ *modulo* $p$, *then* $A(pqr) \le (p+1)/2$. *If* $q$ *or* $r$ *is congruent to* $(p \pm 1)/2$ *modulo* $p$, *then* $A(pqr) \le (p+3)/2$.

In a further paper Beiter [4] points out that her conjecture is true for $p \le 5$ and shows that $A(pqr) \le p - \lfloor p/4 \rfloor$, thus improving on a result from Bang [2] proved in 1895, to the effect that $A(pqr) \le p - 1$. The best known general upper bound to date is due to Bachman [1], who proved that $A(pqr) \le p - \lceil p/4 \rceil$. In the same paper Bachman showed:

**Theorem 2** (Gennady Bachman, 2003). *Let* $q^*$ *and* $r^*$, $0 < q^*, r^* < p$ *be the inverses of* $q$ *and* $r$ *modulo* $p$ *respectively. Set* $a = \min(q^*, r^*, p-q^*, p-r^*)$. *Then* $A(pqr) \le \min(\frac{p-1}{2} + a, p - a)$.

H. Möller [12] indicated for every prime $p > 3$ a cyclotomic polynomial $\Phi_{pqr}(x)$ having a coefficient equal to $(p+1)/2$. This shows that Beiter's conjecture is best possible, if true. In particular Möller proved:

**Theorem 3** (Herbert Möller, 1971). *Let* $3 < p < q < r$ *be prime numbers satisfying* $q \equiv 2 (\bmod p)$ *and* $r = (mpq - 1)/2$ *for some integer* $m$. *Then*

$$a_{pqr}(\frac{1}{2}(p-1)(qr+1)) = \frac{p+1}{2}.$$

Earlier Emma Lehmer [11] had shown that for $q$ and $r$ as in the latter Theorem we have $a_{pqr}(\frac{1}{2}(p-3)(qr+1)) = (p-1)/2$. On combining Möller's result with Theorem 1 we infer that for his choice of $p, q$ and $r$ we have $A(pqr) = (p+1)/2$.

Let $M(p)$ be the maximum of the heights of the ternary cyclotomic polynomials, where $p$ is the smallest prime factor of $n$. The case $p = 3$ was investigated in detail by Beiter [5], who found that $M(3) = 2$. Beiter's conjecture in combination with $M(3) = 2$ and Möller's result leads to the following conjecture.

**Conjecture 2** *For* $p > 2$ *we have* $M(p) = \frac{p+1}{2}$.

We will show that our main result, presented below, can be used to infer that Beiter's conjecture is 'very false'.

**Theorem 4** *Let* $p$ *be a prime. Given an* $1 \le \beta \le p$ *we let* $\beta^*$ *be the unique integer* $1 \le \beta^* \le p - 1$ *with* $\beta\beta^* \equiv 1 (\bmod p)$.

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

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

*For every prime* $q \equiv \beta (\bmod p)$ *with* $q > q_-(p)$ *and* $\beta \in \mathcal{B}_-(p)$, *there exists a prime* $r_- > q$ *and an integer* $n_-$ *such that* $a_{pqr_-}(n_-) = \beta_- - p$, *where* $q_-(p), r_-$

*and $n_-$ can be explicitly given.*

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

$$1 \le \beta \le \frac{p-3}{2},\ \beta + \beta^* \ge p,\ \beta^* \le 2\beta, \tag{2}$$

*For every prime $q \equiv \beta (\mathrm{mod}\ p)$ with $q > q_+(p)$ and $\beta \in \mathcal{B}_+(p)$ there exists a prime $r_+ > q$ and an integer $n_+$ such that $a_{pqr_+}(n_+) = p - \beta$, where $q_+(p), r_+$ and $n_+$ can be explicitly given. In case $\beta \in \mathcal{B}_+(p)$ and $\beta + \beta^* = p$, then $A(pqr_+) = p - \beta$.*

*Put $\mathcal{B}(p) = \mathcal{B}_-(p) \cup \mathcal{B}_+(p)$. If $\mathcal{B}(p)$ is non-empty, then*

$$M(p) \ge p - \min\{\mathcal{B}(p)\} > \frac{p+1}{2},$$

*and so Beiter's conjecture is false for the prime $p$.*

Explicit choices of $q_-(p), r_-$ and $n_-$ are given in Theorem 10 and explicit choices of $q_+(p), r_+$ and $n_+$ in Theorem 11, see also Tables 7 and 8.

Note that the sets $\mathcal{B}_-(p)$ and $\mathcal{B}_+(p)$ are disjoint. For $p \le 11$ the set $\mathcal{B}(p)$ turns out to be empty. For $11 \le p \le 73$ it is given in Table 1. The underlined element is $(p-3)/2$ and for this range always turns out to be in $\mathcal{B}(p)$. The final column gives a lower bound for $M(p)$. The table shows that Beiter's conjecture is false for $11 \le p \le 73$.

**Proposition 1** *For $p \ge 11$, $\mathcal{B}(p)$ is non-empty and* $\max\{\mathcal{B}(p)\} = (p-3)/2$.

*Proof.* Consider $\beta = (p-3)/2$. If $p \equiv 1(\mathrm{mod}\ 3)$, then $\beta^* = 2(p-1)/3$ and one checks that $\beta \in \mathcal{B}_+(p)$. If $p \equiv 2(\mathrm{mod}\ 3)$, then $\beta^* = (p-2)/3$ and one checks that $\beta \in \mathcal{B}_-(p)$. □

**Table 1:** `The sets` $\mathcal{B}_-(p)$, $\mathcal{B}_+(p)$ and $\mathcal{B}(p)$

| $p$ | $\mathcal{B}_-(p)$ | $\mathcal{B}_+(p)$ | $\mathcal{B}_-(p) \cup \mathcal{B}_+(p) = \mathcal{B}(p)$ | $p - \min \mathcal{B}(p)$ |
|---|---|---|---|---|
| 11 | $\{\underline{4}\}$ | $\emptyset$ | $\{4\}$ | 7 |
| 13 | $\emptyset$ | $\{\underline{5}\}$ | $\{5\}$ | 8 |
| 17 | $\{\underline{7}\}$ | $\emptyset$ | $\{7\}$ | 10 |
| 19 | $\emptyset$ | $\{\underline{8}\}$ | $\{8\}$ | 11 |
| 23 | $\{\underline{10}\}$ | $\{9\}$ | $\{9, 10\}$ | 14 |
| 29 | $\{\underline{13}\}$ | $\{12\}$ | $\{12, 13\}$ | 17 |
| 31 | $\{13\}$ | $\{\underline{14}\}$ | $\{13, 14\}$ | 18 |
| 37 | $\emptyset$ | $\{\underline{17}\}$ | $\{17\}$ | 20 |
| 41 | $\{18, \underline{19}\}$ | $\{17\}$ | $\{17, 18, 19\}$ | 24 |
| 43 | $\{18\}$ | $\{19, \underline{20}\}$ | $\{18, 19, 20\}$ | 25 |
| 47 | $\{\underline{22}\}$ | $\{18, 20\}$ | $\{18, 20, 22\}$ | 29 |
| 53 | $\{\underline{25}\}$ | $\{22, 23, 24\}$ | $\{22, 23, 24, 25\}$ | 31 |
| 59 | $\{23, 26, \underline{28}\}$ | $\{27\}$ | $\{23, 26, 27, 28\}$ | 36 |
| 61 | $\{25, 28\}$ | $\{27, \underline{29}\}$ | $\{25, 27, 28, 29\}$ | 36 |
| 67 | $\emptyset$ | $\{26, 30, \underline{32}\}$ | $\{26, 30, 32\}$ | 40 |
| 71 | $\{32, 33, \underline{34}\}$ | $\{27, 29, 30, 31\}$ | $\{27, 29, 30, 31, 32, 33, 34\}$ | 44 |
| 73 | $\{33\}$ | $\{27, 30, 34, \underline{35}\}$ | $\{27, 30, 33, 34, 35\}$ | 46 |

From Theorem 4, Proposition 1 and Dirichlet's theorem on arithmetic progressions the following result is inferred.

**Theorem 5** *Suppose $p \geq 11$ is a prime. Then the set of $q$ for which $A(pqr) > (p+1)/2$ for some prime $r$ has a positive lower density $\underline{\delta}$ satisfying*

$$\underline{\delta} \geq \frac{|\mathcal{B}_+(p)| + |\mathcal{B}_-(p)|}{p-1} \geq \frac{1}{p-1} > 0,$$

*and hence Beiter's conjecture is false for this prime.*

The elementary method of proof of Proposition 1 allows one to prove, e.g., that if $p \equiv 23 \pmod{24}$ and $p > 23$, then $M(p) \geq (5p-3)/8$ and more generally it allows one to indicate for every $\epsilon > 0$ an arithmetic progression such that for all primes larger than some explicit number in this progression we have $M(p) \geq (\frac{2}{3} - \epsilon)p$ (Proposition 4). On invoking a result from the theory of inverses modulo $p$ it can be even shown that the latter lower bound holds for *all* primes $p$ sufficiently large.

**Theorem 6** *Let $\epsilon > 0$. Then $\frac{2}{3}(1-\epsilon)p \leq M(p) \leq \frac{3}{4}p$ for every sufficiently large prime $p$.*

In Table 2 we give for some small primes $p$ intervals $[a, b]$ such that $a \leq M(p) \leq b$. The number $b = p - \lceil p/4 \rceil$ and $a = |a_{pqr}(n)|$, showing that $M(p) \geq a$. The values of $a$ are the largest known to us and were found by extensive computer calculation.

**Table 2:** `Interval for` $M(p)$

| $p$ | $(p+1)/2$ | $q$ | $r$ | $n$ | $M(p)$ interval | $[2p/3]$ | $\delta(p)$ |
|---|---|---|---|---|---|---|---|
| 3 | 2 | 5 | 7 | 7 | [2, 2] | 2 | 0 |
| 5 | 3 | 7 | 11 | 119 | [3, 3] | 3 | 0 |
| 7 | 4 | 11 | 37 | 963 | [4, 5] | 4 | $\geq 0$ |
| 11 | 6 | 19 | 601 | 34884 | [7, 8] | 7 | $\geq 1$ |
| 13 | 7 | 31 | 1097 | 137160 | [8, 9] | 8 | $\geq 1$ |
| 17 | 9 | 29 | 41 | 4801 | [10, 12] | 11 | $\geq 1$ |
| 19 | 10 | 53 | 859 | 318742 | [12, 14] | 12 | $\geq 2$ |
| 23 | 12 | 41 | 4903 | 1583731 | [14, 17] | 15 | $\geq 2$ |
| 29 | 15 | 127 | 7793 | 8915220 | [18, 21] | 19 | $\geq 3$ |
| 31 | 16 | 89 | 4519 | 4424131 | [19, 23] | 20 | $\geq 3$ |
| 37 | 19 | 47 | 1217 | 743670 | [22, 27] | 24 | $\geq 3$ |
| 41 | 21 | 71 | 97 | 96529 | [26, 30] | 27 | $\geq 5$ |
| 43 | 22 | 53 | 2963 | 2358548 | [26, 32] | 28 | $\geq 4$ |
| 47 | 24 | 347 | 12113 | 64756445 | [29, 35] | 31 | $\geq 5$ |
| 53 | 27 | 61 | 17377 | 18037438 | [33, 39] | 35 | $\geq 6$ |
| 59 | 30 | 67 | 21247 | 27047555 | [37, 44] | 39 | $\geq 7$ |
| 61 | 31 | 191 | 30203 | 126913006 | [38, 45] | 40 | $\geq 7$ |
| 67 | 34 | 191 | 91127 | 417817361 | [42, 50] | 44 | $\geq 8$ |
| 71 | 36 | 311 | 13327 | 91183645 | [44, 53] | 47 | $\geq 8$ |
| 73 | 37 | 83 | 4241 | 9156474 | [46, 54] | 48 | $\geq 9$ |

The last column gives information about the difference $\delta(p) := M(p) - (p+1)/2$. In case $\delta(p) > 0$ the associated $p, q$ and $r$ give rise to a counter-example to Beiter's conjecture.

If $\beta \in \mathcal{B}_-(p)$, then $p \le 3\beta$ and $p - \beta \le 2p/3$. If $\beta \in \mathcal{B}_+(p)$, then $p \le \beta + \beta^* \le 3\beta$ and so $\beta \ge p/3$ and hence $p - \beta \le 2p/3$. Thus Theorem 4 only allows one to find counter-examples $\le 2p/3$ to Beiter's conjecture. Extensive numerical computations gave many counter-examples not covered by Theorem 4, but all of them are $\le 2p/3$. Thus the strongest corrected version of Beiter's conjecture which we can presently neither disprove nor prove is as follows.

**Conjecture 3** (Corrected Beiter conjecture). *We have* $M(p) \le 2p/3$.

Note that it implies that Beiter's original conjecture is correct for $p = 7$. This is at present still an open problem. If $A(7qr) > 4$, then we must have $q \equiv \pm 3 (\text{mod } 7)$ by Theorem 1.

Our final result deals with some apparent variations of $M(p)$. Let $M_+(p)$ and $M_-(p)$ be the maximum, respectively minimum of the coefficients of the ternary cyclotomic polynomials with $p$ the smallest prime factor of $n$.

**Theorem 7** *We have* $M_-(p) = M_+(p) = M(p)$.

For a nice survey of properties of coefficients of cyclotomic polynomials see Thangadurai [15].

## 1.1 Some results of Nathan Kaplan

Using the identity

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

Kaplan [8] proved the following lemma.

**Lemma 1** (Nathan Kaplan, 2007). *Let $n \ge 0$ be an integer. Put*

$$b_i = \begin{cases} a_{pq}(i) & \text{if } ri \le n; \\ 0 & \text{otherwise.} \end{cases}$$

*We have*

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

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

Since the $a_{pq}(i)$ are easily computed, Kaplan's lemma is actually useful. Indeed, his lemma plays a crucial role in our counter-example constructions. A nice feature of the lemma is that it works for every $n \ge 0$. Thus if it shows that $|a_{pqr}(n)| \ne 0$, then we know that $n \le \varphi(pqr)$. In our counter-example constructions this saves us from checking that for the chosen $n$ we have $n \le \varphi(pqr)$.

The next lemma gives the values of $a_{pq}(i)$. For a proof see e.g. Lam and Leung [9] or Thangadurai [15],

**Lemma 2** *Let $p < q$ be odd primes. Let $\rho$ and $\sigma$ be the (unique) non-negative integers for which $(p-1)(q-1) = \rho p + \sigma q$ 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 $\alpha_1 p \equiv m (\mathrm{mod}\ q)$ and $0 \leq \beta_1 \leq p-1$ the unique integer such that $\beta_1 q \equiv m (\mathrm{mod}\ p)$. The cyclotomic coefficient $a_{pq}(m)$ equals*

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

The following result of Kaplan [8] together with Dirichlet's theorem shows that given one counter-example $(p, q, r)$ infinitely many counter-examples to Beiter's conjecture exist with the same values of $p$ and $q$.

**Theorem 8** (Nathan Kaplan, 2007). *For any prime $s > q$ such that $s \equiv \pm r (\mathrm{mod}\ pq)$ we have $A(pqr) = A(pqs)$.*

`Example`. Put $p = 17$ and $q = 29$. By computation one finds that $A(pq \cdot 1931) = 10$. On applying Kaplan's result one then finds from this that also $A(pq \cdot 2917) = A(pq \cdot 2999) = 10$.

Implicit in Kaplan's proof of Theorem 8 is the following result using which we immediately infer that Theorem 7 holds true.

**Proposition 2** *Suppose that $a_{pqr}(n) = m$. Write $n = [\frac{n}{r}]r + n_0$ with $0 \leq n_0 < r$.*
1) *Let $s > r$ be a prime satisfying $s \equiv r (\mathrm{mod}\ pq)$. Then*

$$a_{pqs}\Big(\Big[\frac{n}{r}\Big]s + n_0\Big) = m.$$

2) *Let $t > pq$ be a prime satisfying $t \equiv -r (\mathrm{mod}\ pq)$. Let $0 \leq n_1 < pq$ be the unique integer such that $n_1 \equiv q + p - 1 - n_0 (\mathrm{mod}\ pq)$. Then*

$$a_{pqt}\Big(\Big[\frac{n}{r}\Big]t + n_1\Big) = -m.$$

# 2 A counter-example construction for $p = 11$

Using Lemma 1 and Lemma 2 (we leave this as an exercise to the reader) one finds that for the $p, q$ and $r$ in the Möller construction we have $b_{f(m)} = 1$ for $0 \leq m \leq (p-1)/2$ and $b_{f(m)} = 0$ for the remaining $m$ in (3), giving $a_{pqr}(n) = (p+1)/2$. Likewise, for the Lehmer example we find $b_{f(m)} = 1$ for $0 \leq m \leq (p-3)/2$ and $b_{f(m)} = 0$ for the remaining $m$, giving $a_{pqr}(n) = (p-1)/2$.

For the counter-examples to Beiter's conjecture we find in general rather more complicated vectors $(b_{f(0)}, \ldots, b_{f(p-1)})$ and $(b_{f(q)}, \ldots, b_{f(q+p-1)})$. However, some of them are regular enough as to build a general construction on. We give an example which is intended as an appetizer that should help the reader digest more easily the general construction given in Theorem 10. Notice that Theorem 10 implies Theorem 9. The first few counter-examples produced by Theorem 9 are given in Table 3.

**Table 3:** `Some counter-examples produced by Theorem 9`

| $p$ | $q$ | $\alpha$ | $r$ | $n$ | $a_{pqr}(n)$ |
|---|---|---|---|---|---|
| 11 | 59 | 2 | 877 | 175410 | -7 |
| | 103 | 4 | 1229 | 381000 | -7 |
| | 191 | 6 | 4639 | 3173086 | -7 |
| | | 7 | 16937 | 10280769 | -7 |
| | 257 | 8 | 3011 | 2788196 | -7 |
| | | 9 | 1163 | 987397 | -7 |
| | | 10 | 8731 | 6740342 | -7 |
| | 367 | 12 | 56999 | 72844732 | -7 |
| | | 13 | 811 | 974021 | -7 |
| | | 14 | 39157 | 44012478 | -7 |

**Theorem 9** *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*

$$\frac{q}{33} < \alpha \leq \frac{3q-1}{77}.$$

*Then $a_{11qr}(10 + (6q - 77\alpha)r) = -7$.*

*Proof.* Put $p = 11$ and $n = 10 + (6q - 77\alpha)r$. Note that $n \geq 10$. We will compute $a_{pqr}(n)$ using Lemma 1. Since this will have -7 as outcome, it follows that $n \leq \varphi(pqr)$. Observe that

$$0 \leq \frac{n-10}{r} = (q - 7\alpha)p + 6q - pq \leq 6q < pq$$

and so $f(10) = (q - 7\alpha)p + 6q - pq$. This expresses $f(10)$ as a linear combination in $p$ and $q$. Let $0 \leq r_1 < pq$ be the unique integer with $r_1 \equiv -\frac{1}{r} (\text{mod } pq)$. It is easy to see that $r_1 = q - \alpha p$. On noting that $f(m) \equiv f(10) + (m-10)r_1 \equiv f(10) + (m-10)(q - \alpha p)$, we infer that $f(m)$ is congruent modulo $pq$ to the corresponding entry in Table 4 (and likewise for $f(m+q)$ on noting that $-q/r \equiv 4q (\text{mod } pq)$ and $f(m+q) \equiv f(m) - q/r \equiv f(m) + 4q (\text{mod } pq)$). In the $f(m+q)$ column we trivially have

$$0 \leq f(q) < \cdots < f(q+p-1) = 10q - 7\alpha p \leq 10q < pq.$$

Using this we infer that $f(m+q)$ is actually equal to the corresponding entry in Table 4. In the $f(m)$ column we have $0 \leq f(0) < \cdots < f(4) < pq$ and on using that $\alpha \leq q/(2p)$ we find $0 \leq f(5) < \cdots < f(10) < 6q < pq$. Again we see that $f(m)$ is actually equal to the corresponding entry in Table 4.

Now we are ready to invoke Lemma 2. One computes that $\sigma = 2$ and $\rho = (8q - 10)/11$. The conditions on $\alpha$ ensure that $q - 7\alpha \geq \rho + 1$ and $3\alpha \leq \rho$. On applying Lemma 2 we then infer that $c_m := a_{pq}(f(m))$ and $c_{m+q} := a_{pq}(f(m+q))$ are as given in Table 4. Since $[n/r] = f(10)$ it follows, by Lemma 1 that $b_m = c_m$ if $f(m) \leq f(10)$ and $b_m = 0$ otherwise. Thus to compute say the $b_m$ column we have $b_m = 0$ if $c_m = 0$. If $c_m \neq 0$ we have

$$b_m = \begin{cases} c_m & \text{if } f(m) \leq f(10); \\ 0 & \text{otherwise.} \end{cases}$$

Note that clearly $f(7) < .... < f(10)$. It then follows that the $b_m$ column equals the $c_m$ column. Next let us determine the $c_{m+q}$ column. We claim that $f(q) < f(q+1) < f(q+2) < f(10)$. To establish this we have to check that $\alpha p + 2q < (q-7\alpha)p - 5q$. Note that $f(q+4) < \cdots < f(q+10)$. The conditions on $\alpha$ ensure that $f(q+4) > f(10)$ and we see that $f(10) < f(q+4) < \cdots < f(q+10)$ and thus $b_{q+4} = \ldots = b_{q+10} = 0$. Finally, on applying Lemma 1 we infer that

$$a_{pqr}(n) = \sum_{m=0}^{p-1} b_{f(m)} - \sum_{m=0}^{p-1} b_{f(m+q)} = -4 - 3 = -7.$$

This completes the proof. □

`Remark`. Note that the conditions imposed on $\alpha$ are such that $\alpha \le q/(2p)$, $3\alpha \le \rho$, $q - 7\alpha \ge \rho + 1$, $f(q+4) > f(10)$ and $f(q+2) \le f(10)$.

**Table 4:** `A counter-example construction for` $p = 11$

| $m$ | $f(m)$ | $c_m$ | $b_m$ | $m+q$ | $f(m+q)$ | $c_{m+q}$ | $b_{m+q}$ |
|---|---|---|---|---|---|---|---|
| 0 | $3\alpha p + q(p-4)$ | 0 | 0 | $q$ | $3\alpha p$ | 1 | 1 |
| 1 | $2\alpha p + q(p-3)$ | 0 | 0 | $q+1$ | $2\alpha p + q$ | 1 | 1 |
| 2 | $\alpha p + q(p-2)$ | 0 | 0 | $q+2$ | $\alpha p + 2q$ | 1 | 1 |
| 3 | $q(p-1)$ | 0 | 0 | $q+3$ | $3q$ | 0 | 0 |
| 4 | $(q-\alpha)p$ | 0 | 0 | $q+4$ | $(q-\alpha)p + 4q - pq$ | -1 | 0 |
| 5 | $(q-2\alpha)p + q - pq$ | 0 | 0 | $q+5$ | $(q-2\alpha)p + 5q - pq$ | -1 | 0 |
| 6 | $(q-3\alpha)p + 2q - pq$ | 0 | 0 | $q+6$ | $(q-3\alpha)p + 6q - pq$ | -1 | 0 |
| 7 | $(q-4\alpha)p + 3q - pq$ | -1 | -1 | $q+7$ | $(q-4\alpha)p + 7q - pq$ | -1 | 0 |
| 8 | $(q-5\alpha)p + 4q - pq$ | -1 | -1 | $q+8$ | $(q-5\alpha)p + 8q - pq$ | -1 | 0 |
| 9 | $(q-6\alpha)p + 5q - pq$ | -1 | -1 | $q+9$ | $(q-6\alpha)p + 9q - pq$ | -1 | 0 |
| 10 | $(q-7\alpha)p + 6q - pq$ | -1 | -1 | $q+10$ | $(q-7\alpha)p + 10q - pq$ | -1 | 0 |

# 3 General counter-example construction

## 3.1 The negative coefficient case

We now establish a more general counter-example construction. The approach will be similar to that of the previous section. For reasons of space the analogue of Table 4, Table 5, is split into two tables, for $f(m)$, respectively $f(m+q)$.

**Table 5A:** `General negative coefficient construction,` $f(m)$ `case`

| $m$ | $f(m)$ | $c_m$ | $b_m$ |
|---|---|---|---|
| 0 | $(\sigma+1)\alpha p+(p-\beta)q$ | 0 | 0 |
| 1 | $\sigma\alpha p+(p-\beta+1)q$ | 0 | 0 |
| $\cdots$ | $\cdots$ | 0 | 0 |
| $\sigma+1$ | $0\cdot p+(\sigma+1+p-\beta)q$ | 0 | 0 |
| $\sigma+2$ | $(q-\alpha)p+(\sigma+2+p-\beta)q-pq$ | -1 | 0 |
| $\cdots$ | $\cdots$ | -1 | 0 |
| $\beta-1$ | $(q-(\beta-\sigma-2)\alpha)p+(p-1)q-pq$ | -1 | 0 |
| $\beta$ | $(q-(\beta-\sigma-1)\alpha)p+0\cdot q$ | 0 | 0 |
| $\beta+1$ | $(q-(\beta-\sigma)\alpha)p+1\cdot q-\delta_1 pq$ | 0 | 0 |
| $\cdots$ | $\cdots$ | 0 | 0 |
| $\beta+\sigma$ | $(q-(\beta-1)\alpha)p+\sigma q-\delta_\sigma pq$ | 0 | 0 |
| $\beta+\sigma+1$ | $(q-\beta\alpha)p+(\sigma+1)q-pq$ | -1 | -1 |
| $\cdots$ | $\cdots$ | -1 | -1 |
| $\beta+k$ | $(q-(\beta-\sigma-1+k)\alpha)p+kq-pq$ | -1 | -1 |
| $\cdots$ | $\cdots$ | -1 | -1 |
| $p-1$ | $(q-(p-\sigma-2)\alpha)p+(p-\beta-1)q-pq$ | -1 | -1 |

In Table 5A $\delta_j$ is the unique integer such that the corresponding entry is in the interval $[0, pq)$.

**Table 5B:** `General negative coefficient construction,` $f(m+q)$ `case`

| $m+q$ | $f(m+q)$ | $c_{m+q}$ | $b_{m+q}$ |
|---|---|---|---|
| $q$ | $(\sigma+1)\alpha p$ | 1 | 1 |
| $q+1$ | $\sigma\alpha p+q$ | 1 | 1 |
| $\cdots$ | $\cdots$ | 1 | 1 |
| $q+\sigma$ | $\alpha p+\sigma q$ | 1 | 1 |
| $q+\sigma+1$ | $0\cdot p+(\sigma+1)q$ | 0 | 0 |
| $q+\sigma+2$ | $(q-\alpha)p+(\sigma+2)q-pq$ | -1 | 0 |
| $\cdots$ | $\cdots$ | -1 | 0 |
| $q+p-1$ | $(q-(p-\sigma-2)\alpha)p+(p-1)q-pq$ | -1 | 0 |

**Lemma 3** *Let $p$ be a prime. Let $1\le\beta\le(p-3)/2$. Let $q>p$ be a prime satisfying $q\equiv\beta(\mathrm{mod}\ p)$ and $r>q$ be a prime satisfying $qr\equiv-1(\mathrm{mod}\ p)$. Let $1\le\alpha\le q-1$ be the unique integer such that $pr\alpha\equiv1(\mathrm{mod}\ q)$. Put*

$$w_-=(p-\beta-1)q-(p-\sigma-2)\alpha p,$$

*where $\rho$ and $\sigma$ are uniquely determined by $(p-1)(q-1)=\rho p+\sigma q$, $\rho,\sigma\ge0$. Suppose that*

$$p\ge\beta+\sigma+2,\ \beta\ge\sigma+2$$

*and*

$$\alpha\le\frac{q(\sigma+1)}{p\beta}, \tag{4}$$

$$\alpha \le \frac{q(p-1-\sigma)-(p-1)}{p(\sigma+1)}, \tag{5}$$

$$\alpha \le \frac{q(\sigma+1)-1}{p(p-\sigma-2)}, \tag{6}$$

$$\alpha \le \frac{q(p-\sigma-1-\beta)}{p(p-\sigma-1)}, \tag{7}$$

*and*

$$\alpha > \frac{q(p-3-\sigma-\beta)}{p(p-\sigma-3)}, \tag{8}$$

*then* $a_{pqr}(p-1+rw)=\beta-p$.

`Remark`. The conditions (4), (5), (6), (7) and (8) are used to ensure that respectively, $f(\beta+\sigma+1)\ge 0$, $(\sigma+1)\alpha\le\rho$, $q-(p-\sigma-2)\alpha\ge\rho+1$, $f(q+\sigma)\le f(p-1)$ and $f(q+\sigma+2)>f(p-1)$.

*Proof of Lemma* 3. Reasoning as in the proof of Theorem 9 we find that $f(m)$ and $f(m+q)$ are congruent modulo $pq$ to the numbers given in Table 5A, respectively 5B.

In Table 5A we distinguish 3 ranges: $0\le m\le\beta$, $\beta+1\le m\le\beta+\sigma$ and $\beta+\sigma+1\le m\le p-1$. In the first range the entries 0 up to $\beta$ are non-negative and in ascending order. Since the entry for $\beta$ is $< pq$ it follows that for $0\le m\le\beta$, $f(m)$ is actually equal to the corresponding entry given in Table 5A. Since $(\sigma+1)\alpha\le\rho$ and $p-\beta\ge\sigma+1$ it follows by Lemma 1 that $c_m=0$ (and hence $b_m=0$) for $m=0,\ldots,\sigma+1$. For $\sigma+2\le m\le\beta-1$ one finds that $c_m=-1$. Since

$$f(\sigma+2)=f(q+\sigma+2)+(p-\beta)q>f(q+\sigma+2)>f(p-1),$$

we infer that $b_m=0$ for $\sigma+2\le m\le\beta-1$. Clearly $b_\beta=c_\beta=0$.

In the second range we have, for $1\le k\le\sigma$,

$$(q-(\beta-\sigma+k-1)\alpha)p+kq-\delta_k pq$$

as entry in row $\beta+k$, where a priori $\delta_k$ is an integer. Since

$$q-1\ge q-(\beta-\sigma+k-1)\alpha\ge q-(p-\sigma-2)\alpha\ge\rho+1>0,$$

we find that $0\le(q-\beta-\sigma+k-1)\alpha)p+kq<2pq$ and hence $\delta_k\in\{0,1\}$. By Lemma 1 again we now find that $c_m=b_m=0$ for $\beta+1\le m\le\beta+\sigma$.

In the range $\beta+\sigma+1\le m\le p-1$ the entries in Table 5A are in ascending order and the final entry is less than $pq$. Since $\alpha\le(\sigma+1)q/(\beta p)$, it follows that the $\beta+\sigma+1$ entry in the table is $\ge 0$. It follows that $f(m)$ is actually equal to the corresponding entry in Table 5A. By Lemma 1 it now follows that $c_m=-1$ for $\beta+\sigma+1\le m\le p-1$. Since $f(m)\le f(p-1)$ for $\beta+\sigma+1\le m\le p-1$ we infer that also $b_m=-1$ in this range.

Establishing the correctness of the $f(m+q)$ and $c_{m+q}$ column is straightforward and left to the reader. Note that once we have $f(q+\sigma)\le f(p-1)$ and

$f(q+\sigma+2) > f(p-1)$, the $b_{m+q}$ column is as given in the table. That these inequalities hold is ensured by conditions (7), respectively (8). Finally on applying Lemma 1 we infer that

$$a_{pqr}(p-1+rw_-) = -\sum_{j=\beta+\sigma+1}^{p-1} 1 - \sum_{j=q}^{q+\sigma} 1 = -(p-1-\beta-\sigma)-(\sigma+1) = \beta - p.$$

This concludes the proof. □

In the next lemma the set of *real* numbers $\alpha$ satisfying (4), (5), (6), (7) and (8) is determined.

**Lemma 4** *Let $\mathcal{I}$ be the set of real numbers satisfying* (4), (5), (6), (7) and (8) *and suppose the conditions of Lemma* 3 *are satisfied. Then the set $\mathcal{I}$ is non-empty iff $p \le \beta + 2\beta^* + 1$. In that case*

$$\mathcal{I} = \begin{cases} \left(\frac{q}{p}\Big(1-\frac{\beta}{p-\beta^*-2}\Big), \frac{q}{p}\Big(1-\frac{\beta}{p-\beta^*}\Big)\right] & \text{if } p < \beta+2\beta^*+1; \\ \left(\frac{q}{p}\Big(1-\frac{\beta}{p-\beta^*-2}\Big), \frac{q\beta^*-1}{p(p-\beta^*-1)}\right] & \text{if } p = \beta+2\beta^*+1. \end{cases}$$

*If $\mathcal{I}$ is non-empty then it consists of positive reals only.*

*Proof.* From $(\rho+1)p+(\sigma+1)q = pq+1$ we infer that $(\sigma+1)q \equiv 1(\text{mod } p)$ and hence $\sigma \equiv 1/q - 1(\text{mod } p)$. Since $q \equiv \beta(\text{mod } p)$, we infer that $\sigma = \beta^* - 1$. Note that if (6) is satisfied then, since $p-\sigma-2 \ge \beta$, automatically (4) is satisfied. Note that if $\alpha$ satisfies (6), then

$$\alpha \le \frac{q(\sigma+1)}{p(p-\sigma-3)}.$$

Now if $\alpha$ is also to satisfy (8), then we must have $\sigma+1 > p-3-\sigma-\beta$ and so $p \le 2\sigma+3+\beta$. Thus if $p > \beta+2\beta^*+1$, then $\mathcal{I}$ is empty and hence we may assume that $p \le \beta+2\beta^*+1$. By (7) and since $p \ge 2\sigma+3 = 2\beta^*+1$ we infer that

$$\alpha \le \frac{q}{p} \le \frac{q(p-2-\sigma)}{p(\sigma+1)} \le \frac{q(p-1-\sigma)-(p-1)}{p(\sigma+1)},$$

and hence the condition (5) is also superfluous. Note that the inequality

$$\frac{q(p-\sigma-1-\beta)}{p(p-\sigma-1)} \le \frac{q(\sigma+1)-1}{p(p-\sigma-2)}$$

can be rewritten as

$$p \le \beta+3+2\sigma-\frac{1}{q}-\frac{\beta}{p-\sigma-1}.$$

We observe that

$$0 < \frac{1}{q}+\frac{\beta}{p-\sigma-1} \le \frac{1}{q}+\frac{\beta}{\beta+1} \le \frac{1}{q}+1-\frac{1}{p} < 1.$$

It follows that if $p = \beta + 3 + 2\sigma = \beta + 2\beta^* + 1$, then (7) is redundant and if $p < \beta + 2\beta^* + 1$, then (6) is redundant. In the latter case we obtain that

$$\mathcal{I} = \Big(\frac{q}{p}\Big(1 - \frac{\beta}{p - \beta^* - 2}\Big), \frac{q}{p}\Big(1 - \frac{\beta}{p - \beta^*}\Big)\Big],$$

a clearly non-empty interval. In the former case we obtain

$$\mathcal{I} = \Big(\frac{q}{p}\Big(1 - \frac{\beta}{p - \beta^* - 2}\Big), \frac{q\beta^* - 1}{p(p - \beta^* - 1)}\Big)\Big],$$

in which case an easy calculation shows that it is a non-empty interval. Since $\beta + \beta^* \le 2\beta - 1 \le p - 4$ it follows that $p - \beta^* - 2 > \beta$ and thus if $\mathcal{I}$ is non-empty, it contains positive reals only. □

**Theorem 10** *Suppose that $\mathcal{B}_-(p)$ is non-empty and $\beta \in \mathcal{B}_-(p)$. Suppose also that $p < \beta + 2\beta^* + 1$. Let $q > p$ be a prime satisfying $q \equiv \beta (\mathrm{mod}\ p)$ and $q \ge q_-(p)$ with $q_-(p) = p(p - \beta^*)(p - \beta^* - 2)/(2\beta)$. Then the interval*

$$\mathcal{I} = \Big(\frac{q}{p}\Big(1 - \frac{\beta}{p - \beta^* - 2}\Big), \frac{q}{p}\Big(1 - \frac{\beta}{p - \beta^*}\Big)\Big]$$

*contains at least one integer $a$. Let $r > q$ be a prime with $r(q - pa) \equiv -1 (\mathrm{mod}\ pq)$, then*

$$a_{pqr}(p - 1 + [(p - \beta - 1)q - (p - \beta^* - 1)ap]r) = \beta - p < -\frac{(p+1)}{2}$$

*is a counter-example to Beiter's conjecture.*

*In case $p = \beta + 2\beta^* + 1$ the same conclusion holds, but with $q_-(p)$ replaced by $(\beta + \beta^* - 1)(p(\beta + \beta^*) + 1)/\beta$ and $\mathcal{I}$ by*

$$\mathcal{I} = \Big(\frac{q}{p}\Big(1 - \frac{\beta}{p - \beta^* - 2}\Big), \frac{q\beta^* - 1}{p(p - \beta^* - 1)}\Big].$$

*Proof.* Note that as a function of $q$ the length of $\mathcal{I}$ is increasing. If the length of $\mathcal{I}$ is at least one, then it contains at least one positive integer. Now $q_+(p)$ is obtained on solving the equation $|\mathcal{I}| = 1$ for $q$. The proof is completed on invoking Lemma 3 and Lemma 4. □

Small counter-examples produced by this result are given in Table 8.

## 3.2 The positive coefficient construction

Since the method of proof in this section is similar to that in the previous section, some of the details will be suppressed.

**Lemma 5** *Let $p$ be a prime. Let $1 \le \beta \le (p-3)/2$. Let $q > p$ be a prime satisfying $q \equiv \beta (\mathrm{mod}\ p)$ and $r > q$ be a prime satisfying $qr \equiv -1 (\mathrm{mod}\ p)$. Let $1 \le \alpha \le q - 1$ be the unique integer such that $pr\alpha \equiv 1 (\mathrm{mod}\ q)$. Put*

$$w_+ = 1 + (p - \beta - 1)q - (p - \beta)\alpha p,$$

*where* $\rho$ *and* $\sigma$ *are uniquely determined by* $(p-1)(q-1) = \rho p + \sigma q,\ \ \rho,\sigma \geq 0$. *Suppose that*

$$\beta + \sigma \geq p - 1$$

*and*

$$\alpha < \frac{(\sigma+1)q-1}{p(\beta-1)}, \tag{9}$$

$$\alpha \leq \frac{q(p-\sigma-1)}{p(p-\beta)}, \tag{10}$$

$$\alpha \leq \frac{q(\sigma+1-\beta)}{p(\sigma+1)}, \tag{11}$$

*and*

$$\alpha > \frac{q(p-2\beta-1)}{p(p-\beta-1)}, \tag{12}$$

*then* $a_{pqr}(p-1+rw_+) = p - \beta$.

`Remark`. The conditions (9), (10), (11) and (12) are used to ensure that respectively, $\rho+1+(\beta-1)\alpha \leq q-1$, $\rho+1-(p-\beta)\alpha \geq 0$, $f(q+p-\sigma-2) \leq f(p-1)$ and $f(q+\beta) > f(p-1)$.

*Proof of Lemma* 5. The proof is a more general variant of the proof of Theorem 9. Again we make use of tables in the proof.

**Table 6A:** `General positive coefficient construction:` $f(m)$ `case`

| $m$ | $f(m)$ | $c_m$ | $b_m$ |
|---|---|---|---|
| $0$ | $(\rho+1+(\beta-1)\alpha)p+(\sigma-\beta+1)q-\tau_0 pq$ | 0 | 0 |
| $\cdots$ | $\cdots$ | 0 | 0 |
| $\beta-2$ | $(\rho+1+\alpha)p+(\sigma-1)q-\tau_{\beta-2}pq$ | 0 | 0 |
| $\beta-1$ | $(\rho+1)p+\sigma q-\tau_{\beta-1}pq$ | 0 | 0 |
| $\beta$ | $(\rho+1-\alpha)p+(\sigma+1)q-\tau_\beta pq$ | 0 | 0 |
| $\cdots$ | $\cdots$ | 0 | 0 |
| $p-\sigma+\beta-2$ | $(\rho+1-(p-\sigma-1)\alpha)p+(p-1)q-\tau_{p-\sigma+\beta-2}pq$ | 0 | 0 |
| $p-\sigma+\beta-1$ | $(\rho+1-(p-\sigma)\alpha)p$ | 1 | 1 |
| $p-\sigma+\beta$ | $(\rho+1-(p-\sigma+1)\alpha)p+q$ | 1 | 1 |
| $\cdots$ | $\cdots$ | 1 | 1 |
| $p-1$ | $(\rho+1-(p-\beta)\alpha)p+(\sigma-\beta)q$ | 1 | 1 |

In Table 5A $\tau_j$ is the unique integer in $\{0,1\}$ such that the corresponding entry for $f(m)$ is in the interval $[0,pq)$.

**Table 6B:** `General positive coefficient construction:` $f(m+q)$ `case`

| $m+q$ | $f(m+q)$ | $c_{m+q}$ | $b_{m+q}$ |
|---|---|---|---|
| $q$ | $(\rho+1+(\beta-1)\alpha)p+(\sigma+1)q-pq$ | -1 | -1 |
| $\cdots$ | $\cdots$ | -1 | -1 |
| $q+p-\sigma-2$ | $(\rho+1+(\beta+\sigma+1-p)\alpha)p+(p-1)q-pq$ | -1 | -1 |
| $q+p-\sigma-1$ | $(\rho+1+(\beta+\sigma-p)\alpha)p$ | 0 | 0 |
| $\cdots$ | $\cdots$ | 0 | 0 |
| $q+\beta-1$ | $(\rho+1)p+(\beta+\sigma-p)q$ | 0 | 0 |
| $q+\beta$ | $(\rho+1-\alpha)p+(\beta+\sigma+1-p)q$ | 1 | 0 |
| $\cdots$ | $\cdots$ | 1 | 0 |
| $q+p-1$ | $(\rho+1-(p-\beta)\alpha)p+\sigma q$ | 1 | 0 |

Since $(\rho+1)p+(\sigma+1)q=qp+1$ we can rewrite $w_+$ as

$$w_+=(\rho+1-(p-\beta)\alpha)p+(\sigma-\beta)q.$$

The condition (10) ensures that $\rho+1-(p-\beta)\alpha\geq 0$. From $\beta\leq(p-3)/2$ and $\beta+\sigma\geq p-1$ we infer that $\sigma\geq\beta+2$. It follows that

$$0\leq w_+=(p-1)q+1-(p-\beta)\alpha p-\beta q<pq.$$

Thus $f(p-1)=w_+$. The condition (9) ensures that $\rho+1+(\beta-1)\alpha\leq q-1$. Let $0\leq r_1<pq$ be the unique integer with $r_1\equiv-\frac{1}{r}(\text{mod } pq)$. It is easy to see that $r_1=q-\alpha p$. We have $f(m)\equiv w_++(m-p+1)r_1(\text{mod } pq)$. Using these observations one arrives at Table 6A. For $m\leq p-\sigma+\beta-2$ we do not care about whether $\tau_m=0$ or $\tau_m=1$; in either case we find $b_m=0$ and hence $c_m=0$.

On noting that $f(m+q)\equiv f(m)+\beta q(\text{mod } pq)$ (cf. the proof of Theorem 9), we easily infer that the $f(m+q)$ are as given in Table 6B, with the caveat that the entries from $q+p-\sigma-1$ to $q+\beta-1$ do not arise if $\beta+\sigma=p-1$. Using that $f(q+p-\sigma-2)\leq f(p-1)$ and $f(q+\beta)>f(p-1)$ (a consequence of $\alpha$ satisfying (11), respectively (12))), we deduce that the $b_{m+q}$ and $c_{m+q}$ columns are as given in Table 6B. Finally on applying Lemma 1 we infer that

$$a_{pqr}(p-1+rw_+)=\sum_{j=p-\sigma+\beta-1}^{p-1}1+\sum_{j=q}^{q+p-\sigma-2}1=(\sigma-\beta+1)+(p-\sigma-1)=p-\beta.$$

This concludes the proof. □

**Lemma 6** *Let $\mathcal{I}$ be the set of real numbers satisfying* (9), (10), (11), (12) *and suppose the conditions of Lemma* 5 *are satisfied. Put*

$$\gamma=\min\Big\{\frac{p-\beta^*}{p-\beta},\frac{\beta^*-\beta}{\beta^*}\Big\}.$$

*The set $\mathcal{I}$ is non-empty iff $\beta^*\leq 2\beta$. In that case*

$$\mathcal{I}=\Big(\frac{q(p-1-2\beta)}{p(p-1-\beta)},\frac{q\gamma}{p}\Big].$$

*If $\mathcal{I}$ is non-empty then it consists of positive reals only.*

*Proof.* Left to the reader. □

`Remark`. Note that

$$\gamma = \begin{cases} \frac{p-\beta^*}{p-\beta} & \text{if } p < \beta + \frac{\beta^*}{\beta}(\beta^* - \beta); \\ \frac{\beta^*-\beta}{\beta^*} & \text{otherwise.} \end{cases}$$

On combining the latter two lemmas one obtains an explicit counter-example construction in the positive case.

**Theorem 11** *Suppose that $\mathcal{B}_+(p)$ is non-empty and $\beta \in \mathcal{B}_+(p)$. Let $q > p$ be a prime satisfying $q \equiv \beta (\mathrm{mod}\ p)$ and $q \geq q_+(p)$ with*

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

*Then the interval*

$$\mathcal{I} = \Big[\frac{q(p-1-2\beta)}{p(p-1-\beta)}, \frac{q\gamma}{p}\Big]$$

*contains at least one integer $a$. Let $r > q$ be a prime with $r(q - pa) \equiv -1 (\mathrm{mod}\ pq)$, then*

$$a_{pqr}(p - 1 + [(p-\beta-1)q - (p-\beta)ap]r) = p - \beta > \frac{(p+1)}{2}$$

*is a counter-example to Beiter's conjecture.*

*Proof.* Note that as a function of $q$ the length of $\mathcal{I}$ is increasing. If the length of $\mathcal{I}$ is at least one, then it contains at least one positive integer. Now $q_+(p)$ is obtained on solving the equation $|\mathcal{I}| = 1$ for $q$. The proof is completed on combining Lemma 5 and Lemma 6. □

Small counter-examples produced by this result are given in Table 7.

# 4 The proofs of Theorem 4 and Theorem 6

As is well-known the distribution of inverses modulo $p$ can be studied by connecting this problem to Kloosterman sums and estimates for those. For us, the following typical lemma, see e.g. Cobeli [6, Lemma 4, Chapter 3.2], will do.

Let $\mathcal{I} = \{a, a + r, \ldots, a + (M-1)r\} \subset [1, p]$ and put

$$N(\mathcal{I}_1, \mathcal{I}_2; p) = \#\{(x, y) : x \in \mathcal{I}_1,\ y \in \mathcal{I}_2,\ xy \equiv 1 (\mathrm{mod}\ p)\}.$$

**Lemma 7** *Let $p$ be a prime number. Suppose $|\mathcal{I}_1| \leq p$ and $|\mathcal{I}_2| \leq p$. Then*

$$\Big| N(\mathcal{I}_1, \mathcal{I}_2; p) - \frac{|\mathcal{I}_1| \cdot |\mathcal{I}_2|}{p} \Big| \leq \sqrt{p}\ (2 + \log p)^2.$$

The set of points $(x, y)$ with $xy \equiv d (\mathrm{mod}\ p)$ is called a *modular hyperbola*. For a survey of this area of study see e.g. Shparlinski [14].

*Proof of Theorem* 6. Bachman's upper bound $p - \lceil p/4 \rceil$ shows that $M(p) \le 3p/4$.

Suppose that for $p \ge 29$ and some $0 < \epsilon < 1/6$ we have

$$\frac{p}{3}(1+\epsilon) \le \beta \le \frac{p}{3}(1+2\epsilon),\ \frac{2p}{3}(1-\epsilon) \le \beta^* \le \frac{2p}{3}(1+\epsilon). \tag{13}$$

Then one checks that $\beta \in \mathcal{B}_+(p)$. It then follows by Theorem 4 that $M(p) \ge 2p(1-\epsilon)/3$. It only remains to show that for every $p$ sufficiently large there is a $\beta$ satisfying (13). This follows on invoking Lemma 7 with $\mathcal{I}_1$ the integers in the interval $[\frac{p}{3}(1+\epsilon), \frac{p}{3}(1+2\epsilon)]$ and $\mathcal{I}_2$ the integers in the range $[\frac{2p}{3}(1-\epsilon), \frac{2p}{3}(1+\epsilon)]$. This completes the proof. $\square$

**Proposition 3** *Let $\epsilon > 0$. There are infinitely many primes $p$ such that there exist primes $q$ and $r$ so that*

$$A(pqr) = \min(\frac{p-1}{2} + a, p-a) \ge (\frac{2}{3} - \epsilon)p,$$

*with $a$ as in Theorem 2.*

*Proof.* Suppose that

$$p \ge 29,\ 0 < \epsilon < \frac{1}{9},\ \beta \in \mathcal{B}_+(p),\ \beta < \frac{p}{3}(1+3\epsilon),\ \beta + \beta^* = p, \tag{14}$$

then by Theorem 4 we obtain $a_{pqr_+}(n_+) = p - \beta \ge (\frac{2}{3} - \epsilon)p$. In this case also Bachman's upper bound given in Theorem 2 gives $A(pqr_+) = \beta^* = p - \beta$. To see this note that $r^* = p - \beta$ and $q^* = \beta^*$. Since $\beta < \beta^*$ we infer that $a = p - \beta^*$. By Theorem 2 it then follows that $A(pqr_+) = \min(\frac{p-1}{2} + p - \beta^*, \beta^*) \le \beta^*$. Since $a_{pqr_+}(n_+) = \beta^*$, it follows that $A(pqr_+) = \beta^*$ and thus Bachman's upper bound is assumed.

Duke et al. [7] proved that if $f$ is a quadratic polynomial with complex roots, $0 \le a < b \le 1$, then $\#\{(p,\nu) : p \le x,\ f(\nu) \equiv 0 (\mathrm{mod}\ p),\ a \le \nu/p\} < b\} \sim (b-a)\pi(x)$, where $\pi(x)$ denotes the number of primes $p \le x$. In particular it follows that there are asymptotically $\epsilon\pi(x)/3$ primes $p$ for which there exist $x$ satisfying $x + x^* = p$ (that is $x^2 + 1 \equiv 0 (\mathrm{mod}\ p)$), and $p/3 < x < p(1+3\epsilon)/3$. On putting $x = \beta$ we then see that $\beta \in \mathcal{B}_+(p)$ and thus it follows that there exists infinitely many primes $p$ for which there is a $\beta$ satisfying (14). $\square$

The final result in this section shows that by elementary methods one can easily prove that $M(p) \ge (\frac{2}{3} - \epsilon)p$ for infinitely many primes $p$.

**Proposition 4** *Let $\epsilon > 0$, $e \ge 1$ be an integer, $N = 2^{2e+1}$ and $p$ a prime satisfying $p \equiv N - 9 (\mathrm{mod}\ 3N)$. If $p > \frac{N^2}{2} - 9$, then*

$$M(p) \ge \frac{(2N-1)p - 9}{3N} > \Big(\frac{2}{3} - \frac{N}{3(N^2-18)}\Big)p.$$

*If $p > \frac{N^2}{2} - 9$ and $N > \frac{1}{3\epsilon} + 3$, then $M(p) > (\frac{2}{3} - \epsilon)p$.*

*Proof.* Consider $\beta = ((N+1)p + 9)/(3N)$. Then $\beta^* = (2p+N)/3$. One checks that if $p > N^2/2 - 9$, then $\beta^*/2 < \beta$ and finally that $\beta \in \mathcal{B}_+(p)$. Then invoke Theorem 4. $\square$

`Examples`.
If $p \equiv 23 (\mathrm{mod}\ 24)$ and $p > 23$ then $M(p) \geq (5p-3)/8 > 0.608p$.
If $p \equiv 23 (\mathrm{mod}\ 96)$ and $p > 503$ then $M(p) \geq (21p-3)/32 > 0.656p$.
If $p \equiv 119 (\mathrm{mod}\ 384)$ and $p > 8183$ then $M(p) \geq (85p-3)/128 > 0.664p$.
If $p \equiv 503 (\mathrm{mod}\ 1536)$ and $p > 131063$ then $M(p) \geq (341p-3)/512 > 0.666p$.

*Proof of Theorem* 4. Follows on combining Theorem 10 and Theorem 11. Theorem 11 together with Theorem 2 yields that $A(pqr_+) = p - \beta$ if $\beta \in \mathcal{B}_+(p)$ and $\beta + \beta^* = p$ (cf. the proof of Proposition 3). $\square$

# 5 Reciprocal cyclotomic polynomials

We point out that for the so called reciprocal cyclotomic polynomials the analogue of Beiter's conjecture is known. Let

$$\frac{1}{\Phi_n(x)} = \sum_{k=0}^{\infty} c_n(k) x^k$$

be the Taylor series of $1/\Phi_n(x)$ around $x = 0$. The coefficients turn out to be periodic with period dividing $n$. Moree [13] established the following result concerning the height, $H(n)$, of $1/\Phi_n(x)$ (thus $\max_{k \geq 0} |c_n(k| = H(n))$.

**Theorem 12** *Let $p < q < r$ be odd primes. Then $H(pqr) = p - 1$ iff*

$$q \equiv r \equiv \pm 1 (\mathrm{mod}\ p) \text{ and } r < \frac{(p-1)}{(p-2)}(q-1).$$

*In the remaining cases $H(pqr) < p - 1$.*

This result in combination with Dirichlet's theorem on arithmetic progressions shows that for every odd prime $p$ there are infinitely many pairs $(q, r)$ such that $H(pqr) = p - 1$.

`Acknowledgement`. We thank C. Cobeli, M.Z. Garaev and I. Shparlinski for helpful information concerning the distribution of inverses modulo $p$.

**Table 7:** The set $\mathcal{B}_+(p)$, all $\beta$ and $\beta^*$ included, smallest $q$ for which $\alpha$ exists in the interval $\mathcal{I}$ of Theorem 11 and smallest $r$.

| $p$ | $\beta$ | $\beta^*$ | $q$ | $\alpha$ | $r$ | $n$ | $a_{pqr}(n)$ |
|---|---|---|---|---|---|---|---|
| 13 | 5 | 8 | 83 | 2 | 2423 | 906214 | 8 |
| 19 | 8 | 12 | 179 | 2 | 32611 | 44774921 | 11 |
| 23 | 9 | 18 | 331 | 5 | 161741 | 435730276 | 14 |
| 29 | 12 | 17 | 331 | 3 | 5783 | 22079522 | 17 |
| 31 | 14 | 20 | 107 | 1 | 5281 | 6263296 | 17 |
| 37 | 17 | 24 | 239 | 1 | 61507 | 233849650 | 20 |
| 41 | 17 | 29 | 263 | 2 | 35149 | 143478258 | 24 |
| 43 | 19 | 34 | 191 | 1 | 4051 | 13619504 | 24 |
| | 20 | 28 | 751 | 2 | 144323 | 2099178077 | 23 |
| 47 | 18 | 34 | 347 | 3 | 444539 | 2501865538 | 29 |
| | 20 | 40 | 1289 | 7 | 1015207 | 25006578870 | 27 |
| 53 | 22 | 41 | 181 | 1 | 5471 | 20724200 | 31 |
| | 23 | 30 | 977 | 4 | 208207 | 4575140670 | 30 |
| | 24 | 42 | 607 | 2 | 89899 | 1251663829 | 29 |
| 59 | 27 | 35 | 263 | 1 | 89527 | 560976240 | 32 |
| 61 | 27 | 52 | 271 | 1 | 141773 | 973980570 | 34 |
| | 29 | 40 | 761 | 1 | 45161 | 977284100 | 32 |
| 67 | 26 | 49 | 1031 | 6 | 188891 | 4676752335 | 41 |
| | 30 | 38 | 1303 | 4 | 4930693 | 182401126215 | 37 |
| | 32 | 44 | 367 | 1 | 279413 | 2831571408 | 35 |
| 71 | 27 | 50 | 311 | 2 | 119159 | 849127104 | 44 |
| | 29 | 49 | 739 | 4 | 376393 | 6915092266 | 42 |
| | 30 | 45 | 811 | 3 | 157433 | 3732421634 | 41 |
| | 31 | 55 | 457 | 2 | 146063 | 1773789142 | 40 |
| 73 | 27 | 46 | 3823 | 21 | 3233051 | 328212871490 | 46 |
| | 30 | 56 | 1709 | 7 | 3510587 | 174848296194 | 43 |
| | 34 | 58 | 691 | 1 | 711181 | 16650169644 | 39 |
| | 35 | 48 | 619 | 1 | 2069 | 41649042 | 38 |

**Table 8**: The set $\mathcal{B}_-(p)$, all $\beta$ and $\beta^*$ included, smallest $q$ for which $a$ exists in the interval $\mathcal{I}$ of Theorem 10 and smallest $r$.

| $p$ | $\beta$ | $\beta^*$ | $q$ | $a$ | $r$ | $n$ | $a_{pqr}(n)$ |
|---|---|---|---|---|---|---|---|
| 11 | 4 | 3 | 59 | 2 | 877 | 175410 | -7 |
| 17 | 7 | 5 | 41 | 1 | 29 | 5294 | -10 |
| 23 | 10 | 7 | 79 | 1 | 5743 | 3463051 | -13 |
| 29 | 13 | 9 | 419 | 5 | 39779 | 140419898 | -16 |
| 31 | 13 | 12 | 199 | 2 | 72497 | 164350729 | -18 |
| 41 | 18 | 16 | 797 | 5 | 79319 | 1000529906 | -23 |
| | 19 | 13 | 593 | 4 | 359311 | 2883470815 | -22 |
| 43 | 18 | 12 | 1093 | 10 | 924101 | 12320114574 | -25 |
| 47 | 22 | 15 | 163 | 1 | 136379 | 334810491 | -25 |
| 53 | 25 | 17 | 1297 | 7 | 994369 | 21909926598 | -28 |
| 59 | 23 | 18 | 967 | 7 | 697303 | 12080774533 | -36 |
| | 26 | 25 | 557 | 2 | 900551 | 12544675488 | -33 |
| | 28 | 19 | 1031 | 5 | 28183 | 547454833 | -31 |
| 61 | 25 | 22 | 1123 | 6 | 1021301 | 25937981557 | -36 |
| | 28 | 24 | 577 | 2 | 200971 | 2828063972 | -33 |
| 71 | 32 | 20 | 1381 | 7 | 4008001 | 110733051698 | -39 |
| | 33 | 28 | 317 | 1 | 5581 | 48817077 | -38 |
| | 34 | 23 | 1951 | 8 | 296473 | 12908434490 | -37 |
| 73 | 33 | 31 | 1201 | 3 | 1668019 | 63151199412 | -40 |

# References


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

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

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

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

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

[6] C. Cobeli, Topics on the Distribution of Inverses, Ph.D. thesis, University of Rochester, 1997.

[7] 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.

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

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

[10] D.H. Lehmer, Some properties of cyclotomic polynomials, *J. Math. Anal. Appl.* **15** (1966), 105–117.

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

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

[13] P. Moree, Reciprocal cyclotomic polynomials, arXiv:0709.1570, submitted.

[14] I.E. Shparlinski, Distribution of points on modular hyperbolas, *Sailing on the Sea of Number Theory*: Proc. 4th China-Japan Seminar on Number Theory, Weihai, 2006, World Scientific, 2007, 155–189.

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

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`