ACTA ARITHMETICA
144.1 (2010)

Bounds on ternary cyclotomic coefficients

by

Bartłomiej Bzdęga (Poznań)

1. Introduction. Let

$$\Phi_{pqr}(x) = \prod_{(k,pqr)=1,\, 0<k<pqr} (x - \zeta_{pqr}^k) = \sum_n a_{pqr}(n) x^n$$

be a ternary cyclotomic polynomial with $p < q, r$ prime, $q \neq r$ and $\zeta_{pqr} = e^{2\pi i/pqr}$. The coefficients of Φ_{pqr} have been the subject of study for over a century. The main problem is to estimate the following parameters:

$$A_+ = \max_n a_{pqr}(n), \quad A_- = \min_n a_{pqr}(n), \quad A = \max\{A_+, -A_-\}. \tag{1.1}$$

The first bound on A was given by Bang [2] who showed that $A \le p-1$. This bound was later improved by Beiter [3]. She proved that $A \le p - \lfloor p/4 \rfloor$. Beiter also came up with the following conjecture:

Conjecture 1.1. $A \le (p+1)/2$.

This is now known to be false. Gallot and Moree [5] found infinitely many pairs of primes q, r for every $\varepsilon > 0$ and p sufficiently large, such that $A > (2/3 - \varepsilon)p$. Also they updated Beiter's Conjecture into the following form:

Conjecture 1.2. $A \le \frac{2}{3}p$.

This is still an open problem.

In this paper we derive a new bound on the size of ternary cyclotomic coefficients, which depends on the inverses of q and r modulo p (denoted here by q' and r', respectively). The main results of this paper are given in the three theorems below, with Theorem 1.4 being an easy consequence of Theorem 1.3.

Theorem 1.3. *Let A_+ and A_- be defined as in* (1.1). *Then*

$$A_+ \le \min\{2\alpha + \beta, p - \beta\}, \quad -A_- \le \min\{p + 2\alpha - \beta, \beta\},$$

where $\alpha = \min\{q', r', p - q', p - r'\}$ and $\alpha\beta qr \equiv 1 \pmod p$, $0 < \beta < p$.

2010 *Mathematics Subject Classification*: Primary 11B83.
Key words and phrases: ternary cyclotomic polynomial, coefficient bounds.

DOI: 10.4064/aa144-1-2

Theorem 1.4. *Put* $\beta^* = \min\{\beta, p-\beta\}$. *Then*

$$A \le \min\{2\alpha + \beta^*, p - \beta^*\}. \tag{1.2}$$

Theorem 1.4 improves the following bound obtained by Bachman [1]:

$$A \le \min\{(p-1)/2 + \alpha, p - \beta^*\}. \tag{1.3}$$

One can deduce, by *reductio ad absurdum*, that the bound (1.2) is at least as strong as (1.3). It is also easy to check that the bound (1.2) is strictly stronger than (1.3) if and only if $\alpha + \beta^* < (p-1)/2$. This happens for exactly $\frac{1}{2}(p-3)(p-5)$ of all the $(p-1)^2$ pairs (x, y) of residue classes q and r modulo p.

As an application, we prove a density result showing that Conjecture 1.2 holds for at least $25/27 + O(1/p)$ of all the ternary cyclotomic polynomials with the smallest prime factor dividing their order equal to p. We also prove that the average A of these polynomials does not exceed $(p+1)/2$ (Bachman's Theorem gives $8/9 + O(1/p)$, respectively $(7p-1)/12 + O(1/p)$, for these values; methods of computing them are similar to those used in our proofs of Corollaries 4.2 and 4.3).

We also exhibit, for every prime $p > 12$, some new classes of ternary cyclotomic polynomials Φ_{pqr} for which the set of coefficients is very small. For example $A \le 3$ if $q \equiv \pm 1 \pmod p$ and $r \equiv \pm 1 \pmod p$.

Our method also leads to a simpler, independent proof of the so called *jump one property* of the ternary cyclotomic coefficients due to Gallot and Moree [6]:

Theorem 1.5. *If* $\Phi_{pqr}(x) = \sum_{n\in\mathbb{Z}} a_{pqr}(n)x^n$ *is a ternary cyclotomic polynomial, then*

$$|a_{pqr}(n) - a_{pqr}(n-1)| \le 1 \quad \textit{for every } n \in \mathbb{Z}.$$

2. The numbers F_k. We define some special numbers, which are the key tools in the proofs of Theorems 1.3 and 1.5. Throughout the paper we assume that $k \in \mathbb{Z}$, fix p, q, r and denote by a_k, b_k, c_k the unique integers such that $0 \le a_k < p$, $0 \le b_k < q$, $0 \le c_k < r$ and

$$k \equiv a_k qr + b_k rp + c_k pq \pmod{pqr}.$$

Let

$$F_k = \frac{a_k}{p} + \frac{b_k}{q} + \frac{c_k}{r} - \frac{k}{pqr}.$$

Observe that $F_k \in \{0, 1, 2\}$ for $-(qr + rp + pq) < k < pqr$, since

$$0 \le a_k qr + b_k rp + c_k pq - k < (p-1)qr + (q-1)rp + (r-1)pq + qr + rp + pq = 3pqr.$$

In this section we establish some properties of the sequence F_k.

LEMMA 2.1. *If $F_k = 0$ then $a_k \le \lfloor k/qr \rfloor$. If $F_k = 2$ then*

$$a_k \ge \left\lceil \frac{k + pq + rp}{qr} \right\rceil.$$

Proof. The first implication is obvious. For the second one we note that

$$k + 2pqr = a_k qr + b_k rp + c_k pq \le a_k qr + (q-1)rp + (r-1)pq,$$

thus $a_k qr \ge k + rp + pq$, completing the proof. ■

LEMMA 2.2. *Let p'_q, p'_r be the inverses of p modulo q and r respectively. Then*

$$F_k - F_{k-q} = \begin{cases} -1 & \text{if } a_k < r' \text{ and } c_k < p'_r, \\ 1 & \text{if } a_k \ge r' \text{ and } c_k \ge p'_r, \\ 0 & \text{otherwise.} \end{cases}$$

The analogous statement holds for $F_k - F_{k-r}$ with c_k, r', p'_r replaced by b_k, q', p'_q respectively.

Proof. Observe that $a_{k-q} \equiv a_k - r' \pmod p$, $c_{k-q} \equiv c_k - p'_r \pmod r$ and $b_{k-q} = b_k$. Therefore

$$a_k - a_{k-q} = \begin{cases} r' - p & \text{if } a_k < r', \\ r' & \text{if } a_k \ge r', \end{cases} \qquad c_k - c_{k-q} = \begin{cases} p'_r - r & \text{if } c_k < p'_r, \\ p'_r & \text{if } c_k \ge p'_r. \end{cases}$$

Let $[P] \in \{0, 1\}$ be the logical value of a statement P. Then

$$\begin{aligned} F_k - F_{k-q} &= \frac{a_k - a_{k-q}}{p} + \frac{b_k - b_{k-q}}{q} + \frac{c_k - c_{k-r}}{r} - \frac{1}{pr} \\ &= \frac{r'}{p} + \frac{p'_r}{r} - \frac{1}{pr} - [a_k < r'] - [c_k < p'_r] \\ &= 1 - [a_k < r'] - [c_k < p'_r], \end{aligned}$$

and the lemma holds. ■

LEMMA 2.3. *Let $M = \max\{q', r'\}$ and $m = \min\{q', r'\}$. Then*

$$F_k - F_{k-q} - F_{k-r} + F_{k-q-r} = \begin{cases} 0 & \text{if } a_k < M + m - p, \\ -1 & \text{if } M + m - p \le a_k < m, \\ 0 & \text{if } m \le a_k < M, \\ 1 & \text{if } M \le a_k < M + m, \\ 0 & \text{if } M + m \le a_k. \end{cases}$$

This equality also holds for any permutation of (p, q, r) with similarly defined M and m.

Proof. Using Lemma 2.2 we obtain

$$F_k - F_{k-q} = 1 - [a_k < r'] - [c_k < p'_r],$$

$$F_{k-r} - F_{k-q-r} = 1 - [a_{k-r} < r'] - [c_{k-r} < p'_r].$$

Since $a_{k-r} \equiv a_k - q' \pmod{p}$ and $c_{k-r} = c_k$, we have

$$\begin{aligned}F_k - F_{k-q} - F_{k-r} + F_{k-q-r} \\ &= [a_{k-r} < r'] - [a_k < r'] \\ &= [a_k < q' + r' - p] - [a_k < q'] + [a_k < q' + r'] - [a_k < r'] \\ &= [a_k < M + m - p] - [a_k < m] - [a_k < M] + [a_k < M + m].\end{aligned}$$

Now it is easy to verify the lemma, since $M+m-p<m \le M < M+m$. ∎

LEMMA 2.4. *We have*

$$F_k + F_{k-p-q} + F_{k-q-r} + F_{k-r-p} = F_{k-p} + F_{k-q} + F_{k-r} + F_{k-p-q-r}.$$

Proof. By Lemma 2.3, the value of $F_k - F_{k-q} - F_{k-r} + F_{k-q-r}$ depends only on k modulo p. Thus

$$F_k - F_{k-q} - F_{k-r} + F_{k-q-r} = F_{k-p} - F_{k-p-q} - F_{k-r-p} + F_{k-p-q-r}. \ \blacksquare$$

3. Proof of Theorem 1.3. Bloom [4] gave a relation between the ternary cyclotomic coefficients and the numbers k such that $k = a_k qr + b_k rp + c_k pq$ with a_k, b_k and c_k defined in the previous section. This equality holds if and only if $F_k = 0$, so we can express his result in terms of F_k.

LEMMA 3.1. *Denote by $N_d(t_1, \ldots, t_l)$ the number of d's in the given sequence. Then*

$$\begin{aligned}a_{pqr}(n) &= \sum_{k=n-p+1}^{n} (N_0(F_k, F_{k-q-r}) - N_0(F_{k-q}, F_{k-r})) \\ &= \sum_{k=n-p+1}^{n} (N_2(F_k, F_{k-q-r}) - N_2(F_{k-q}, F_{k-r})) \\ &= \frac{1}{2} \sum_{k=n-p+1}^{n} (N_1(F_{k-q}, F_{k-r}) - N_1(F_k, F_{k-q-r})).\end{aligned}$$

Proof. The first equality is due to Bloom [4]. Here we rewrite his proof which uses formal series:

$$\begin{aligned}\Phi_{pqr}(x) &= \frac{(1-x^{pqr})(1-x^p)(1-x^q)(1-x^r)}{(1-x)(1-x^{qr})(1-x^{rp})(1-x^{pq})} \\ &\equiv (1-x^q)(1-x^r)(1+x+\cdots+x^{p-1}) \sum_{a,b,c\ge 0} x^{aqr+brp+cpq} \pmod{x^{pqr}}.\end{aligned}$$

Note that if $k \le \deg(\Phi_{pqr}) < pqr$ then there exists at most one triple (a, b, c) such that $k = aqr + brp + cpq$. This equality holds if and only if $F_k = 0$ with

$a = a_k$, $b = b_k$, $c = c_k$. Then

$$\begin{aligned} a_{pqr}(n) &= \sum_{k=n-p+1}^{n} ([F_k = 0] - [F_{k-q} = 0] - [F_{k-r} = 0] + [F_{k-q-r} = 0]) \\ &= \sum_{k=n-p+1}^{n} (N_0(F_k, F_{k-q-r}) - N_0(F_{k-q}, F_{k-r})). \end{aligned}$$

For simplicity we will use the following notations:

$$\begin{aligned} N_0^+ &= N_0(F_n, F_{n-1}, \dots, F_{n-p+1}, F_{n-q-r}, F_{n-q-r-1}, \dots, F_{n-q-r-p+1}), \\ N_0^- &= N_0(F_{n-q}, F_{n-q-1}, \dots, F_{n-q-p+1}, F_{n-r}, F_{n-r-1}, \dots, F_{n-r-p+1}), \end{aligned}$$

and similarly $N_1^+, N_1^-, N_2^+, N_2^-$. We have just proved that $a_{pqr}(n) = N_0^+ - N_0^-$. Now by Lemma 2.3 we have

$$\begin{aligned} N_1^+ + 2N_2^+ - N_1^- - 2N_2^- &= \sum_{k=n-p+1}^{n} (F_k - F_{k-q} - F_{k-r} + F_{k-q-r}) \\ &= \min\{M+m, p\} - M + m - \max\{M+m-p, 0\} = 0, \end{aligned}$$

where we have used the fact that there is a bijection between the sets $\{n, n-1, \dots, n-p+1\}$ and $\{a_n, a_{n-1}, \dots, a_{n-p+1}\}$, because $a_k qr \equiv k \pmod{p}$. Moreover

$$N_0^+ + N_1^+ + N_2^+ = N_0^- + N_1^- + N_2^- = 2p.$$

By simple arithmetical operations, these equalities lead to

$$a_{pqr}(n) = N_0^+ - N_0^- = N_2^+ - N_2^- = \frac{1}{2}(N_1^- - N_1^+). \ \blacksquare$$

Using the first equality of Lemma 3.1, we consider the 4-tuples $Q_k = (F_k, F_{k-q}, F_{k-r}, F_{k-q-r})$, where $k \in \{n, n-1, \dots, n-p+1\}$, such that $N_0(F_k, F_{k-q-r}) \neq N_0(F_{k-q}, F_{k-r})$. Lemmas 2.2 and 2.3 will help us to exclude the existence of most of the 81 possible such 4-tuples.

If $N_0(Q_k) \in \{0, 4\}$ then $N_0(F_k, F_{k-q-r}) = N_0(F_{k-q}, F_{k-r})$, so we are not going to consider these cases. Also if $N_0(Q_k) = 2$, then $N_0(F_k, F_{k-q-r}) = N_0(F_{k-q}, F_{k-r})$ or $|F_k - F_{k-q} - F_{k-r} + F_{k-q-r}| \geq 2$, contradicting Lemma 2.3, therefore this case does not need to be considered either.

To describe the other possibilities we note the following facts:

- if $N_0(Q_k) = 3$ then by Lemma 2.2 the only non-zero entry here is equal to 1,
- if $N_0(Q_k) = 1$ then $F_l = 0$ for some $l \in \{k, k-q, k-r, k-q-r\}$. By Lemma 2.2 we have $F_{l\pm q} = 1$ and $F_{l\pm r} = 1$, where the sign depends on l.

All these cases are described in the table below.

Case	Q_k	$F_k - F_{k-q}$ $-F_{k-r} + F_{k-q-r}$	$N_0(F_n, F_{n-q-r})$ $-N_0(F_{n-q}, F_{n-r})$
1	$(0,0,1,0), (0,1,0,0),$ $(0,1,1,1), (1,1,1,0)$	-1	1
2	$(0,0,0,1), (1,0,0,0),$ $(1,0,1,1), (1,1,0,1)$	1	-1
3	$(0,1,1,2), (2,1,1,0)$	0	1
4	$(1,0,2,1), (1,2,0,1)$	0	-1

Denote by C_l the number of integers $k \in \{n, n-1, \ldots, n-p+1\}$ for which the lth case occurs. Then we have

$$A_+ \le C_1 + C_3, \quad -A_- \le C_2 + C_4.$$

In order to prove Theorem 1.3 it is enough to show that

$$C_1, C_2 \le \alpha, \tag{3.1}$$

$$C_3 \le \min\{\alpha + \beta, p - \alpha - \beta\}, \tag{3.2}$$

$$C_4 \le \min\{\beta - \alpha, p + \alpha - \beta\}. \tag{3.3}$$

In fact, we will count values of a_k instead of k.

Note that $\alpha = \min\{m, p - M\}$, where M and m are defined in Lemma 2.3.

Case 1. By Lemma 2.3 we have $M + m - p \le a_k < m$, so

$$C_1 \le m - \max\{0, M + m - p\} = \min\{m, p - M\} = \alpha.$$

Case 2. By Lemma 2.3 we have $M \le a_k < M + m$, so

$$C_2 \le \min\{M + m, p\} - M = \min\{m, p - M\} = \alpha.$$

Note that

$$\text{if} \quad M + m \ge p \quad \text{then} \quad \alpha = p - M \text{ and } \beta = p - m$$

and

$$\text{if} \quad M + m \le p \quad \text{then} \quad \alpha = m \text{ and } \beta = M.$$

We also put $\gamma = \lfloor n/qr \rfloor + 1$ and recall that $k \in \{n, n-1, \ldots, n-p+1\}$.

In order to simplify the notation, we divide the third case into Cases 3a and 3b and define $C_{3\mathrm{a}}$ and $C_{3\mathrm{b}}$ as above for the 4-tuples $(0,1,1,2)$ and $(2,1,1,0)$ respectively. Obviously, $C_3 = C_{3\mathrm{a}} + C_{3\mathrm{b}}$.

Case 3a. By Lemma 2.2 we have $a_k < m, M$, thus by Lemma 2.3 $a_k < M + m - p$. By Lemma 2.1, $a_k < \gamma$ and $a_k - M - m + 2p = a_{k-q-r} \ge \gamma$. Finally

$$\max\{\gamma + M + m - 2p, 0\} \le a_k < \min\{\gamma, M + m - p\},$$

and we obtain

$$\begin{aligned} C_{3\mathrm{a}} &\le \min\{\gamma, M+m-p\} - \max\{\gamma+M+m-2p, 0\} \\ &= \min\{\gamma, p-\gamma, M+m-p, 2p-M-m\} \\ &\le \min\{M+m-p, 2p-M-m\} = \min\{\alpha+\beta, p-\alpha-\beta\} \end{aligned}$$

as long as $M+m \ge p$. Otherwise $C_{3\mathrm{a}} = 0$.

CASE 3b. By Lemma 2.2, $a_k \ge M \ge m$, so by Lemma 2.3, $a_k \ge M+m$. By Lemma 2.1, $a_k - M - m = a_{k-q-r} < \gamma$ and $a_k \ge \gamma$. Finally

$$\max\{\gamma, M+m\} \le a_k < \min\{p, \gamma+M+m\}.$$

Therefore

$$\begin{aligned} C_{3\mathrm{b}} &\le \min\{p, \gamma+M+m\} - \max\{\gamma, M+m\} \\ &= \min\{\gamma, p-\gamma, M+m, p-M-m\} \\ &\le \min\{M+m, p-M-m\} = \min\{\alpha+\beta, p-\alpha-\beta\} \end{aligned}$$

as long as $M+m \le p$. Otherwise $C_{3\mathrm{b}} = 0$.

CASE 3. We claim that $C_3 \le \min\{\alpha+\beta, p-\alpha-\beta\}$. If $M+m = p$, then $C_3 = 0$, $\alpha+\beta = p$ and so the estimate holds. In case $M+m \ne p$ Cases 3a and 3b exclude each other and then the estimate also holds.

CASE 4. Assume that $q' = m$ and $r' = M$. By Lemma 2.2, we have $M \le a_k < m$ (for $F_{k-q} = 0$) or $m \le a_k < M$ (when $F_{k-r} = 0$). The first inequality is impossible, so $F_{k-q} = 2$ and $F_{k-r} = 0$. By Lemma 2.1, $a_k - m = a_{k-r} < \gamma$ and $a_k - M + p = a_{k-q} \ge \gamma$. Finally

$$\max\{M+\gamma-p, m\} \le a_k < \min\{m+\gamma, M\},$$

and

$$\begin{aligned} C_4 &\le \min\{m+\gamma, M\} - \max\{M+\gamma-p, m\} \\ &= \min\{\gamma, p-\gamma, p-M+m, M-m\} \\ &\le \min\{p-M+m, M-m\} = \min\{\beta-\alpha, p+\alpha-\beta\}. \end{aligned}$$

This completes the verification of (3.1)–(3.3) and the proof of Theorem 1.3. ∎

4. The bound on A. In this section we derive a bound on $A = \max\{A_+, -A_-\}$. We also establish some infinite families of triples (p, q, r) with restrictions on q and r modulo p only, for which A is bounded by a constant independent of p, q, r.

We also apply our bound on A to estimate the density of the set of ternary cyclotomic polynomials such that $A \le cp$, for any real $c > 0$ and fixed p. In view of Conjecture 1.2, the most interesting case is $c = 2/3$.

At the end we prove a weaker version of the old Beiter's Conjecture.

Proof of Theorem 1.4. By Theorem 1.3, we have

$$A \le \max\{\min\{2\alpha+\beta, p-\beta\}, \min\{p+2\alpha-\beta, \beta\}\}.$$

If $\beta < \frac{1}{2}p$ then

$$\begin{aligned} A &\le \max\{\min\{2\alpha+\beta, p-\beta\}, \beta\} = \min\{2\alpha+\beta, p-\beta\} \\ &= \min\{2\alpha+\beta^*, p-\beta^*\}. \end{aligned}$$

Also if $\beta > \frac{1}{2}p$ then

$$\begin{aligned} A &\le \max\{p-\beta, \min\{p+2\alpha-\beta, \beta\}\} = \min\{2\alpha+p-\beta, \beta\} \\ &= \min\{2\alpha+\beta^*, p-\beta^*\}. \ \blacksquare \end{aligned}$$

COROLLARY 4.1. *Let $p > 12$ and $p = 2d_2 \pm 1 = 3d_3 \pm 1 = 4d_4 \pm 1 = 6d_6 \pm 1$ for some integers d_2, d_3, d_4, d_6. Let also $d_1 = 1$. If q is congruent to $\pm d_i$ and r is congruent to $\pm d_j$ modulo p, then*

$$A \le \min\{2i+j, i+2j\} \le 18.$$

Proof. Just observe that $\alpha = \min\{i,j\}$, $\beta^* = \max\{i,j\}$ and apply Theorem 1.4. $\blacksquare$

Denote by

$$D_p(c) = \limsup_{n\to\infty} \frac{\#\{(q,r) : p < q < r < n,\ A_{pqr} \le cp\}}{\#\{(q,r) : p < q < r < n\}}$$

the density of the ternary cyclotomic polynomials with the smallest prime factor of their order equal to p, for which $A \le cp$.

COROLLARY 4.2.

$$D_p(c) \begin{cases} \ge \frac{4}{3}c^2 + O(1/p) & \text{if } 0 < c \le 1/2, \\ \ge 1 - \frac{2}{3}(3-4c)^2 + O(1/p) & \text{if } 1/2 < c < 3/4, \\ = 1 & \text{if } c \ge 3/4. \end{cases}$$

Proof. Note that α and β^* depend only on the residue classes of q and r modulo p. Let $a(i,j) = \min\{2\alpha+\beta^*, p-\beta^*\}$, where α and β^* are computed for the polynomial Φ_{pqr} with $q' \equiv i \pmod p$ and $r' \equiv j \pmod p$. Using Theorem 1.4 and Dirichlet's Prime Number Theorem we obtain

$$\begin{aligned} D_p(c) &\ge \lim_{n\to\infty} \frac{\sum_{a(i,j)\le cp} \#\{(q,r) : p < q < r < n,\ (q,r) \equiv (i,j) \pmod p\}}{\#\{(q,r) : p < q < r < n\}} \\ &= \lim_{n\to\infty} \frac{\frac{n^2}{2(p-1)^2 \log^2 n} \sum_{a(i,j)\le cp} 1}{\frac{n^2}{2\log^2 n}} = \frac{1}{(p-1)^2} \sum_{a(i,j)\le cp} 1, \end{aligned}$$

where the sum runs over all the non-zero residue classes i and j modulo p.

It is not difficult to see that

$$\sum_{a(i,j)\le cp} 1 = 8 \sum_{1\le\alpha\le\beta^*\le(p-1)/2} \quad \sum_{\min\{2\alpha+\beta^*,p-\beta^*\}\le cp} 1 + O(p).$$

In case $c \le 1/2$ we have

$$\begin{aligned} D_p(c) &\ge \frac{8}{(p-1)^2} \sum_{\alpha=1}^{\lfloor cp/3\rfloor} \sum_{\beta^*=\alpha}^{\lfloor cp\rfloor-2\alpha} 1 + O(1/p) \\ &= \frac{8(p^2c^2/6 + O(p))}{(p-1)^2} + O(1/p) = \frac{4}{3}c^2 + O(1/p). \end{aligned}$$

Assume that $1/2 < c < 3/4$. Then

$$\begin{aligned} D_p(c) &\ge \frac{8}{(p-1)^2}\Big(\sum_{\beta^*=1}^{(p-1)/2} \sum_{\alpha=1}^{\beta^*} 1 - \sum_{\beta^*=\lfloor cp/3\rfloor+1}^{\lceil(1-c)p\rceil-1} \quad \sum_{\alpha=\lfloor(cp-\beta^*)/2\rfloor+1}^{\beta^*} 1\Big) + O(1/p) \\ &= 8(p^2/8 - p^2(9-24c+16c^2)/12 + O(p))/(p-1)^2 + O(1/p) \\ &= 1 - \frac{2}{3}(3-4c)^2 + O(1/p). \end{aligned}$$

The third equality in the corollary is obvious. ∎

Our bound on the value $D(c) = \lim_{p\to\infty} D_p(c)$ may be interpreted as a quotient of two areas. The denominator is the area of the triangle described by the inequalities $0 < x < y < 1/2$. The numerator is the area defined by the inequalities

$$0 < x < y < 1/2, \quad 2x + y < c, \quad 1 - y < c.$$

We can apply our estimation of $D_p(c)$ to check that Conjecture 1.2 is true in at least $25/27 + O(1/p)$ cases and the old Beiter's Conjecture 1.1 holds for at least $1/3 + O(1/p)$ cases.

Although Conjecture 1.1 does not hold in general, we are able to prove a weaker version of it, with the same bound. Let $\bar{A}(p)$ denotes the average value of A for all the ternary cyclotomic polynomials with the smallest prime dividing their order equal to p. More precisely,

$$\bar{A}(p) = \limsup_{n\to\infty} \frac{\sum_{p<q<r<n} A_{pqr}}{\#\{(q,r) : p < q < r < n\}}.$$

Corollary 4.3. $\bar{A}(p) \le (p+1)/2$.

Proof. Applying the method of Corollary 4.2 we obtain

$$\bar{A}(p) \le \frac{1}{(p-1)^2} \sum_{i=1}^{p-1}\sum_{j=1}^{p-1} a(i,j) = \frac{4}{(p-1)^2} \sum_{i=1}^{(p-1)/2} \sum_{j=1}^{(p-1)/2} a(i,j).$$

Let $k \le (p-1)/2$ be a positive integer. Then

$$\sum_{i=1}^{k} a\left(i, i+\frac{p-1}{2}-k\right) = \sum_{i=1}^{k} \min\left\{3i-k+\frac{p-1}{2}, k-i+\frac{p+1}{2}\right\}$$
$$= \frac{(p+1)k}{2} + \sum_{i=1}^{k} \min\{3i-k-1, k-i\} = \frac{(p+1)k}{2}.$$

Now we have

$$\sum_{i=1}^{(p-1)/2} \sum_{j=1}^{(p-1)/2} a(i,j)$$
$$= \sum_{k=1}^{(p-1)/2} \sum_{i=1}^{k} \left(a\left(i, i+\frac{p-1}{2}-k\right) + a\left(i+\frac{p-1}{2}-k, i\right)\right) - \sum_{i=1}^{(p-1)/2} a(i,i)$$
$$= 2\sum_{k=1}^{(p-1)/2} \sum_{i=1}^{k} a\left(i, i+\frac{p-1}{2}-k\right) - \sum_{i=1}^{(p-1)/2} a(i,i)$$
$$= \frac{p+1}{2}\left(2\sum_{k=1}^{(p-1)/2} k - \frac{p-1}{2}\right) = \frac{(p+1)(p-1)^2}{8}.$$

Finally we get $\bar{A}(p) \le (p+1)/2$. ∎

5. Proof of Theorem 1.5. First we present a simple expression for the difference of two consecutive coefficients of a ternary cyclotomic polynomial in terms of F_k:

Lemma 5.1. *Put*

$$N_+ = N_1(F_n, F_{n-p-q}, F_{n-q-r}, F_{n-r-p}),$$

$$N_- = N_1(F_{n-p}, F_{n-q}, F_{n-r}, F_{n-p-q-r}).$$

Then

$$a_{pqr}(n) - a_{pqr}(n-1) = \frac{1}{2}(N_- - N_+).$$

Moreover

$$a_{pqr}(n) - a_{pqr}(n-1)$$
$$= N_0(F_n, F_{n-p-q}, F_{n-q-r}, F_{n-r-p}) - N_0(F_{n-p}, F_{n-q}, F_{n-r}, F_{n-p-q-r})$$
$$= N_2(F_n, F_{n-p-q}, F_{n-q-r}, F_{n-r-p}) - N_2(F_{n-p}, F_{n-q}, F_{n-r}, F_{n-p-q-r}).$$

Proof. By Lemma 3.1,

$$\begin{aligned}
&a_{pqr}(n) - a_{pqr}(n-1)\\
&= \frac{1}{2}\sum_{k=n-p+1}^{n} (N_1(F_{k-q}, F_{k-r}) - N_1(F_k, F_{k-q-r}))\\
&\quad - \frac{1}{2}\sum_{k=n-p}^{n-1} (N_1(F_{k-q}, F_{k-r}) - N_1(F_k, F_{k-q-r}))\\
&= \frac{1}{2}(N_1(F_{n-p}, F_{n-q}, F_{n-r}, F_{n-p-q-r}) - N_1(F_n, F_{n-p-q}, F_{n-q-r}, F_{n-r-p}))\\
&= \frac{1}{2}(N_- - N_+).
\end{aligned}$$

The remaining two equalities can be established in the same way. ∎

Now we are ready to prove Theorem 1.5. By Lemma 5.1 we have

$$|a_{pqr}(n) - a_{pqr}(n-1)| = \frac{1}{2}|N_- - N_+| \le 2,$$

where equality may hold only if $N_- = 4, N_+ = 0$ or $N_+ = 4, N_- = 0$. We will show that either is impossible.

Indeed, for some permutation (t, u, v) of (p, q, r) by Lemma 5.1 we have $F_{n-t} = F_{n-u} \in \{0, 2\}$ in the case of $(F_n, F_{n-p-q}, F_{n-q-r}, F_{n-r-p}) = (1, 1, 1, 1)$. Therefore $|F_n - F_{n-t} - F_{n-u} + F_{n-t-u}| = 2$.

Also if $(F_{n-p}, F_{n-q}, F_{n-r}, F_{n-p-q-r}) = (1, 1, 1, 1)$ then for some permutation (t, u, v) we have $F_{n-t-u} = F_{n-u-v} \in \{0, 2\}$ and $|F_{n-u} - F_{n-t-u} - F_{n-u-v} + F_{n-t-u-v}| = 2$. Both cases contradict Lemma 2.3. ∎

Acknowledgments. This research was done when the author was a student at the Faculty of Mathematics and Computer Science of the Adam Mickiewicz University in Poznań. The author would like to thank Wojciech Gajda for suggesting the problem and his help in improving the paper. He would also like to thank Pieter Moree for helpful comments, and the referee for help in simplifying the proof of Corollary 4.2.

References

[1] G. Bachman, *On the coefficients of ternary cyclotomic polynomials*, J. Number Theory 100 (2003), 104–116.
[2] A. S. Bang, *Om ligningen $\Phi_n(x) = 0$*, Tidsskr. Math. 6 (1895), 6–12.
[3] M. Beiter, *Magnitude of the coefficients of the cyclotomic polynomial Φ_{pqr}, II*, Duke Math. J. 38 (1971), 591–594.
[4] D. M. Bloom, *On the coefficients of the cyclotomic polynomials*, Amer. Math. Monthly 75 (1968), 370–372.

[5] Y. Gallot and P. Moree, *Ternary cyclotomic polynomials having a large coefficient*, J. Reine Angew. Math. 632 (2009), 105–125.
[6] —, —, *Neighboring ternary cyclotomic coefficients differ by at most one*, J. Ramanujan Math. Soc. 24 (2009), 235–248.

Bartłomiej Bzdęga
Stróżyńskiego 15A/20
60-688 Poznań, Poland
E-mail: exul@wp.pl

Received on 3.1.2009
and in revised form on 12.10.2009 (5904)