SISTER BEITER AND KLOOSTERMAN: A TALE OF CYCLOTOMIC COEFFICIENTS AND MODULAR INVERSES

CRISTIAN COBELI, YVES GALLOT, PIETER MOREE AND ALEXANDRU ZAHARESCU

ABSTRACT. For a fixed prime p, the maximum coefficient (in absolute value) $M(p)$ of the cyclotomic polynomial $\Phi_{pqr}(x)$, where r and q are free primes satisfying $r > q > p$ exists. Sister Beiter conjectured in 1968 that $M(p) \leq (p+1)/2$. In 2009 Gallot and Moree showed that $M(p) \geq 2p(1-\epsilon)/3$ for every p sufficiently large. In this article Kloosterman sums ('cloister man sums') and other tools from the distribution of modular inverses are applied to quantify the abundancy of counter-examples to Sister Beiter's conjecture and sharpen the above lower bound for $M(p)$.

1. INTRODUCTION

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

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

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 $A(n) = \max\{|a_n(k)| : k \geq 0\}$, 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 behavior of the coefficients of $\Phi_n(x)$ is the ternary case, where $n = pqr$, with $2 < p < q < r$ odd primes. It is for this reason that in this paper we will be mainly interested in the behavior of coefficients of ternary cyclotomic polynomials.

If n is a prime, then we have $\Phi_n(x) = 1 + x + \cdots + x^{n-1}$. Already if $n = pq$ consists of two prime factors and is odd, modular inverses come into the picture. In this binary case the coefficients are computed in the following lemma. For a proof see e.g. Lam and Leung [18] or Thangadurai [24].

Lemma 1. *Let $p < q$ be odd primes. Let ρ and σ be the (unique) non-negative integers for which $1 + pq = \rho p + \sigma q$. 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 $\alpha_1 p \equiv m \pmod q$ and $0 \leq \beta_1 \leq p-1$ the*

2000 *Mathematics Subject Classification.* Primary 11T22, Secondary 11L05 .

Key Words and Phrases: Cyclotomic coefficients, Sister Beiter conjecture, Modular inverses, Kloosterman sums.

unique integer such that $\beta_1 q \equiv m (\mathrm{mod}\ p)$. *The cyclotomic coefficient* $a_{pq}(m)$ *equals*

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

Note that ρ is merely the modular inverse of p modulo q and σ is the modular inverse of q modulo p. In the ternary case Kaplan's lemma [17] can be used to express a ternary cyclotomic coefficient into a sum of binary ones. It is thus not surprising that also in the ternary case modular inverses make their appearance. We will give some examples of this.

Let $\overline{q}$ and $\overline{r}$, $0 < \overline{q}, \overline{r} < p$ be the inverses of q and r modulo p respectively. Set $a = \min(\overline{q}, \overline{r}, p - \overline{q}, p - \overline{r})$. Put $b = \max(\min(\overline{q}, p - \overline{q}), \min(\overline{r}, p - \overline{r}))$. Note that $b \ge a$. Bzdęga [8] showed that

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

It is easy to show from this estimate that $A(pqr) < 3p/4$ (see, e.g., Section 3 of Gallot et al. [14]). Notice that this bound does not depend on the two largest prime factors of n. Indeed, for an arbitrary n it was shown by Justin [16] and independently by Felsch and Schmidt [12] that there is an upper bound for $A(n)$ that does not depend on the largest and second largest prime factor of n. Thus for a fixed prime p the maximum

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

where q, r range over all the primes satisfying $p < q < r$, exists. The major open problem involving ternary cyclotomic coefficients, is to find a finite procedure to determine $M(p)$.

H. Möller [21] gave a construction showing that $M(p) \ge (p + 1)/2$ for $p > 5$. On the other hand, in 1968 Sister Marion Beiter [1] had conjectured (a conjecture she repeated in 1971 [2]) that $M(p) \le (p + 1)/2$ and shown that $M(3) = 2$ [3], which on combining leads to the conjecture that $M(p) = (p + 1)/2$ for $p > 2$. The bound of Möller together with $M(5) \le 3$ (established independently by Beiter [2] and Bloom [4]) shows that $M(5) = 3$. Zhao and Zhang [27] showed that $M(7) = 4$. Thus Beiter's conjecture holds true for $p \le 7$. However, work of Gallot and Moree [13] has made clear that the true behavior of $M(p)$ is much more complicated than suggested by Beiter's conjecture. Theorem 1, the main result of [13], produces counter-examples to Sister Beiter's conjecture. The goal of this paper is to investigate the abundance of these counter-examples using techniques from the study of the distribution of modular inverses (for a survey, see, e.g., Shparlinski [23]). These techniques involve Kloosterman sums $K(a, b; p)$. Recall that for a prime p the Kloosterman sum $K(a, b; p)$ is defined as

$$K(a, b; p) = \sum_{1 \le x \le p-1} e^{2\pi i (ax + b\overline{x})/p},$$

where $\overline{x}$ denotes an inverse of x modulo p. By a fundamental result of Weil [25] we have that

$$|K(a, b; p)| \le 2\sqrt{p}. \tag{2}$$

Theorem 1. *Let* p *be a prime. Given an* $1 \le \beta \le p - 1$, *we let* $\overline{\beta}$ *be the unique integer* $1 \le \overline{\beta} \le p - 1$ *with* $\beta\overline{\beta} \equiv 1 (\mathrm{mod}\ p)$.

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

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

For every prime $q \equiv \beta \pmod p$ 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 β satisfying

$$1 \le \beta \le \frac{p-3}{2},\ \beta + \overline{\beta} \ge p,\ \overline{\beta} \le 2\beta, \tag{4}$$

For every prime $q \equiv \beta \pmod p$ 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 $\beta + \overline{\beta} = p$, then $A(pqr_+) = p - \beta$.

Corollary 1. *Put $\mathcal{B}(p) = \mathcal{B}_-(p) \cup \mathcal{B}_+(p)$. If $\mathcal{B}(p)$ is non-empty, then*

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

an so Beiter's conjecture is false for the prime p.

The explicit values of $q_-(p), r_-, n_-, q_+(p), r_+$ and n_+ will be of no concern to us here. For these the reader is referred to Theorems 10 and 11 in [13].

We like to remark that the sets $\mathcal{B}_\pm(p)$ are not merely 'figments of the proof of Theorem 1'. Similar (but not equal) sets were independently found by E. Roşu in her construction of 'Non-Beiter ternary cyclotomic polynomials with an optimally large set of coefficients', see [22].

To fully exploit the power of Theorem 1, one needs information on the sets $\mathcal{B}_-(p), \mathcal{B}_+(p)$ and $\mathcal{B}(p)$. By an elementary method in [13] the following information on $\mathcal{B}(p)$ was deduced, which in combination with Theorem 1 shows that Beiter's conjecture is false for every $p \ge 11$.

Lemma 2. *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 $p \equiv 1 \pmod 3$, then $\overline{\beta} = 2(p-1)/3$ and one checks that $\beta \in \mathcal{B}_+(p)$. If $p \equiv 2 \pmod 3$, then $\overline{\beta} = (p-2)/3$ and one checks that $\beta \in \mathcal{B}_-(p)$. □

Showing the non-emptiness of $\mathcal{B}(p)$ for $p \ge 11$ is thus almost trivial. Estimating its cardinality is rather more challenging and this is were the Kloosterman sums come in.

Theorem 2. *For any prime number p,*

$$\begin{aligned} \left| \#\mathcal{B}_-(p) - \frac{p}{48} \right| &\le 12\, p^{3/4} \log p\,, \\ \left| \#\mathcal{B}_+(p) - \frac{p}{24} \right| &\le 12\, p^{3/4} \log p\,, \\ \left| \#\mathcal{B}(p) - \frac{p}{16} \right| &\le 24\, p^{3/4} \log p\,. \end{aligned} \tag{5}$$

It was shown [13, Proposition 4], working with explicit inverses modulo p, that if $e \ge 1$ and p are such (with $N = 2^{2e+1}$) that if

$$\epsilon > 0,\ N > \frac{1}{3\epsilon} + 3,\ p > \frac{N^2}{2} - 9 \text{ and } p \equiv N - 9 \pmod{3N},$$

then $\min\{\mathcal{B}_+(p)\} < \frac{p}{3}(1+\epsilon)$ and hence $M(p) > (\frac{2}{3}-\epsilon)p$. An easy application of Lemma 3 below (see the proof of Theorem 6 of [13]) yields the stronger result that

$$\frac{2}{3}p(1-\epsilon) \leq M(p), \tag{6}$$

for *every* prime p large enough.

If there are p with $M(p) > 2p/3$, then Theorem 1 does not allow to find them, since $\min\{\mathcal{B}(p)\} \geq p/3$. On this basis and extensive numerical experiments by Gallot, the following Corrected Beiter Conjecture (Conjecture 3 from [13]) can be made:

$$M(p) \leq \frac{2p}{3}. \tag{7}$$

If true, this conjecture would place $M(p)$ in a rather short interval of size ϵp.

A natural question that arises would be to see how much one can shorten this interval by improving on the lower bound in (6). We will establish the following result.

Theorem 3.
1) *We have*

$$M(p) > \frac{2p}{3} - 3\,p^{3/4}\log p. \tag{8}$$

2) *For an infinite class of prime numbers p we have*

$$M(p) > \frac{2p}{3} - c_1\sqrt{p}, \tag{9}$$

with c_1 a positive constant.

Given fixed primes $2 < p < q$, put

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

where r ranges over all the primes $> q$. There is a finite procedure to determine $M(p;q)$. We say that a function is ultimately constant on an infinite sequences of integers, if it takes on the same value for all sufficiently large elements in the sequence. The study of $M(p;q)$ was initiated by Gallot et al. [14]. The main conjecture is that given a prime p, there exists a modulus d_p, such that $M(p;q)$ is ultimately constant on every primitive residue class modulo d_p. This would imply that

$$\delta_p = \lim_{x\to\infty} \frac{\#\{p < q \leq x : M(p;q) > (p+1)/2\}}{\pi(x)},$$

exists and is rational (by the prime number theorem for arithmetic progressions). Here as usual $\pi(x)$ denotes the number of primes $p \leq x$, Put

$$\underline{\delta}_p = \liminf_{x\to\infty} \frac{\#\{p < q \leq x : M(p;q) > (p+1)/2\}}{\pi(x)}.$$

By Theorem 1, Lemma 2 and the prime number theorem for arithmetic progressions $\underline{\delta}_p$ is positive for $p \geq 11$. We will establish the following result, which in conjunction with Lemma 2 implies that there is a positive constant c_2 such that $\underline{\delta}_p \geq c_2$ for every prime $p \geq 11$.

Theorem 4. *We have*

$$\underline{\delta}_p \geq \frac{\#\mathcal{B}(p)}{p-1} \text{ and } \liminf_{p\to\infty} \underline{\delta}_p \geq \frac{1}{16}.$$

Proof. The first inequality is a consequence of the prime number theorem for arithmetic progressions and Theorem 1. The second inequality follows from the first one and Theorem 2. □

We conjecture that δ_p exists. It is known that $\delta_3 = \delta_5 = \delta_7 = 0$ and $\underline{\delta}_{11} \geq \frac{2}{5}$. We conjecture that $\delta_{11} = \frac{2}{5}$, $\delta_{13} = \frac{1}{3}$, $\delta_{17} = \frac{3}{8}$, $\delta_{19} = \frac{4}{9}$, $\delta_{23} = \frac{5}{11}$ (cf. [14]).

2. Kloosterman sums and their application to cyclotomic coefficients

Let p be a prime and, for any $\Omega \subset \mathbb{R}^2$, let

$$\mathcal{I}(\Omega) := \#\big\{(x,y) \in \Omega \cap \mathbb{N}\times\mathbb{N} :\ xy \equiv 1 (\mathrm{mod}\ p)\big\}.$$

A familiar argument using the Weil bound (2) provides us with a sharp estimate for $\mathcal{I}(\Omega)$ when Ω is a rectangle:

Lemma 3. *For any $0 \leq a < b < p$ and $0 \leq c < d < p$, let $\mathcal{R} := [a,b)\times[c,d)$ or $\mathcal{R} := (a,b]\times(c,d]$. Then we have:*

$$\left|\mathcal{I}\big(\mathcal{R}\big) - \frac{\mathrm{Area}(\mathcal{R})}{p}\right| < \sqrt{p}\,\big(\log p + 1.1\big)^2.$$

Proof. We adapt the calculations from [9, Section 3.2, Lemma 4].

Writing the characteristic function of the points counted by $\mathcal{I}(\mathcal{R})$ in terms of exponential sums, we have:

$$\mathcal{I}(\mathcal{R}) = \frac{1}{p}\sum_{\substack{x\in(a,b]\\ p\nmid x}}\sum_{y\in(c,d]}\sum_{k=1}^{p} e\Big(k\frac{y-\overline{x}}{p}\Big). \tag{10}$$

The main contribution is given by the terms with $k = p$. This is equal to

$$\frac{\big((b-a)+\delta_1\big)\times\big((d-c)+\delta_1\big)}{p} = \frac{\mathrm{Area}(\mathcal{R})}{p} + \eta, \tag{11}$$

where $|\delta_1| \leq 1$, $|\delta_2| \leq 1$, which implies $|\eta| \leq 3$ for any prime $p \geq 2$. Changing the order of summation of the remaining terms, we have

$$\frac{1}{p}\sum_{\substack{x\in(a,b]\\ p\nmid x}}\sum_{y\in(c,d]}\sum_{k=1}^{p-1} e\Big(k\frac{y-\overline{x}}{p}\Big) = \frac{1}{p}\sum_{k=1}^{p-1}\sum_{y\in(c,d]} e\Big(\frac{ky}{p}\Big)\sum_{\substack{x\in(a,b]\\ p\nmid x}} e\Big(\frac{-k\overline{x}}{p}\Big). \tag{12}$$

The most inner sum on the right-hand side of (12) is an incomplete Kloosterman sum. Using a standard completion together with the upper bound (2), yields

$$\left|\sum_{\substack{x\in(a,b]\\ p\nmid x}} e\Big(\frac{-k\overline{x}}{p}\Big)\right| \leq (2+\log p)\sqrt{p}. \tag{13}$$

On combining this with (10), (11), and (12), we obtain:

$$\begin{aligned}\left|\mathcal{I}\big(\mathcal{R}\big)-\frac{\mathrm{Area}(\mathcal{R})}{p}\right| \leq & \frac{1}{p}\sum_{k=1}^{p-1}\frac{2}{\left|e\big(\frac{k}{p}\big)-1\right|}\times(2+\log p)\sqrt{p}+3\\ \leq & \frac{2+\log p}{\sqrt{p}}\sum_{k=1}^{p-1}\frac{1}{\sin\frac{k\pi}{p}}+3\\ \leq & \frac{2+\log p}{\sqrt{p}}\sum_{k=1}^{\frac{p-1}{2}}\frac{p}{k}+3\leq(1.1+\log p)^2\sqrt{p}.\end{aligned}$$

This completes the proof of the lemma. □

For a region Ω contained in $[0,1]\times[0,1]$ with piecewise smooth boundary one can show that

$$\Big|\mathcal{I}\big(p\,\Omega\big)-p\,\mathrm{Area}(\Omega)\Big|<c(\Omega)\;p^{3/4}\log p,$$

for some constant $c(\Omega)$, which depends only on the region Ω. For a derivation of this result from Lemma 3, the reader is referred to the papers of Laczkovich [19] and Weyl [26]. In our context the regions of interest are triangles, and in such case we can directly derive via a dyadic approximation an estimate as accurate as the one above. Moreover, we show that $c(\text{triangle})<12$.

Lemma 4. *Let p be a prime number and let $\triangle ABC\subset[0,p-1]\times[0,p-1]$ be a right triangle with two sides parallel to the axes of coordinates. Then*

$$\left|\mathcal{I}\big(\triangle ABC\big)-\frac{\mathrm{Area}(\triangle ABC)}{p}\right|<3\;p^{3/4}\log p. \tag{14}$$

Proof. To get the lower bound, we cover dyadicly $\triangle ABC$ with rectangles D_j^k, as in Figure 1(a). There are n diagonal rows, the j-th row containing 2^{j-1} equal rectangles. Thus we have

$$\mathcal{I}\big(\triangle ABC\big)\geq\sum_{\substack{1\leq j\leq n\\ 1\leq k\leq 2^{j-1}}}\mathcal{I}\big(D_j^k\big).$$

Then we apply Lemma 3 for each rectangle D_j^k:

$$\mathcal{I}\big(\triangle ABC\big)\geq\sum_{\substack{1\leq j\leq n\\ 1\leq k\leq 2^{j-1}}}\frac{\mathrm{Area}(D_j^k)}{p}-\big(1+2+\cdots+2^{n-1}\big)\times\sqrt{p}\,(\log p+1.1)^2. \tag{15}$$

We denote by T the area of $\triangle ABC$ and notice that $\mathrm{Area}\left(D_1^1\right)=T/2$, while the size of the rectangles in row j is 4 times smaller than the size of rectangles in row $j-1$. Then, by

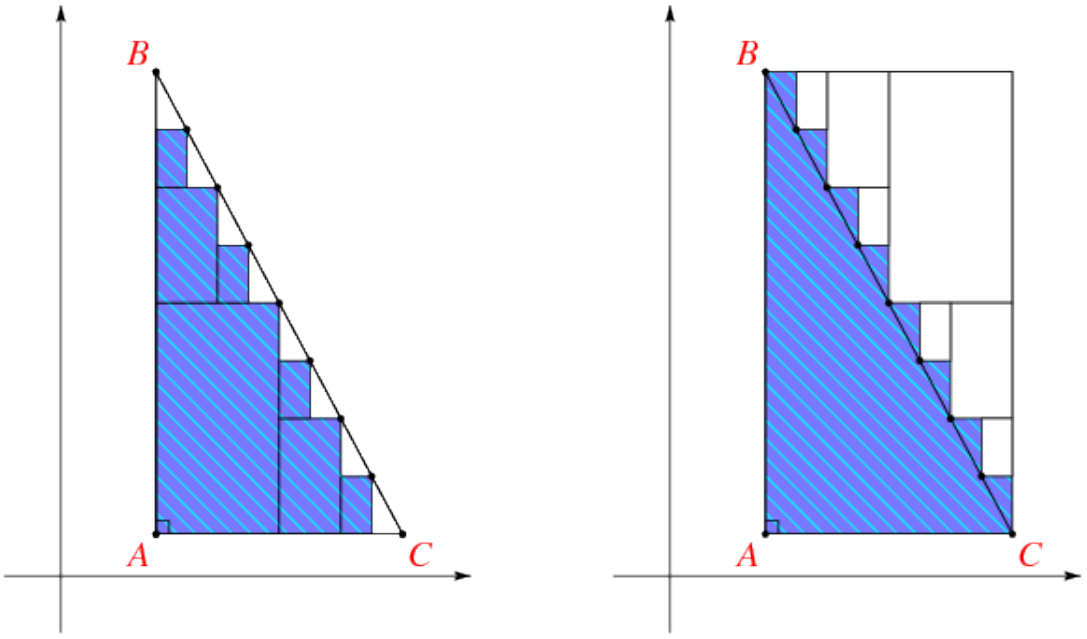
relation (15) it follows:

$$\begin{aligned}\mathcal{I}\big(\triangle ABC\big) &\geq \sum_{1\leq j\leq n} \frac{T}{2p}\cdot\frac{1}{4^{j-1}}\cdot 2^{j-1} - \big(2^n-1\big)\times\sqrt{p}\,(\log p+1.1)^2\\ &> \sum_{1\leq j\leq n} \frac{T}{p\,2^j} - \big(2^n-1\big)\times\sqrt{p}\,(\log p+1.1)^2\\ &= \frac{T}{p} - \frac{T}{p\,2^n} - \big(2^n-1\big)\times\sqrt{p}\,(\log p+1.1)^2\\ &> \frac{T}{p} - \frac{p}{2^{n+1}} - \big(2^n-1\big)\times\sqrt{p}\,(\log p+1.1)^2\,,\end{aligned} \tag{16}$$

since $T\leq p^2/2$. We balance the last two terms taking $n=\left\lfloor \frac{1}{4}\log_2 p - \log_2\left(\sqrt{2}(\log p+1.1)\right)\right\rfloor$. Thus, by (16) it follows that there exists $c>0$ and $p_0\geq 2$, such that

$$\mathcal{I}\big(\triangle ABC\big) > \frac{T}{p} - c\,p^{3/4}\log p\,,\quad \text{for } p\geq p_0. \tag{17}$$

For the upper bound, we proceed similarly, covering completely $\triangle ABC$ with an additional row along the diagonal, the $(n+1)$-th one, containing 2^n rectangles. Each of these new rectangles are equal to those in n-th row. Another way to get the upper bound is to work with the complement covering, which is the difference between the smallest rectangle that includes $\triangle ABC$ and a series of rectangles like those used to deduce the lower bound (17) (see Figure 1(b)).



(a) The inner covering. (b) The outer covering, by difference.

FIGURE 1. The dyadic approximations of a right triangle using three rows of rectangles.

We remark that a constant c for which the left hand side of (14) is less than $c\,p^{3/4}\log p$ must be larger than $2\sqrt{2}$, but for sufficiently large p, it can be chosen as close to $2\sqrt{2} = 2.828427125...$ as one wishes. Numerical computations for smaller p show that if $c = 2.8320056$ the estimations hold for all prime numbers p. This completes the proof of the lemma. □

Since any $\triangle ABC \subset [0,p-1)^2$ can be obtained by starting with a rectangle whose edges are parallel with the axes of coordinates from which at most 3 right triangles with two sides parallel with the axes of coordinates are cut off, applying Lemma 3 and Lemma 4, we obtain:

Lemma 5. *Let p be a prime number and let $\triangle ABC \subset [0,p-1]\times[0,p-1]$. Then*

$$\left|\mathcal{I}\big(\triangle ABC\big) - \frac{\mathrm{Area}(\triangle ABC)}{p}\right| < 12\,p^{3/4}\log p. \tag{18}$$

We now apply Lemma 5 to some special triangles. Let

$$\mathcal{B}_-^{\times}(p) := \left\{(x,y)\in[1,p-1]^2\cap\mathbb{N}^2\colon \begin{array}{l} 1\le x\le (p-3)/2,\ p\le x+2y+1,\ x>y,\\ xy\equiv 1(\mathrm{mod}\ p)\end{array}\right\} \tag{19}$$

and

$$\mathcal{B}_+^{\times}(p) := \left\{(x,y)\in[1,p-1]^2\cap\mathbb{N}^2\colon \begin{array}{l} 1\le x\le (p-3)/2,\ p\le x+y,\ y\le 2x,\\ xy\equiv 1(\mathrm{mod}\ p)\end{array}\right\}. \tag{20}$$

For the 52-nd prime, $p = 239$, in Figure 2(a) we have pictured the sets

$$B_+(239) = \big\{(90,162),(99,169),(102,157),(103,181),(105,173),(107,172),\\ (108,135),(109,182),(110,176),(112,207),(117,143)\big\}$$

and

$$B_-(239) = \big\{(94,89),(95,78),(100,98),(101,71),(114,65),(115,106),(116,68),(118,79)\big\}.$$

The sets defined by (19) and (20) are two disjoint triangles[1], and we denote their union by $\mathcal{B}^{\times}(p) := \mathcal{B}_-^{\times}(p)\cup\mathcal{B}_+^{\times}(p)$. Then $\mathcal{B}(p)$, $\mathcal{B}_-(p)$, $\mathcal{B}_+(p)$ are the projection onto Ox of $\mathcal{B}^{\times}(p)$, $\mathcal{B}_-^{\times}(p)$, and $\mathcal{B}_+^{\times}(p)$, respectively. Notice that by projection no point is lost, as they have distinct x-coordinates. (This follows since each nonzero residue class modulo p has exactly one inverse modulo p.)

Despite some irregularities for small primes, it turns out that the number of elements in $\mathcal{B}_-(p)$ and $\mathcal{B}_+(p)$ are approximately equal to the area of $\mathcal{B}^{\times}(p)$ and $\mathcal{B}_-^{\times}(p)$, respectively, and this follows immediately by Lemma 5.

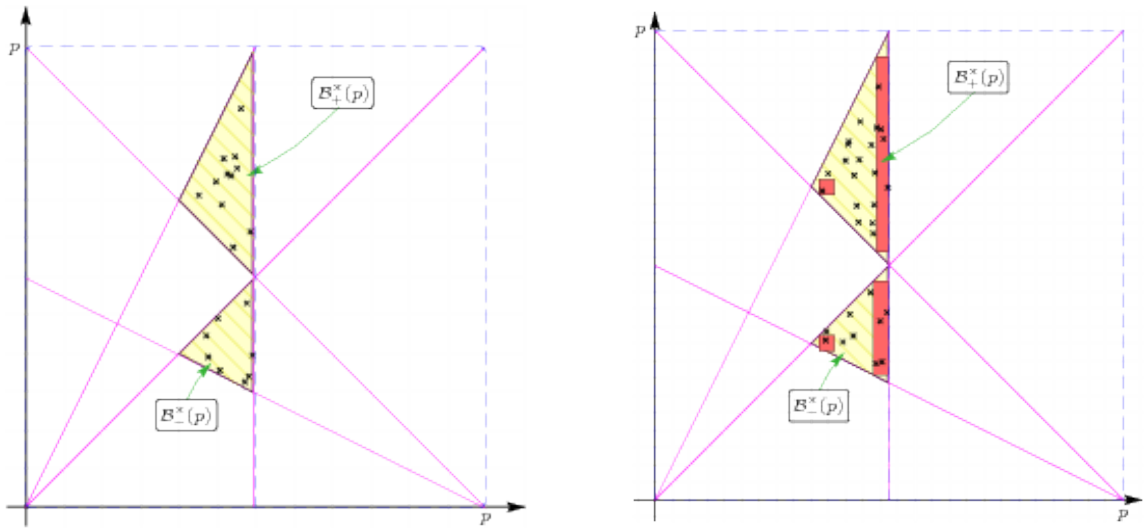
Let us see how far one has to go from the left or from the right side of $\mathcal{B}(p)$ to find points in $\mathcal{B}_-(p)$ or $\mathcal{B}_+(p)$. We denote

$$m_-(p) := \min_{x\in\mathcal{B}_-(p)} x\,,\quad m_+(p) := \min_{x\in\mathcal{B}_+(p)} x\,,\ m_\pm(p) := \min_{x\in\mathcal{B}_-(p)\cup\mathcal{B}_+(p)} x\,, \tag{21}$$

and

$$M_-(p) := \max_{x\in\mathcal{B}_-(p)} x\,,\quad M_+(p) := \max_{x\in\mathcal{B}_+(p)} x\,.\ \text{and}\ \ M_\pm(p) := \max_{x\in\mathcal{B}_-(p)\cup\mathcal{B}_+(p)} x\,. \tag{22}$$

[1] When it is clear from the context, we use the same notations $\mathcal{B}_+^{\times}(p)$ and $\mathcal{B}_+^{\times}(p)$ not only for the lattice points, but for the triangles defined by the inequalities on the right-hand side of (19) and (20), respectively.



(a) $\mathcal{B}_+^\times(239)$ and $\mathcal{B}_-^\times(239)$ with 11 and 8 points, respectively.

(b) $\mathcal{B}_+^\times(541)$ and $\mathcal{B}_-^\times(541)$ and some catching rectangles for their extreme elements.

FIGURE 2. The triangles $\mathcal{B}_+^\times(p)$ and $\mathcal{B}_-^\times(p)$.

In case any of the sets involved is empty we set the corresponding quantity to be $p/2$ if a 'max' is involved, and $p/3$ is a 'min' is involved. Thus if $\mathcal{B}_-(p)$ is empty, then $m_-(p) = p/3$, for example.

The known methods to study the distribution of inverses ultimately reduce to showing the existence of small boxes $\mathcal{R} = \mathcal{I} \times \mathcal{J} \subset [1, p]^2$ that capture points $(x, \overline{x})$. In our case the problems are not the same at both ends. This is due to the vertical edges that exist only on the right-hand side of $\mathcal{B}_-^\times(p)$ and $\mathcal{B}_+^\times(p)$ (see Figure 2). What we are looking for is a slim box $\mathcal{R} = \mathcal{I} \times \mathcal{J} \subset \mathcal{B}(p)$ that contains elements of $\mathcal{B}_-^\times(p)$ or $\mathcal{B}_+^\times(p)$, has the edge $\mathcal{I}$ as small as possible (which by Lemma 3 means that the length of the other edge $\mathcal{J}$ is forced to be as large as possible), and is situated as close as possible to the left or to the right of $\mathcal{B}(p)$, respectively.

Lemma 3 shows that the points counted by $\mathcal{I}(\mathcal{R})$ are rather uniformly spread out into $[0, p]^2$, therefore it suffices to allow us to find the smallest rectangles $\mathcal{R} \subset [0, p]^2$ for which we know for sure that $\mathcal{I}(\mathcal{R})$ is positive. The condition is:

$$0 \le \frac{\text{Area}(\mathcal{R})}{p} - \sqrt{p}(\log p + 1.1)^2 < \mathcal{I}\big(\mathcal{R}\big)\,,$$

which becomes

$$p^{3/2}(\log p + 1.1)^2 \le \text{Area}(\mathcal{R})\,. \tag{23}$$

Condition (23) and inclusion in $\mathcal{B}_-(p)$, $\mathcal{B}_+(p)$ or $\mathcal{B}(p)$ are the only two requirements that our capturing boxes must fulfill. These imply sharper estimates for $M_-(p)$, $M_+(p)$ and $M_\pm(p)$ than for the corresponding ones on the left-hand side. The reason is that near $x = p/2$ the edges of the triangles from Figure 2 are long, so we can afford to take $\mathcal{J}$ with $|\mathcal{J}| = O(p)$. On the other hand, for the bound of $m_-(p)$, $m_+(p)$ and $m_\pm(p)$ we can not due better than fit approximately square boxes (rectangles with edges of the same order of magnitude), because of the slopes of the edges of the triangles $\mathcal{B}_-(p)$, $\mathcal{B}_+(p)$ that meet at $x = p/3$ (see Figure 2(b)).

The following theorem gives the estimates that follow for the quantities defined in (21) and (22). Numerically we found that, for $p < 10^8$, $m_-(p) \le p/3 + 6\sqrt{p}$, $m_+(p) \le p/3 + 4\sqrt{p}$ and that for $p < 10^{10}$, $p/2 - 4\log p \le M_-(p)$, $p/2 - 2\log p \le M_+(p)$.

Theorem 5. *For $p \ge 2$ we have:*

$$\frac{p}{3} \le m_-(p) \le \frac{p}{3} + 4.25\, p^{3/4}\log p \tag{24}$$

$$\frac{p}{3} \le m_+(p) \le \frac{p}{3} + 3\, p^{3/4}\log p \tag{25}$$

$$\frac{p}{3} \le m_\pm(p) \le \frac{p}{3} + 3\, p^{3/4}\log p \tag{26}$$

and

$$\frac{p}{2} - 3\, p^{1/2}\log^2 p \le M_+(p) \le \frac{p}{2} \tag{27}$$

$$\frac{p}{2} - 6\, p^{1/2}\log^2 p \le M_-(p) \le \frac{p}{2} \tag{28}$$

Moreover, for $p \ge 11$:

$$\text{if } p \equiv 1 (\text{mod } 3),\ \text{then } M_+(p) = (p-3)/2\,,$$
$$\text{if } p \equiv 2 (\text{mod } 3),\ \text{then } M_-(p) = (p-3)/2\,,$$

and

$$M_\pm(p) = \max\big\{M_-(p),\, M_+(p)\big\} = (p-3)/2\,.$$

Proof. When dealing with any of the six quantities, we may assume that the associated $\mathcal{B}$ set is non-empty, for if it is empty the inequality to be proved trivially holds true.

First we find the upper bound of $m_+(p)$. Let $\mathcal{R} \subset \mathcal{B}_+(p)$ be the capturing box from the left side of in Figure 2(b). We denote its height by H, and assume it to be the largest possible. Also, let L be the length of the horizontal edge of $\mathcal{R}$, and let l be the distance from the left edge of $\mathcal{R}$ to $x = p/3$. By the similarity of triangles, it follows that $H/(p/2) = l/(p/6)$, that is, $l = H/3$. Denoting $\alpha := H/L$, this can be written as

$$l = \frac{\alpha}{3} L\,. \tag{29}$$

Putting $b(p) := p^{3/2}(\log p + 1.1)^2$, the inequality (23) becomes

$$b(p) \le \alpha L^2\,. \tag{30}$$

Let us remark that if $\mathcal{R}$ is a box that contains points from $\mathcal{B}_+^\times(p)$, then $m_+(p) \le p/3 + l + L$. Then, because we need the best available bound, using (29) and (30), we get:

$$m_+(p) - \frac{p}{3} \le \min_{b(p)\le \alpha L^2} (l + L) \le \min_{\frac{b(p)}{L} \le \alpha L} \left(\frac{\alpha L}{3} + L\right) = \min_L \left(\frac{b(p)}{3L} + L\right),$$

where we have made the choice $\alpha = b(p)L^{-2}$, that is $HL = b(p)$. We balance the terms here, taking $L = \sqrt{b(p)/3}$. These yield

$$m_+(p) - \frac{p}{3} \le \frac{2\sqrt{b(p)}}{\sqrt{3}} \le c_+ p^{3/4}\log p\,,$$

for some positive constant c_+. For sufficiently large p, we can take c_+ close to $2/\sqrt{3}$, while $c_+ = 3$ covers the inequality for all $p \geq 2$.

The bound for $m_-(p)$ is obtained in a similar way. In this case $H/(p/4) = l/(p/6)$, and equality (29) has to be replaced by $l = 2\alpha L/3$. Then, the same reasoning (with $b(p)$ replaced by $2b(p)$) gives

$$m_-(p) - \frac{p}{3} \leq \frac{2\sqrt{2b(p)}}{\sqrt{3}} \leq c_- p^{3/4} \log p\,,$$

where $c_- = \sqrt{2}\, c_+$. To cover the bound for all $p \geq 2$, it suffices to take $c_- = 4.25$.

On noticing that

$$m_\pm(p) = \min\left\{m_-(p),\, m_+(p)\right\},$$

the estimate (26) follows.

Now we focus on the other side of the triangle and consider a rectangle $\mathcal{R} \subset \mathcal{B}_+^\times(p)$ with one edge glued on the right edge of $\mathcal{B}_+^\times(p)$. The length of the horizontal edge of $\mathcal{R}$ is L and the length of the vertical one is H. As before, we assume that H is as large as possible.

Then, by the similarity of triangles, it follows that $H/(p/2) = (p/6 - L)/(p/6)$, that is, $H = (p - 6L)/2$. Then, the inequality (23) becomes

$$2\, b(p) \leq PL - 6L^2\,. \tag{31}$$

We need to find the smallest L for which (31) is satisfied, since

$$\frac{p}{2} - M_+ \leq \min_{2b(p) \leq pL - 6L^2} L\,.$$

Such an L gives rise to the estimate

$$\frac{p}{2} - M_+ \leq C_+ \sqrt{p}\, \log^2 p\,,$$

for some $C_+ > 2$, but it can be chosen infinitely close to 2 for all $p > p_{C_+}$.

The analogous estimate for M_- is obtained similarly in the other triangle $\mathcal{B}_-^\times$, and we get

$$\frac{p}{2} - M_- \leq C_- \sqrt{p}\, \log^2 p\,, \qquad \text{for } p \geq p_{C_-}\,.$$

Moreover, we get $C_- = 2\, C_+$ and $p_{C_-} = 2\, p_{C_+}$.

For instance, we may take get $C_+ = 3$ and $p_{C_+} = 8.6 \times 10^8$, but one may establish variants of these estimates, tightening up or down both the constants and/or the domain on which they are fulfilled.

By direct computation one then checks that the inequalities (27) and (28) are satisfied for every prime $2 \leq p \leq 8.6^8$.

The remaining part of the result follows from the proof of Lemma 2. □

We remark that the exponents 3/4 and 1/2 are essentially the smallest that can derived by this method. How much further can they be decreased? Let $\mathcal{R} = \mathcal{I} \times \mathcal{J} \subset [1, p]^2$ be a rectangle. Arguing probabilistically, if p is large, for any $x \in [1, p-1]$, the probability that $\overline{x} \in \mathcal{J}$ is $\sim |\mathcal{J}|/p$. Then the probability that there exists a point with coordinates $(x, \overline{x}) \in \mathcal{R}$ should be $\sim \mathrm{Area}(\mathcal{R})/p$. This leads us to conjecture that

Conjecture 1. *Let $\epsilon > 0$. We have*

$$\begin{aligned} m &= \frac{p}{3} + O(p^{1/2+\epsilon}), \\ M &= \frac{p}{2} + O(p^{\epsilon}). \end{aligned} \tag{32}$$

We claim that the exponent $1/2$ on the right side of (32) is best possible. Indeed, assume for instance that $p \equiv 1 (\mathrm{mod}\ 3)$. If $(x, y) \in \mathcal{B}_{-}^{\times}(p)$, write $x = \frac{p-1}{3} + a$, $y = \frac{p-1}{3} + b$, and then from $xy \equiv 1 (\mathrm{mod}\ p)$ it follows that $(3a-1)(3b-1) \equiv 9 (\mathrm{mod}\ p)$. We cannot have $(3a-1)(3b-1) = 9$, therefore $|(3a-1)(3b-1) - 9| \geq p$, and since $|b| \ll a$, we deduce that $a \gg \sqrt{p}$.

3. A sharper lower bound for $M(p)$ valid for an infinite set of primes

In this section we show that the inequality (9) holds for an infinite class of prime numbers p and we establish Theorem 3. For our construction to work we need an improvement over the well known Bombieri-Vinogradov Theorem. We may arrange the proof so that we work with a fixed residue class, and in such case a strong improvement over the Bombieri-Vinogradov Theorem has been provided in a series of papers by Bombieri, Friedlander and Iwaniec [5, 6, 7]. The Main Theorem from [7] gives a continuous transition from Bombieri-Vinogradov type theorems to Brun-Titchmarsh type theorems. It states that:

Theorem 6 (Bombieri-Friedlander-Iwaniec [7])**.** *Let $a \neq 0$ be an integer and $A > O$, $2 \leq Q \leq x^{3/4}$ be reals. Let $\mathcal{C}$ be the set of all integers q, prime to a, from an interval $Q' < q \leq Q$. Then*

$$\begin{aligned} &\sum_{q \in \mathcal{C}} \left| \pi(x; q, a) - \frac{\pi(x)}{\varphi(q)} \right| \\ &\qquad \leq \left\{ K\Big(\theta - \frac{1}{2}\Big)^2 \frac{x}{L} + O_A\Big(\frac{x}{L^3}\big(\log\log x\big)^2\Big) \right\} \sum_{q \in \mathcal{C}} \frac{1}{\varphi(q)} + O_{a,A}\Big(\frac{x}{L^A}\Big), \end{aligned} \tag{33}$$

where $\theta = \log Q / \log x$, $L = \log x$, K is absolute, and the subscripts of O indicate the dependence on those constants.

Fix a constant $c_3 > 1$, and two other constants $0 < c_4 < c_5$. Take a large positive real number X and apply the above estimate with $a = -9$, $A = 3$, $x = X$, $Q = c_5\sqrt{X}$, and $Q' = c_4\sqrt{X}$. Then $L = \log X$ and $\theta = \log Q / \log X = 1/2 + \log c_5 / \log X$, so

$$\left(\theta - \frac{1}{2}\right)^2 = \frac{\log^2 c_5}{\log^2 X}.$$

Landau [20, p. 113] showed that

$$\sum_{n \leq x} \frac{1}{\varphi(n)} = \alpha \log x + \beta + O\left(\frac{\log x}{x}\right),$$

with $\alpha > 0$ and β constants that can be explicitly given. This implies

$$\sum_{\substack{Q' < q < Q \\ (q,3)=1}} \frac{1}{\varphi(q)} = O\left(\sum_{Q' < q < Q} \frac{1}{\varphi(q)}\right) = O(1).$$

It follows that

$$\sum_{\substack{c_4\sqrt{X}<q<c_5\sqrt{X}\\(q,3)=1}}\left|\pi(X;q,-9)-\frac{\pi(X)}{\varphi(q)}\right|=O\left(\frac{X(\log\log X)^2}{\log^3 X}\right). \tag{34}$$

Applying the estimate a second time, with $a=-9$, $A=3$, $x=c_3X$, $Q=c_5\sqrt{X}$, and $Q'=c_4\sqrt{X}$, we have

$$\sum_{\substack{c_4\sqrt{X}<q<c_5\sqrt{X}\\(q,3)=1}}\left|\pi(c_3X;q,-9)-\frac{\pi(c_3X)}{\varphi(q)}\right|=O\left(\frac{X(\log\log X)^2}{\log^3 X}\right). \tag{35}$$

Next, we restrict the summation over q on the left sides of (34) and (35) to prime numbers congruent to $-1(\mathrm{mod}\ 3)$, and then combine the two estimates to obtain

$$\sum_{\substack{q\text{ prime}\\c_4\sqrt{X}<q<c_5\sqrt{X}\\q\equiv-1(\mathrm{mod}\ 3)}}\left|\pi(c_3X;q,-9)-\pi(X;q,-9)-\frac{\pi(c_3X)-\pi(X)}{q-1}\right|=O\left(\frac{X(\log\log X)^2}{\log^3 X}\right). \tag{36}$$

Furthermore,

$$\sum_{\substack{q\text{ prime}\\c_4\sqrt{X}<q<c_5\sqrt{X}\\q\equiv-1(\mathrm{mod}\ 3)}}\frac{1}{q}\sim\frac{\log c_5-\log c_4}{\log X}, \tag{37}$$

and

$$\sum_{\substack{q\text{ prime}\\c_4\sqrt{X}<q<c_5\sqrt{X}\\q\equiv-1(\mathrm{mod}\ 3)}}\frac{\pi(c_3X)-\pi(X)}{q-1}\sim\frac{(c_3-1)(\log c_5-\log c_4)X}{\log^2 X}. \tag{38}$$

Combining (36) and (38), we find that

$$\sum_{\substack{q\text{ prime}\\c_4\sqrt{X}<q<c_5\sqrt{X}\\q\equiv-1(\mathrm{mod}\ 3)}}(\pi(c_3X;q,-9)-\pi(X;q,-9))\sim\frac{(c_3-1)(\log c_5-\log c_4)X}{\log^2 X}. \tag{39}$$

Let us remark that for each prime number $p\le c_3X$, there are at most two prime numbers $q\in(c_4\sqrt{X},c_5\sqrt{X})$ for which $p\equiv-9(\mathrm{mod}\ q)$, so each prime p is counted at most twice on the left side of (39). We deduce that

$$\#\left\{p\ :\ \begin{array}{c}p\text{ prime, }X<p<c_3X,\\ p\equiv-9(\mathrm{mod}\ q),\ \text{ for some prime } q \text{ with}\\ c_4\sqrt{X}<q<c_5\sqrt{X}\text{ and }q\equiv-1(\mathrm{mod}\ 3)\end{array}\right\}\ge\frac{c_6X}{\log^2 X}, \tag{40}$$

for any fixed real number c_6, satisfying

$$0<c_6<\frac{(c_3-1)(\log c_5-\log c_4)}{2}, \tag{41}$$

and all X large enough.

We now take any prime p from the set on the left side of (40), choose a corresponding q, and write $p+9=qm$. We distinguish two cases.

(I) $p \equiv -1 (\mathrm{mod}\ 3)$. In this case we have $m \equiv 1 (\mathrm{mod}\ 3)$. We write q and m in the form $q = 3a - 1$, $m = 3b + 1$. Here a and b are positive integers, and each of them lies between two (suitable) constants times $\sqrt{X}$. We put $y = \frac{2p-1}{3} + a$, $x = \frac{p+1}{3} + b$. Then x and y are integers and satisfy the congruence $xy \equiv 1 (\mathrm{mod}\ p)$. The point (x, y) lies (for suitably chosen constants c_3, c_4 and c_5) inside the upper yellow triangle in Figure 2, close to its left vertex.

(II) $p \equiv 1 (\mathrm{mod}\ 3)$. In this case $m \equiv -1 (\mathrm{mod}\ 3)$. Write $q = 3a-1$, $m = 3b-1$. As before, a and b are positive integers and each lies between two constants times $\sqrt{X}$. We now put $x = \frac{p-1}{3} + a$, $y = \frac{p-1}{3} + b$. Then x and y are integers satisfying $xy \equiv 1 (\mathrm{mod}\ p)$. Moreover, one of the points (x, y) or (y, x) lies (for suitably chosen c_3, c_4 and c_5) inside the lower yellow triangle (shaded triangle in a black-white rendition of this article) in Figure 2, close to its left vertex.

Putting both cases together, we see that for such prime numbers p, the first equality in Conjecture 1 holds in the stronger form $m = p/3 + O(\sqrt{p})$. This m here is the one defined via the union of the two yellow triangles in Figure 2(a) (and 2(b)), and the implied constant is effectively computable.

In conclusion, we have proved the following theorem.

Theorem 7. *For all large X, we have $\#\{p \le X : M(p) > 2p/3 - c_8\sqrt{p}\} \ge c_7 X \log^{-2} X$.*

Finally, we will establish Theorem 3 stated in the introduction.

Proof of Theorem 3. The estimate (8) is a consequence of Theorem 5 and the inequality $M(p) \ge p - m_{\pm}(p)$, which follows by Corollary 1. Part 2 is a corollary of Theorem 7. □

References

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

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

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

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

[5] E. Bombieri, J.B. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli*, Acta Math. **156** (1986), 203–251.

[6] E. Bombieri, J.B. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli. II*, Math. Ann. **277** (1987), 361–393.

[7] E. Bombieri, J.B. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli. III*, J. Amer. Math. Soc. **2**, (1989), 215–224.

[8] B. Bzdęga, *Bounds on ternary cyclotomic coefficients*, Acta Arith. **144** (2010), 5–16.

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

[10] C. Cobeli, S.M. Gonek and A. Zaharescu, *The distribution of patterns of inverses modulo a prime*, J. Number Theory **101**, (2003), 209–222.

[11] C. Cobeli, M. Vâjâitu and A. Zaharescu, *Average estimates for the number of tuples of inverses* (mod p) *in short intervals*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **43** (91), (2000), 155–164.

[12] V. Felsch and E. Schmidt, *Über Perioden in den Koeffizienten der Kreisteilungspolynome $F_{np}(x)$*, *Math. Z.* **106** (1968), 267-272.

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

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

[15] H. Iwaniec, *Almost-primes represented by quadratic polynomials*, Invent. Math. **47** (1978), 171–188.
[16] J. Justin, *Bornes des coefficients du polynôme cyclotomique et de certains autres polynômes*, C. R. Acad. Sci. Paris Sr. A-B **268** (1969), A995–A997
[17] N. Kaplan, *Flat cyclotomic polynomials of order three*, J. Number Theory **127** (2007), 118–126.
[18] T.Y. Lam and K.H. Leung, *On the cyclotomic polynomial* $\Phi_{pq}(X)$, Amer. Math. Monthly **103** (1996), 562–564.
[19] M. Laczkovich, *Discrepancy estimates for sets with small boundary*, Studia Sci. Math. Hungar. **30** (1995), 105–109.
[20] E. Landau, *Collected works*, Vol. 1., L. Mirsky, I. J. Schoenberg, W. Schwarz and H. Wefelscheid (Eds.), Thales-Verlag, Essen, 1985.
[21] H. Möller, *Über die Koeffizienten des nten Kreisteilungspolynoms*, Math. Z. **119** (1971), 33–40.
[22] P. Moree and E. Roşu, *Non-Beiter ternary cyclotomic polynomials with an optimally large set of coefficients*, arXiv:1111.6800v1, to appear in the International Journal of Number Theory (2012).
[23] I. E. Shparlinski, *Modular hyperbolas*, preprint, arXiv:1103.2879.
[24] R. Thangadurai, *On the coefficients of cyclotomic polynomials*, *Cyclotomic fields and related topics* (Pune, 1999), 311–322, Bhaskaracharya Pratishthana, Pune, 2000.
[25] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. USA **34** (1948), 204–207.
[26] H. Weyl, *On the volume of tubes*, Amer. J. Math. **61** (1939), 461–472.
[27] J. Zhao and X. Zhang, *Coefficients of ternary cyclotomic polynomials*, J. Number Theory **130** (2010), 2223–2237.

Cristian Cobeli, Institute of Mathematics "Simion Stoilow" of the Romanian Academy, P. O. Box 1-764, Bucharest 70700, Romania.
E-mail address: cristian.cobeli@imar.ro

Yves Gallot, 12 bis rue Perrey, 31400 Toulouse, France.
E-mail address: galloty@orange.fr

Pieter Moree, Max-Planck-Institut für Mathematik, Vivatsgasse 7, D–53111 Bonn, Germany.
E-mail address: moree@mpim-bonn.mpg.de

Alexandru Zaharescu, Department of Mathematics, University of Illinois at Urbana-Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, Illinois 61801, USA and Institute of Mathematics "Simion Stoilow" of the Romanian Academy, P. O. Box 1-764, Bucharest 70700, Romania.
E-mail address: zaharesc@math.uiuc.edu