Available online at www.sciencedirect.com

ScienceDirect

Indagationes Mathematicae 24 (2013) 915–929

indagationes mathematicae

www.elsevier.com/locate/indag

Sister Beiter and Kloosterman: A tale of cyclotomic coefficients and modular inverses

Cristian Cobeli[a,*], Yves Gallot[b], Pieter Moree[c], Alexandru Zaharescu[d,a]

[a] *"Simion Stoilow" Institute of Mathematics of the Romanian Academy, 21 Calea Grivitei Street, P. O. Box 1-764, Bucharest 014700, Romania*

[b] *12 bis rue Perrey, 31400 Toulouse, France*

[c] *Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany*

[d] *Department of Mathematics, University of Illinois at Urbana–Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, IL 61801, USA*

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 $M(p) \le (p+1)/2$. In 2009 Gallot and Moree showed that $M(p) \ge 2p(1-\epsilon)/3$ 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 $M(p)$.

Keywords: Cyclotomic coefficients; Sister Beiter conjecture; Modular inverses; Kloosterman sums

1. Introduction

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

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

* Corresponding author.
E-mail addresses: cristian.cobeli@gmail.com, cristian.cobeli@imar.ro (C. Cobeli), galloty@orange.fr (Y. Gallot), moree@mpim-bonn.mpg.de (P. Moree), zaharesc@math.uiuc.edu (A. Zaharescu).

0019-3577/$ - see front matter
doi:10.1016/j.indag.2013.01.002

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 [23].

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

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

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 [16] 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 $b \geq a$. Bzdęga [8] showed that

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

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 [15] 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 [20] gave a construction showing that $M(p) \geq (p + 1)/2$ for $p > 5$. On the other hand, in 1968 Sister Marion Beiter [1] had conjectured (a conjecture she repeated in 1971 [2]) that $M(p) \leq (p+1)/2$ 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 $M(5) \leq 3$ (established independently by Beiter [2] and Bloom [4]) shows that $M(5) = 3$. Zhao and Zhang [26] showed