Max-Planck-Institut für Mathematik
Bonn

Cyclotomic polynomial coefficients $a(n,k)$ with n and k in prescribed residue classes

by

Jessica Fintzen

Max-Planck-Institut für Mathematik
Preprint Series 2010 (85)

Cyclotomic polynomial coefficients $a(n,k)$ with n and k in prescribed residue classes

Jessica Fintzen

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Jacobs University Bremen
College Ring 3
Mailbox 341
28759 Bremen
Germany

MPIM 10-85

Cyclotomic polynomial coefficients $a(n,k)$ with n and k in prescribed residue classes

Jessica Fintzen

Abstract

Let $a(n,k)$ be the kth coefficient of the nth cyclotomic polynomial. In 2009 Ji, Li and Moree showed that $\{a(n,k) \mid n \equiv 0 \bmod d, n \geq 1, k \geq 0\} = \mathbb{Z}$. In this paper we will determine $\{a(n,k) \mid n \equiv a \bmod d, k \equiv b \bmod f, n \geq 1, k \geq 0\}$.

1 Introduction

Let

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} (x - e^{\frac{2\pi i k}{n}}) = \sum_{k=0}^{\varphi(n)} a(n,k) x^k$$

be the nth cyclotomic polynomial, where φ denotes Euler's totient function, and set $a(n,k) = 0$ for $k > \varphi(n)$.

It can be shown that $a(n,k) \in \mathbb{Z}$. In the 19th century it was conjectured that $|a(n,k)| \leq 1$, which is the case for $n < 105$. However, $a(105,7) = -2$, and in 1931 Schur proved in a letter to Landau (cf. [3]) that $|a(n,k)|$ is unbounded. In 1987 Suzuki [5] showed that $\{a(n,k) \mid n \geq 1, k \geq 0\} = \mathbb{Z}$, and in 2009 Ji, Li and Moree [2] proved the generalization $\{a(mn,k) \mid n \geq 1, k \geq 0\} = \mathbb{Z}$ for an arbitrary fixed positive integer m.

In this paper we will show that one can restrict n and k even further and still obtain every integer as coefficient $a(n,k)$.

Theorem 1. *Let $a < d$ and $b < f$ be four nonnegative integers. Denote $s(n) = n \cdot \prod_{\substack{p \mid n \\ p \text{ prime}}} p^{-1}$. Then*

$$\{a(n,k) \mid n \equiv a \bmod d, k \equiv b \bmod f, n \geq 1, k \geq 0\} = \begin{cases} \mathbb{Z} & \text{if } (s((a,d)), f) \mid b\,; \\ \{0\} & \text{otherwise}. \end{cases}$$

MSC: 11B83, 11C08

Keywords: cyclotomic polynomial, Dirichlet's Theorem, residue classes

We would like to remark that the result also holds true if one replaces the coefficients $a(n,k)$ of the cyclotomic polynomials by the coefficients $c(n,k)$ of the inverse cyclotomic polynomials (see Section 2, equation (3) for a definition), which is a direct corollary to Theorem 1, see Corollary 1 in Section 4.

2 Some properties of cyclotomic polynomials

Using the identity

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \tag{1}$$

and the Möbius inversion formula, one can show that for $n > 1$

$$\Phi_n(x) = \prod_{d|n} (1 - x^d)^{\mu(\frac{n}{d})}, \tag{2}$$

where μ denotes the Möbius function. From equation (2) one can deduce the following lemma (for a proof see, e.g., Thangadurai [6]).

Lemma 1. *Let $n > 1$ and $k \geq 0$ be integers.*

a) If p and q are primes satisfying $k < p < q$ and $(n, pq) = 1$, we have $a(pqn, k) = a(n, k)$.

b) If n is odd, we have $a(2n, k) = a(n, k) \cdot (-1)^k$.

c) If $p|n$, we have $a(pn, pk) = a(n, k)$.

d) If $s(n) \nmid k$, we have $a(n, k) = 0$.

Another helpful tool will be the consideration of the coefficients of the power series expansion of the inverse cyclotomic polynomial $\Phi_n(x)^{-1}$ at $x = 0$. We denote

$$\frac{1}{\Phi_n(x)} = \sum_{k=0}^{\infty} c(n,k) x^k. \tag{3}$$

The coefficients $c(n,k)$ are integers, see for example Moree [4], and we have the following relation with the coefficients of the cyclotomic polynomials, cf. Gallot, Moree and Hommersom [1].

Lemma 2. *Let k be a nonnegative integer and p a prime exceeding k and coprime with $n > 1$. Then $a(pn, k) = c(n, k)$ and $c(pn, k) = a(n, k)$.*

This lemma follows from equation (2) and

$$\sum_{k=0}^{\infty} c(n,k)x^k = \frac{1}{\Phi_n(x)} = \prod_{d|n}(1-x^d)^{-\mu(\frac{n}{d})} \tag{4}$$

(for $|x| < 1$ and $n > 1$).

Definition 1. Let n and k be integers with $n > 0$. Denote by $(k \bmod n)$ the unique integer satisfying $(k \bmod n) \equiv k \bmod n$ and $0 \le (k \bmod n) < n$.

Lemma 3. *Let $n > 0$ and $k \ge 0$ be integers.*

a) We have $c(n,k) = c(n,(k \bmod n))$.

b) If $(k \bmod n) > n - \varphi(n)$, then $c(n,k) = 0$.

Proof. From equation (1) it follows that

$$\sum_{k=0}^{\infty} c(n,k)x^k = \frac{1}{\Phi_n(x)} = -\left(\prod_{d|n,\, d<n} \Phi_d(x)\right)\sum_{j=0}^{\infty} x^{jn}\,.$$

As $\prod_{d|n,\, d<n} \Phi_d(x)$ has degree $n - \varphi(n) < n$, we obtain $c(n,k) = c(n,(k \bmod n))$ and $c(n,k) = 0$ for $(k \bmod n) > n - \varphi(n)$. □

Lemma 4. *Let $n > 1$ be a positive integer, then $c(n,1) = \mu(n)$.*

Proof. Using equation (4) we obtain

$$\sum_{k=0}^{\infty} c(n,k)x^k = \prod_{d|n}(1-x^d)^{-\mu(\frac{n}{d})} \equiv (1-x)^{-\mu(n)} \equiv 1 + \mu(n)x \bmod x^2,$$

and therefore $c(n,1) = \mu(n)$. □

3 Warm-up: special cases of Theorem 1

Before we tackle Theorem 1 in its full generality, we want to demonstrate that it becomes an easy generalization of Theorem 2 if we restrict only n or k to a prescribed residue class while the other variable is not required to satisfy any congruence condition.

Theorem 2. *Let m and N be positive integers. Then*

$$\{a(mn,k)\,|\,n > 1, k \ge 0, (n,N) = 1\} = \mathbb{Z}$$

and

$$\{c(mn,k)\,|\,n > 1, k \ge 0, (n,N) = 1\} = \mathbb{Z}.$$

This theorem follows easily from the proof of $\{a(n,k)\,|\,n \equiv 0 \bmod d, n \geq 1, k \geq 0\} = \mathbb{Z}$ by Ji, Li and Moree [2]. Using it, we prove the following two special cases of Theorem 1.

Theorem 3. *Let $b < f$ be two nonnegative integers. Then*

$$\{a(n,k)\,|\,k \equiv b \bmod f, n \geq 1, k \geq 0\} = \mathbb{Z}\,.$$

Proof. Let z be an arbitrary integer. By Theorem 2 there exist an integer $n > 1$, $(n,f) = 1$ and an integer $k \geq 0$ such that $c(n,k) = z$. As $(n,f) = 1$, we can find an integer $r \geq 1$ with $nr \equiv b - k \bmod f$. Let $p > nr + k$ be a prime. Then by Lemma 2 and Lemma 3 we obtain

$$a(np, nr + k) = c(n, nr + k) = c(n,k) = z$$

with $nr + k \equiv b \bmod f$. □

Theorem 4. *Let $a < d$ be two nonnegative integers. Then*

$$\{a(n,k)\,|\,n \equiv a \bmod d, n \geq 1, k \geq 0\} = \mathbb{Z}\,.$$

Proof. Let $g = (a,d)$, and denote by z an arbitrary integer. Using Theorem 2, there exist an integer $n > 1$, $(n, \frac{d}{g}) = 1$ and an integer $k \geq 0$ such that $c(ng,k) = z$. By Dirichlet's Prime Number Theorem we can pick a prime $p > \max\{k, ng\}$ that satisfies $p \equiv n^{-1}\frac{a}{g} \bmod \frac{d}{g}$. Then by Lemma 2 we have $a(npg,k) = c(ng,k) = z$ with $npg \equiv a \bmod d$. □

Although these special cases have relatively easy proofs, the combination of the congruence restrictions on both n and k in Theorem 1 requires a more complicated proof.

4 The main theorem

Before proving Theorem 1, we will first prove the following key result.

Lemma 5. *Let $a < d$, $b < d$ be three nonnegative integers such that (a,d) is squarefree. Then*

$$\{a(n,k)\,|\,n \equiv a \bmod d, k \equiv b \bmod d, n \geq 1, k \geq 0\} = \mathbb{Z}\,.$$

Let $c = (a,d)$. We will prove Lemma 5 in two parts. First we will consider when c is odd, and then the case where c is even will follow easily.

Suppose c is odd. We will start this case by proving that all negative integers are contained in $\{a(n,k)\,|\,n \equiv a \bmod d, k \equiv b \bmod d,\ n \geq 1, k \geq 0\}$. In order to do this we will show that for every positive integer t there exist positive integers m and q satisfying certain conditions such that $a(cqm,k) = -t$. For this we will need three lemmas. The first will ensure that the integer m can be chosen as a product of primes that are in a prescribed primitive residue class and satisfy certain size conditions. The other two will show that there exist residue classes satisfying the properties that we will need later.

Lemma 6. *Let a, m and t be positive integers with $(a, m) = 1$. Then for each N there exists $n > N$ such that the interval $[n, \frac{3}{2}n)$ contains at least t primes satisfying $p \equiv a \bmod m$.*

Proof. Assume that there exists N_0 such that for every $n \geq N_0$ the interval $[n, \frac{3}{2}n)$ contains less than t primes satisfying $p \equiv a \bmod m$. Then for all $x \geq N_0$ we have

$$\sum_{\substack{p \leq x,\, p \text{ prime} \\ p \equiv a \bmod m}} 1 < N_0 + \log \frac{x}{N_0} \left(\log \frac{3}{2} \right)^{-1} \cdot (t-1) = O(\log x),$$

which contradicts the quantitative version of Dirichlet's Prime Number Theorem

$$\sum_{\substack{p \leq x,\, p \text{ prime} \\ p \equiv a \bmod m}} 1 = (1 + o(1)) \frac{x}{\varphi(m) \log x}.$$

□

Lemma 7. *Let s be an integer, and let d be an odd squarefree natural number. Then there exists an integer x such that $(x, d) = (x + s, d) = 1$.*

Proof. Let $d = \prod_{i=1}^{n} p_i$ be the prime factorization of d with $n \geq 1$ (for $d = 1$ the lemma holds obviously true). For each odd prime there exists an x_i such that $(x_i, p_i) = (x_i + s, p_i) = 1$. Hence by the Chinese Remainder Theorem there exists an integer x satisfying $x \equiv x_i \bmod p_i$ for $1 \leq i \leq n$, and we have $(x, d) = (x + s, d) = 1$. □

Lemma 8. *Let s and $y < c$ be nonnegative integers and let $q_1, \ldots, q_N$ be $N > 1$ distinct primes larger than $\max\{c, 2N + 1\}$. Define $q = \prod_{i=1}^{N} q_i$. Then there exists an integer u with $(u, q) = (u + s, q) = 1$ such that the system of congruences*

$$\begin{aligned} k &\equiv u + s \bmod q \\ k &\equiv y \bmod c \end{aligned}$$

implies

$$cq - \varphi(cq) < (k \bmod cq).$$

Proof. Consider the set $S = \{cq + y - c \cdot j - s \,|\, 1 \leq j \leq 2N + 1\}$. As $q_i > 2N + 1$ and $(q_i, c) = 1$, for each $1 \leq i \leq N$ there is at most one element in S that is not coprime with q_i and at most one element $r \in S$ with $(r + s, q_i) \neq 1$. Thus there exists $u \in S$ with $(u, q) = (u + s, q) = 1$. Note that $u + s \equiv y \bmod c$ and $0 < u + s < cq$. Hence

$$\begin{aligned} (k \bmod cq) &= u + s \geq cq + y - c(2N + 1) \\ &> cq - \prod_{i=1}^{2} (q_i - 1) \geq cq - \prod_{i=1}^{N} (q_i - 1) \geq cq - \varphi(cq). \end{aligned}$$

□

Now we have the necessary preliminaries to prove Lemma 5.

Proof of Lemma 5.
Denote, as above, the squarefree natural number (a, d) by c, and let d_2 be the largest positive integer satisfying

$$d = d_1 d_2 \quad \text{and} \quad (b, d_2) = 1 \quad \text{and} \quad d_1 \in \mathbb{Z}\,. \tag{5}$$

Note that this implies $(d_1, d_2) = 1$. Furthermore, write $c = c_1 c_2$ with nonnegative integers c_1 and c_2 satisfying $c_1 | d_1$ and $c_2 | d_2$.

We distinguish two cases.

Case 1. c **is odd.** Let s be a positive integer coprime with c_1. Note that this implies $(b - s, c_1) = 1$ as every prime divisor of c_1 divides by definition d_1 and therefore b and thus does not divide $b - s$. In addition, by Lemma 7 there exists an integer x such that $(x, c_2) = (x + s, c_2) = 1$ because c_2 is odd in this case. Denote by γ the smallest positive integer satisfying $(c_2\gamma, \frac{d_2}{c_2\gamma}) = 1$. Note that this implies $(x + s, \gamma) = 1$. Since the moduli are coprime and their product is divisible by c, there exists a unique integer $0 \le y < c$ such that the system of congruences

$$\begin{aligned} k &\equiv b \bmod d_1 \\ k &\equiv x + s \bmod c_2\gamma \\ k &\equiv 1 \bmod \frac{d_2}{c_2\gamma} \end{aligned} \tag{6}$$

implies

$$k \equiv y \bmod c\,.$$

Let $q_1, \ldots, q_N$ be $N > 1$ distinct primes all larger than $\max\{d, 2N + 7\}$ and define $q = \prod_{i=1}^{N} q_i$. According to Lemma 8 there exists an integer u such that $(u, q) = (u + s, q) = 1$ and such that $k \equiv u + s \bmod q$ together with the system of congruences (6) implies

$$cq - \varphi(cq) < (k \bmod cq)\,. \tag{7}$$

Furthermore, by the Chinese Remainder Theorem we can find an integer v such that

$$p_i \equiv v \bmod dq$$

implies

$$\begin{aligned} p_i &\equiv u \bmod q \\ p_i &\equiv b - s \bmod c_1 \\ p_i &\equiv x \bmod c_2\,. \end{aligned} \tag{8}$$

As $(u, q) = (b - s, c_1) = (x, c_2) = 1$, the integer v can (and will) be chosen coprime with dq. In addition, since d and q are coprime, there exists an integer w such that the system of congruences

$$\begin{aligned} k &\equiv u+s \bmod q \\ k &\equiv b \bmod d_1 \\ k &\equiv x+s \bmod c_2\gamma \\ k &\equiv 1 \bmod \frac{d_2}{c_2\gamma} \end{aligned} \tag{9}$$

is equivalent to

$$k \equiv w \bmod dq\,.$$

Note that therefore $k \equiv w \bmod dq$ implies $k \equiv b \bmod c_1$ and $k \equiv x+s \bmod c_2$.

Given an arbitrary positive integer t by Lemma 6 there exist primes $p_1, \ldots, p_t$ such that $\max\{2dq, 2N+7\} < p_1 < p_2 < \ldots < p_t < \frac{3}{2}p_1$ and $p_i \equiv v \bmod dq$ for $1 \leq i \leq t$. As $2p_1 - \frac{3}{2}p_1 - \frac{1}{2} \geq dq$, we can choose an integer $k \equiv w \bmod dq$ with $\frac{3p_1}{2} < k < 2p_1$.
Set

$$m = \begin{cases} p_1p_2\cdots p_tp_{t+1} & \text{if } t \text{ is even;} \\ p_1p_2\cdots p_t & \text{otherwise,} \end{cases}$$

where $p_{t+1} > 2p_1$ is a prime. Then we obtain (cf. also [2])

$$\begin{aligned} \Phi_{cqm}(x) &\equiv \prod_{r|cqm,\ r<k+1} (1-x^r)^{\mu(\frac{cqm}{r})} \bmod x^{k+1} \\ &\equiv \prod_{r|cq}(1-x^r)^{\mu(\frac{cq}{r})\mu(m)} \prod_{i=1}^{t}(1-x^{p_i})^{\mu(\frac{cqm}{p_i})} \bmod x^{k+1} \\ &\equiv \Phi_{cq}(x)^{\mu(m)} \prod_{i=1}^{t}(1-x^{p_i})^{-\mu(cqm)} \bmod x^{k+1} \\ &\equiv \frac{1}{\Phi_{cq}(x)} \prod_{i=1}^{t}(1-x^{p_i})^{\mu(cq)} \bmod x^{k+1} \\ &\equiv \frac{1}{\Phi_{cq}(x)} \left(1-\mu(cq)\sum_{i=1}^{t} x^{p_i}\right) \bmod x^{k+1}\,. \end{aligned}$$

Thus by Lemma 3 together with equation (7) and the systems of congruences (8) and (9) we obtain

$$\begin{aligned} a(cqm,k) &= c(cq,k) - \mu(cq)\sum_{i=1}^{t} c(cq,k-p_i) = 0 - \mu(cq)\sum_{i=1}^{t} c(cq,s) \\ &= -\mu(cq)tc(cq,s)\,. \end{aligned} \tag{10}$$

Let us first consider the case $s=1$. As $c(cq,1) = \mu(cq)$ by Lemma 4, equation (10) yields

$$a(cqm,k) = -\mu(cq)^2 t = -t\,. \tag{11}$$

Since $(b, d_2) = 1$ and $(x + s, c_2\gamma) = 1$, we infer from Dirichlet's Prime Number Theorem the existence of a prime $q_{N+1} > k$ coprime with dqm such that

$$\begin{aligned} q_{N+1} &\equiv 1 \bmod d_1, \\ q_{N+1} &\equiv b(x+s)^{-1} \bmod c_2\gamma \\ \text{and} \qquad q_{N+1} &\equiv b \bmod \frac{d_2}{c_2\gamma}. \end{aligned}$$

Let $q_{N+2} > k$ be a prime coprime with $cqmq_{N+1}$ and satisfying

$$q_{N+2} \equiv \frac{a}{c}(qmq_{N+1}^2)^{-1} \bmod \frac{d}{c}\,.$$

Using Lemma 1, the system of congruences (9) and equation (11), we obtain

$$a(cqmq_{N+1}^2 q_{N+2}, kq_{N+1}) = a(cqmq_{N+1}q_{N+2}, k) = a(cqm, k) = -t$$

with

$$cqmq_{N+1}^2 q_{N+2} \equiv qmq_{N+1}^2 a(qmq_{N+1}^2)^{-1} \equiv a \bmod d \;\text{ and}$$

$$kq_{N+1} \equiv b \bmod d_1\,,\; kq_{N+1} \equiv b \bmod c_2\gamma \text{ and } kq_{N+1} \equiv b \bmod \frac{d_2}{c_2\gamma}, \text{ i.e. } kq_{N+1} \equiv b \bmod d\,.$$

Hence, if $c = (a, d)$ is odd, we have

$$\mathbb{Z}_{<0} \subseteq \{a(n, k) \,|\, n \equiv a \bmod d, k \equiv b \bmod d, n \geq 1, k \geq 0\}. \tag{12}$$

As $a(n, k) = 0$ for every $k > \varphi(n)$, it only remains to show that

$$\mathbb{Z}_{>0} \subseteq \{a(n, k) \,|\, n \equiv a \bmod d, k \equiv b \bmod d, n \geq 1, k \geq 0\}\,.$$

In order to do this we will proceed as above, this time exploiting the fact that we proved that $-1 \in \{a(n, k) \,|\; n \equiv a \bmod d, k \equiv 1 \bmod d, n \geq 1, k \geq 0\}$.

Define

$$q_0 = \begin{cases} q & \text{if } \mu(cq) = 1; \\ qq_{N+3} & \text{otherwise,} \end{cases}$$

where $q_{N+3} > \max\{d, 2N + 7\}$ is a prime coprime to q. Then for the special case $b = s = t = 1$ the construction of equation (11) establishes the existence of a prime $m_0 > \max\{2dq, 2N + 7\}$ and an integer $k_0 \geq 0$ such that $a(cq_0m_0, k_0) = -1$ with $(k_0, c) = 1$ (consider the system of congruences (9)).

Let $\tilde{q} = q_0m_0q_{N+4}$, where q_{N+4} is a prime larger than k_0 and coprime with cq_0m_0. Then $\tilde{q}$ is a product of at most $N+3$ and at least 2 primes that are all larger than $\max\{d, 2(N+3)+1\}$. Note that we can therefore apply Lemma 8. Hence by the construction of equation (10) above and by setting $s = k_0$, there exists a product $\widetilde{m}$ of primes all larger than $2d\tilde{q}$ and a nonnegative integer $\tilde{k}$ such that

$$\begin{aligned} a(c\tilde{q}\widetilde{m}, \tilde{k}) &= -\mu(c\tilde{q}) \sum_{i=1}^{t} c(c\tilde{q}, k_0) = -\mu(cq_0 m_0 q_{N+4}) tc(cq_0 m_0 q_{N+4}, k_0) \\ &= -ta(cq_0 m_0, k_0) = t \end{aligned} \tag{13}$$

(we used Lemma 2 for the third equality) and

$$\tilde{k} \equiv u + k_0 \bmod q \ \tilde{k} \equiv b \bmod d_1 \,, \ \tilde{k} \equiv \widetilde{x} + k_0 \bmod c_2\gamma \quad \text{and} \quad \tilde{k} \equiv 1 \bmod \frac{d_2}{c_2\gamma} \,,$$

where $\widetilde{x}$ is an integer satisfying $(\widetilde{x}, c_2) = (\widetilde{x} + k_0, c_2) = 1$. By choosing a prime $\widetilde{q}_{N+1} > \tilde{k}$ coprime with $d\tilde{q}\widetilde{m}$ that satisfies the following system of congruences

$$\begin{aligned} \widetilde{q}_{N+1} \equiv &\ 1 \bmod d_1 \\ \widetilde{q}_{N+1} \equiv &\ b(\widetilde{x} + k_0)^{-1} \bmod c_2\gamma \\ \widetilde{q}_{N+1} \equiv &\ b \bmod \frac{d_2}{c_2\gamma} \end{aligned}$$

and a prime $\widetilde{q}_{N+2} > \tilde{k}$ coprime with $c\tilde{q}\widetilde{m}\widetilde{q}_{N+1}$ satisfying

$$\widetilde{q}_{N+2} \equiv \frac{a}{c} (\tilde{q}\widetilde{m}\widetilde{q}_{N+1}^2)^{-1} \bmod \frac{d}{c},$$

we obtain

$$a(c\tilde{q}\widetilde{m}\widetilde{q}_{N+1}^2 \widetilde{q}_{N+2}, \tilde{k}\widetilde{q}_{N+1}) = a(c\tilde{q}\widetilde{m}\widetilde{q}_{N+1}\widetilde{q}_{N+2}, \tilde{k}) = a(c\tilde{q}\widetilde{m}, \tilde{k}) = t,$$

with

$$c\tilde{q}\widetilde{m}\widetilde{q}_{N+1}^2 \widetilde{q}_{N+2} \equiv \tilde{q}\widetilde{m}\widetilde{q}_{N+1}^2 a (\tilde{q}\widetilde{m}\widetilde{q}_{N+1}^2)^{-1} \equiv a \bmod d \quad \text{and} \quad \tilde{k}\widetilde{q}_{N+1} \equiv b \bmod d \,.$$

Hence we have $\mathbb{Z}_{>0} \subseteq \{a(n,k) \,|\, n \equiv a \bmod d, k \equiv b \bmod d, n \geq 1, k \geq 0\}$, and therefore

$$\mathbb{Z} = \{a(n,k) \,|\, n \equiv a \bmod d, k \equiv b \bmod d, n \geq 1, k \geq 0\} \,.$$

Case 2. c **is even.** We distinguish two subcases.

Case 2.1. $4|d$. The condition that $c = (a,d)$ is squarefree implies that $4 \nmid (a,d)$, but $2|(a,d)$ and therefore $\frac{a}{2}$ is an odd integer. Hence by Case 1 for every integer z there exist integers $n \equiv \frac{a}{2} \bmod d$ and $k \equiv b \bmod d$ such that $a(n,k) = z \cdot (-1)^b$. By Lemma 1 we obtain

$$a(2n,k) = a(n,k) \cdot (-1)^k = z \cdot (-1)^b \cdot (-1)^b = z$$

with $2n \equiv 2\frac{a}{2} \equiv a \bmod d$.

Case 2.2. $4 \nmid d$**.** As $\frac{d}{2}$ is an odd integer, there exists an integer β with $2\beta \equiv 1 \bmod \frac{d}{2}$. Then $(\beta, \frac{d}{2}) = 1$, and, since $\frac{d}{2} + a\beta$ is odd, we have that $(\frac{d}{2} + a\beta, d) = \frac{1}{2}(a, d)$ is squarefree. Thus by Case 1 for every integer z there exist integers $n \equiv \frac{d}{2} + a\beta \bmod d$ and $k \equiv b \bmod d$ such that $a(n, k) = z \cdot (-1)^b$. Using Lemma 1, we obtain

$$a(2n, k) = a(n, k) \cdot (-1)^k = z \cdot (-1)^b \cdot (-1)^b = z$$

with $2n \equiv 2\left(\frac{d}{2} + a\beta\right) \equiv a \bmod d$.

We conclude that also in this case $\{a(n, k) \,|\, n \equiv a \bmod d, k \equiv b \bmod d, n \geq 1, k \geq 0\} = \mathbb{Z}$.

□

Now we are ready to prove Theorem 1.

Proof of Theorem 1.
We denote (a, d) by c and distinguish two cases.

Case 1. $(s(c), f) | \, b$**.** We want to show that in this case

$$\{a(n, k) \,|\, n \equiv a \bmod d, k \equiv b \bmod f, n \geq 1, k \geq 0\} = \mathbb{Z}\,.$$

Note that every prime divisor of $s(c)$ divides $\frac{c}{s(c)}$, which divides every integer congruent $\frac{a}{(s(c),f)} \bmod \frac{d}{(s(c),f)}$. Hence it is enough to find for every integer z integers

$$n \equiv \frac{a}{(s(c), f)} \bmod \frac{d}{(s(c), f)} \quad \text{and} \quad k \equiv \frac{b}{(s(c), f)} \bmod \frac{f}{(s(c), f)}$$

with $a(n, k) = z$ because by Lemma 1 we have

$$a(n(s(c), f), k(s(c), f)) = a(n, k) = z$$

with $n(s(c), f) \equiv a \bmod d$ and $k(s(c), f) \equiv b \bmod f$. As

$$\begin{aligned}
\left(s\left(\left(\frac{a}{(s(c), f)}, \frac{d}{(s(c), f)}\right)\right), \frac{f}{(s(c), f)}\right) &= \left(s\left(\frac{(a, d)}{(s(c), f)}\right), \frac{f}{(s(c), f)}\right) \\
&= \left(\frac{s\left((a, d)\right)}{(s(c), f)}, \frac{f}{(s(c), f)}\right) \\
&= \left(\frac{s\left(c\right)}{(s(c), f)}, \frac{f}{(s(c), f)}\right) \\
&= 1,
\end{aligned}$$

we can assume without loss of generality that $(s(c), f) = 1$.

We will now modify the restrictions $n \equiv a \bmod d$ and $k \equiv b \bmod f$ on the coefficients $a(n, k)$ to be able to apply Lemma 5.

Define

$$\lambda(x) = \prod_{\substack{p|x,\, p^2 \nmid x, \\ p\, prime}} p,$$

and let g_2 be the largest positive integer such that

$$g = lcm\left(\frac{d}{s(c)}, f\right) = g_1 g_2 \quad \text{and} \quad \left(\frac{d}{s(c)}, g_2\right) = 1\,,$$

where g_1 is a positive integer. Let

$$n_0 = \frac{a}{s(c)} + \frac{d}{s(c)} \lambda\left(\frac{a}{s(c)}\right)\,.$$

As $(g_1, g_2) = 1$, by the Chinese Remainder Theorem there exists a unique y satisfying $0 \leq y < g$ such that

$$n \equiv n_0 \bmod g_1 \quad \text{and} \quad n \equiv 1 \bmod g_2$$

is equivalent to

$$n \equiv y \bmod g\,.$$

Note that (n_0, g_1) is squarefree because if p is a prime with $p^2|\,(n_0, g_1)$, then $p^2|g_1$ implies $p|\frac{d}{s(c)}$ by definition of g_1. Hence $p|\frac{a}{s(c)}$ (see definition of n_0). If, however, $p^2|\frac{a}{s(c)}$, then $p^2 \nmid \frac{d}{s(c)}$ and $p \nmid \lambda\left(\frac{a}{s(c)}\right)$, which contradicts $p^2|\,(n_0, g_1)$. Thus $p^2 \nmid \frac{a}{s(c)}$, which implies $p|\lambda\left(\frac{a}{s(c)}\right)$ and therefore $p^2|\frac{d}{s(c)}\lambda\left(\frac{a}{s(c)}\right)$, which again contradicts $p^2|\,(n_0, g_1)$. We conclude that (y, g) is squarefree, and for a given integer z by Lemma 5 there exist integers $n \equiv y \bmod g$ and $k \equiv b \bmod g$ such that $a(n, k) = z$.

Let $p > \max\{d, k, n\}$ be a prime satisfying

$$p \equiv (s(c))^{-1} \bmod f,$$

and let $q > p$ be a prime such that

$$q \equiv p^{-2} \bmod d\,.$$

Since $n \equiv n_0 \bmod g_0$ implies $n \equiv \frac{a}{s(c)} \bmod \frac{d}{s(c)}$, every prime divisor of $s(c)$ divides n, and we have by Lemma 1

$$a(ns(c)p^2q, ks(c)p) = a(np^2q, kp) = a(npq, k) = a(n, k) = z.$$

Furthermore, using $n \equiv n_0 \bmod \frac{d}{s(c)}$, we have

$$ns(c)p^2q \equiv n_0 s(c)p^2p^{-2} \equiv \left(\frac{a}{s(c)} + \frac{d}{s(c)}\lambda\left(\frac{a}{s(c)}\right)\right) s(c) \equiv a \bmod d$$

and $ks(c)p \equiv bs(c)(s(c))^{-1} \equiv b \bmod f$.

Hence $\{a(n,k) \,|\, n \equiv a \bmod d, k \equiv b \bmod f, n \geq 1, k \geq 0\} = \mathbb{Z}$, as desired.

Case 2. $(s(c), f) \nmid b$**.** Suppose that $n \equiv a \bmod d$ and $k \equiv b \bmod f$. Then $s(c)|s(n)$, but $s(c) \nmid k$, i.e. $s(n) \nmid k$. Thus $a(n,k) = 0$ by Lemma 1.

Therefore we obtain in this case $\{a(n,k) \,|\, n \equiv a \bmod d, k \equiv b \bmod f, n \geq 1, k \geq 0\} = \{0\}$, as desired.

□

Corollary 1. *We have*

$$\{c(n,k) \,|\, n \equiv a \bmod d, k \equiv b \bmod f, n \geq 1, k \geq 0\} = \begin{cases} \mathbb{Z} & \text{if } (s((a,d)), f)| \, b \text{ ;} \\ \{0\} & \text{otherwise} . \end{cases}$$

The corollary follows easily from Theorem 1 by using Lemma 2 with a prime $p \equiv 1 \bmod d$.

Lemma 1 implies in addition that each value in the set $\{a(n,k) \,|\, n \equiv a \bmod d, k \equiv b \bmod f, n \geq 1, k \geq 0\}$ is assumed by infinitely many different pairs (n,k).

Acknowledgements

This paper was written during a two month internship at the Max-Planck-Institute for Mathematics in Bonn. I would like to thank the MPIM for its hospitality and nice research atmosphere. In particular, I am grateful to my internship supervisor Pieter Moree for his many helpful comments and suggestions on this paper. Finally, I would like to thank Kestutis Cesnavicius, Nathan Kaplan and Anton Mellit for comments on earlier versions.

References

[1] Yves Gallot, Pieter Moree and Huib Hommersom, Value distribution of coefficients of cyclotomic polynomials, *Unif. Distrib. Theory*, to appear.

[2] Chun-Gang Ji, Wei-Ping Li, Pieter Moree, Values of coefficients of cyclotomic polynomials II, *Discrete Math.* **309** (2009), 1720–1723.

[3] Emma Lehmer, On the magnitude of the coefficients of the cyclotomic polynomial, *Bull. Amer. Math. Soc*, 42, 389-392 (1936)

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

[5] Jiro Suzuki, On coefficients of cyclotomic polynomials, *Proc. Japan Acad. Ser. A Math. Sci.* 63 (1987) 279-280.

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

Jacobs University Bremen, College Ring 3, Mailbox 341, 28759 Bremen, Germany
E-mail address: J.Fintzen@Jacobs-University.de