COEFFICIENTS OF UNITARY CYCLOTOMIC POLYNOMIALS OF ORDER THREE

Gennady Bachman
Department of Mathematical Sciences, University of Nevada Las Vegas, Las Vegas, Nevada
bachman@unlv.nevada.edu

Received: 1/10/22, Accepted: 8/3/22, Published: 8/24/22

Abstract

A unitary cyclotomic polynomial of order three is a polynomial of the form

$$\Phi^*_{PQR}(x) = \frac{(x^{PQR}-1)(x^P-1)(x^Q-1)(x^R-1)}{(x^{PQ}-1)(x^{QR}-1)(x^{RP}-1)(x-1)},$$

where P, Q and R are powers of three distinct primes p, q and r. Fixing any such prime triple generates a family of these polynomials corresponding to all possible choices of $P = p^a$, $Q = q^b$ and $R = r^c$. We study the coefficients of polynomials in such a family. In particular, we show that the coefficients of polynomials in every such family cover all of $\mathbb{Z}$.

1. Introduction and Statement of Results

If positive integers $p, q, r > 2$ are relatively prime in pairs, then the quotient

$$Q_{\{p,q,r\}}(x) = \frac{(x^{pqr}-1)(x^p-1)(x^q-1)(x^r-1)}{(x^{pq}-1)(x^{qr}-1)(x^{rp}-1)(x-1)} \tag{1.1}$$

is a so-called ternary inclusion-exclusion polynomial. The principal special case of these polynomials are the ternary cyclotomic polynomials $\Phi_{pqr}(x)$, corresponding to the case where p, q and r are distinct odd primes. In this paper we address exclusively the ternary case, but the reader interested in the general case of inclusion-exclusion polynomials will find their definition and a discussion of some of their basic properties, such as the fact that $Q_{\{p,q,r\}}$ is a polynomial, in [1].

Two recent papers [7] and [10] emphasized another interesting special case of inclusion-exclusion polynomials, namely, what they dubbed the unitary cyclotomic polynomials. In the ternary case, the unitary cyclotomic polynomials are defined as follows. For three prime powers $p^a, q^b, r^c > 2$ (so p, q, r are distinct primes here) put

$$\Phi^*_{p^a q^b r^c}(x) = Q_{\{p^a,q^b,r^c\}}(x).$$

In other words, unitary cyclotomic polynomials of order three are polynomials $Q_{\{P,Q,R\}}$ where P, Q and R are restricted to be prime powers. The use of the term *unitary* is explained by the fact that all the powers of x appearing on the right in the definition (1.1) of $Q_{\{P,Q,R\}}(x) = \Phi^*_{PQR}(x)$ are *unitary divisors* of $n = PQR$.

We will avoid introducing too many letters and will continue to use letters p, q and r in their dual roles—they are simply relatively prime in pairs when used in the notation $Q_{\{p,q,r\}}$, but they are distinct primes when used in the notation $\Phi^*_{p^aq^br^c}$, $P = p^a$, Φ^*_{PQR}, etc. Let $\mathcal{A}_{\{p,q,r\}}$ be the set of coefficients of the polynomial $Q_{\{p,q,r\}}$. Perhaps the most obvious question about the coefficients of unitary cyclotomic polynomials as a distinct class, is what can be said about the family $\mathcal{A}_{\{p^a,q^b,r^c\}}$ generated by a fixed triple of primes p q and r? In particular, Moree and Tóth [10] raised the question of whether the size of coefficients in every such family grows with out a bound? We shall answer this question in the affirmative and prove the following result.

Theorem 1. *Fix an arbitrary triple of primes p, q, and r and consider the family of unitary cyclotomic polynomials $\Phi^*_{p^aq^br^c}$ it generates. For each $\varepsilon > 0$ and all sufficiently large exponents $a \geq a_\varepsilon$, there exist exponents b and c such that*

$$\mathcal{A}_{\{p^a,q^b,r^c\}} \supset \{\, n : |n| \leq (\tfrac{1}{4} - \varepsilon)p^a \,\}. \tag{1.2}$$

Corollary 1. $\bigcup_{a,b,c} \mathcal{A}_{\{p^a,q^b,r^c\}} = \mathbb{Z}$.

Our proof of Theorem 1 can be readily modified to yield the following one-sided version of this theorem.

Theorem 2. *In addition to the conclusion* (1.2) *of Theorem 1, it is also true that each of the two set inclusions*

$$\mathcal{A}_{\{p^a,q^b,r^c\}} \supset \pm\{\, n : -1 \leq n \leq (\tfrac{1}{2} - \varepsilon)p^a \,\}$$

holds for all $a \geq a_\varepsilon$ and suitably chosen exponents b and c.

The required modifications to the proof of Theorem 1 actually make the argument slightly simpler and we will not include the proof here. In addition to these general results, we shall also give a quick proof of the following striking special case in which primes p, q and r cooperate.

Theorem 3. *Let two primes p and q, $p < q$, satisfy the conditions: (i) $p \equiv q \equiv 3$ or $7 \pmod 8$, (ii) $\gcd(p-1, q-1) = 2$, and (iii) q is a primitive root modulo p^2. Suppose further that a third prime r is a primitive root modulo p^2 and q^2. Then for each exponent a, there are exponents b and c such that*

$$\mathcal{A}_{\{p^a,q^b,r^c\}} = \left\{ n : -\frac{p^a - 1}{2} \leq n \leq \frac{p^a + 1}{2} \right\}.$$

The special merit of this result lies in the fact that we know [2, Corollary 3] that the diameter of the set of coefficients of any polynomial $Q_{\{p,q,r\}}$ satisfies the inequality

$$\operatorname{diam} \mathcal{A}_{\{p,q,r\}} \leq \min(p,q,r), \tag{1.3}$$

where by diameter we mean, of course, the difference between the largest and the smallest coefficients. Restating this for the special case of unitary polynomials and using the notation Φ^*_{PQR}, we see that $\operatorname{diam} \mathcal{A}_{\{P,Q,R\}} \leq P$, and that for unitary families covered by Theorem 3 this holds with equality for every choice of prime power P and suitably chosen prime powers Q and R. It should be mentioned that we take the liberty of restating some of the earlier results on cyclotomic polynomials, such as (1.3), as valid for the entire class of inclusion-exclusion polynomials if the arguments used to prove them carry over to this larger class. We shall continue this practice below without drawing reader's attention to this distinction.

Even though the hypotheses of Theorem 3 are rather technical, they amount to imposing certain arithmetic progression requirements on the primes in question, and the result is certainly non vacuous. Indeed, to give a prime triple fulfilling these requirements we would first select a prime $p \equiv 3$ or $7 \pmod 8$. This choice yields three requirements for our second prime q, the first of which $q \equiv p \pmod 8$ requires no comment. The second requirement is equivalent to $(q-1, \frac{p-1}{2}) = 1$ and is certainly satisfied by taking $q \equiv 2 \pmod{\frac{p-1}{2}}$. (Note that this requirement is vacuous for $p = 3$.) The final requirement is that $q \equiv g \pmod{p^2}$, where g is any primitive root mod p^2. It is well known (see, for example, [11, Theorem 2.39]) that there are $(p-1)\varphi(p-1)$ primitive roots mod p^2, where $\varphi(n)$ is the Euler's totient function, and we may fix any particular one of them in this congruence. So we see that to choose prime q we must choose it satisfying three congruences to the three moduli 8, $\frac{p-1}{2}$ (which is odd) and p^2. By the Chinese remainder theorem and Dirichlet's theorem for primes in arithmetic progressions (see, for example [5]), this can always be accomplished. Analogous considerations yield two congruences $r \equiv g_1 \pmod{p^2}$ and $r \equiv g_2 \pmod{q^2}$ to be satisfied by the third prime r, where g_i are primitive roots to the corresponding moduli. We can always make such selection, by another appeal to the Dirichlet's theorem for primes in arithmetic progressions.

As the "smallest" example of such a triple, we start by taking $p = 3$. 2 is a primitive root mod 3^2, and $q = 11$ satisfies the congruences $q \equiv 3 \pmod 8$ and $q \equiv 2 \pmod{3^2}$. Conveniently, 2 is also a primitive root mod 11^2 and we may take $r = 2$ as our third prime yielding the triple $(p,q,r) = (3,11,2)$. If one wishes instead to complete this construction by choosing an odd prime r, one can do so by taking $r = 29$, since 29 is also a primitive root mod 11^2 and $29 \equiv 2 \pmod{3^2}$. It is interesting to note that these examples give us an easy way to illuminate the fact that the behaviour of the coefficients of ternary inclusion-exclusion (cyclotomic) polynomials is rather nontrivial. Indeed, as a corollary of Theorem 3 and a result due to Kaplan [8] (see also [4]) we give the following example.

Example. Consider the family of unitary polynomials $\Phi^*_{3^a 11^b 2^c}$. For every pair of exponents a and b we can take c such that $2^c \equiv 1 \pmod{3^a 11^b}$, and for every such triple a, b, c we have

$$\mathcal{A}_{\{3^a, 11^b, 2^c\}} = \{-1, 0, 1\}.$$

On the other hand, for each a we can choose b and c so that

$$\mathcal{A}_{\{3^a, 11^b, 2^c\}} = \{\, n : -\frac{3^a - 1}{2} \le n \le \frac{3^a + 1}{2} \,\}.$$

Replacing 2^c with 29^c yields the same conclusions.

In the next section we give a proof of Theorem 3 which easily reduces to a known result on inclusion-exclusion polynomials. In the remainder of the paper we give a proof of Theorem 1 which requires a considerably greater effort.

2. The Case of Cooperating Primes

Our proof of Theorem 3 rests on Proposition 1 below. This is an assertion about inclusion-exclusion polynomials and the reader will recall that the letters p, q and r here need not be prime. The proposition may be viewed as half of the result proved by this author in [3, Section 3].

Proposition 1 ([3])**.** *Assume that $p < q, r$, that p and q are odd, and that*

$$q \equiv 2 \pmod{p}, \quad r \equiv \frac{pq - 1}{2} \pmod{pq}.$$

Then the set of coefficients of $Q_{\{p,q,r\}}$ is

$$\mathcal{A}_{\{p,q,r\}} = \left\{ n : -\frac{p-1}{2} \le n \le \frac{p+1}{2} \right\}.$$

Proof of Theorem 3. Fix an arbitrary power $P = p^a$. Since q is a primitive root modulo p^2, it is also a primitive root modulo P, see, for example, [11, Theorem 2.40]. This allows us to choose another power $Q = q^b$ such that $Q \equiv 2 \pmod{P}$, where b is determined modulo $\varphi(P)$. Similarly, our assumption on r guarantees that the congruences

$$r^i \equiv \frac{P-1}{2} \pmod{P} \quad \text{and} \quad r^j \equiv \frac{Q-1}{2} \pmod{Q} \tag{2.1}$$

have solutions $i \pmod{\varphi(P)}$ and $j \pmod{\varphi(Q)}$. Observe that if we can solve simultaneous congruences

$$c \equiv i \pmod{\varphi(P)} \quad \text{and} \quad c \equiv j \pmod{\varphi(Q)} \tag{2.2}$$

for c, then the triple of powers P, Q and $R = r^c$ $(> P)$ satisfies the requirements of Proposition 1, since the congruences

$$R \equiv \frac{P-1}{2} \pmod{P} \quad \text{and} \quad R \equiv \frac{Q-1}{2} \pmod{Q}$$

are equivalent to the single congruence $R \equiv \frac{PQ-1}{2} \pmod{PQ}$. We can then apply Proposition 1 to the polynomial $Q_{\{P,Q,R\}}$ to reach the desired conclusion. Thus it only remains to solve (2.2).

The obstruction to solving (2.2) is that $\varphi(P)$ and $\varphi(Q)$ are not coprime. In fact

$$\gcd(\varphi(P), \varphi(Q)) = \gcd(p-1, q-1) = 2,$$

by our hypothesis. It follows that (2.2) is soluble if and only if i and j have the same parity. Observe that by (2.1), $r^{\varphi(P)-i} \equiv -2 \pmod{P}$, where we assume, as we may, that $i < \varphi(P)$. This shows that $2 \mid i$ if and only if -2 is a quadratic residue modulo P, whence modulo p. Using the well-known evaluation of the Legendre symbol $\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}}$ [11, Theorems 3.1 and 3.3], we conclude that, for $p \equiv 3$ or $7 \pmod 8$, i is even if $p \equiv 3 \pmod 8$ and odd if $p \equiv 7 \pmod 8$. Of course, exactly the same analysis applies to the exponent j, and since $p \equiv q \pmod 8$ we see that indeed i and j must be of the same parity. This completes the proof of the theorem. □

3. General Case: Preliminaries

In this section we prepare background material on inclusion-exclusion polynomials we will need for the proof of Theorem 1. We begin by introducing some basic notation. It is convenient to put $\tau = \{p, q, r\}$ and to write Q_τ in place of $Q_{\{p,q,r\}}$. It is easy to see ([1]) that the degree of Q_τ is given by

$$\varphi(\tau) \coloneqq (p-1)(q-1)(r-1)$$

and we write

$$Q_\tau(x) = \sum_{m=0}^{\varphi(\tau)} a_m x^m \qquad [a_m = a_m(\tau)].$$

It readily follows from the definition (1.1) that (see [1, (3.8)])

$$\begin{aligned} Q_\tau(x) \equiv (1 - x^q - x^r + x^{q+r})(1 + x + x^2 + \cdots + x^{p-1}) \\ \times \sum_{0 \le i < p} x^{iqr} \sum_{0 \le j < q} x^{jpr} \sum_{0 \le k < r} x^{kpq} \pmod{x^{\varphi(\tau)+1}}, \end{aligned} \tag{3.1}$$

and from this representation it is evident that the key to this problem is understanding the nonnegative linear combinations of qr, pr and pq. Observe that each integer n has a unique representation in the form

$$n = x_n qr + y_n pr + z_n pq + \delta_n pqr, \tag{3.2}$$

with $0 \le x_n < p$, $0 \le y_n < q$, $0 \le z_n < r$, and $\delta_n \in \mathbb{Z}$, so that $n \mapsto (x_n, y_n, z_n, \delta_n)$ is well defined. Furthermore, we have

$$x_n \equiv x_1 n \pmod{p}, \quad y_n \equiv y_1 n \pmod{q}, \quad z_n \equiv z_1 n \pmod{r}. \tag{3.3}$$

Observe further that for $n \le \varphi(\tau)$, we have $\delta_n \le 0$. Thus for the application in (3.1) we are interested in n with $\delta_n = 0$ and we let $\chi(n)$ be the characteristic function of such integers, that is,

$$\chi(n) = \begin{cases} 1, & \text{if } \delta_n = 0 \\ 0, & \text{otherwise.} \end{cases}$$

Using this function in (3.1) we express the coefficients of Q_τ as follows.

Lemma 1 ([3], Lemma 1)**.** *Put $S(m) = \sum_{m-p<n\le m} \chi(n)$. Then we have*

$$a_m = S(m) - S(m-q) - S(m-r) + S(m-q-r).$$

Next we introduce the main tool of this section, the arithmetic function

$$f(n) = x_n q + y_n p, \tag{3.4}$$

based on the representation (3.2). With the aid of this function we can give the following useful characterization of the function χ.

Lemma 2 ([3])**.** *If $n \le \varphi(\tau)$, then $\chi(n) = 1$ if and only if $f(n) \le \lfloor n/r \rfloor$.*

Proof. This is equivalent to Lemma 2 in [3]. □

To work with the function f, we will find it convenient to introduce some additional notation. First, we put $u = x_1$, $v = y_1$ and $w = z_1$, so that

$$1 = uqr + vpr + wpq + \delta_1 pqr.$$

Second, we shall write $\langle n \rangle_p$ and $\langle n \rangle_q$ for the least nonnegative residues of $n \pmod{p}$ and $\pmod{q}$, respectively. Using this notation we may rewrite the first two congruences in (3.3) as equations

$$x_n = \langle un \rangle_p \quad \text{and} \quad y_n = \langle vn \rangle_q, \tag{3.5}$$

and (3.4) becomes

$$f(n) = \langle un \rangle_p q + \langle vn \rangle_q p. \tag{3.6}$$

In addition to this helpful notation it also helps to keep in mind that

$$f(n) \equiv nr^* \pmod{pq}, \tag{3.7}$$

where r^* is the multiplicative inverse of $r \pmod{pq}$.

The chief goal of this section is to prove the following proposition.

Proposition 2. *Let $\tau = \{p, q, r\}$ be a triple of coprime integers with the smallest element p. Put*

$$\mu = \min(x_q, x_r, p - x_q, p - x_r) \quad \textit{and set} \quad C = \lfloor \mu/u \rfloor . \tag{3.8}$$

Assume that $u \le \mu$ (so that $C \ge 1$), and that another element of τ, say q, satisfies

$$q > p^2 \quad \textit{and} \quad v > q - q/p^2. \tag{3.9}$$

Then $\mathcal{A}_\tau \supset \{\, n : |n| \le C \,\}$.

Proof. We know ([6], [1]) that the set of coefficients of Q_τ is just a string of consecutive integers, that is

$$\mathcal{A}_\tau = \{\, n : A^-(\tau) \le n \le A^+(\tau) \,\},$$

where $A^\pm(\tau)$ denotes the largest/smallest coefficients. Whence the claim of the proposition will follow if we simply exhibit a large coefficient $a_m \ge C$ and a small coefficient $a_m \le -C$. This is what we do below.

Considering (3.2) with $n = 1, q, r$ modulo p gives (recall $u = x_1$)

$$uqr \equiv 1, \quad x_q r \equiv 1, \quad x_r q \equiv 1 \pmod{p}, \tag{3.10}$$

and doing the same modulo q gives

$$vpr \equiv 1, \quad y_p r \equiv 1, \quad y_r p \equiv 1 \pmod{q}. \tag{3.11}$$

We see that $u \equiv x_q x_r \pmod{p}$ and $v \equiv y_p y_r \pmod{q}$, or

$$u = \langle x_q x_r \rangle_p \quad \text{and} \quad v = \langle y_p y_r \rangle_q. \tag{3.12}$$

Let us also note the equations

$$x_r q + y_r p = pq + 1 \quad \text{and} \quad x_{-r} q + y_{-r} p = pq - 1, \tag{3.13}$$

which follow from (3.2) with $n = \pm r$, as well as $x_{-r} = p - x_r$ and $y_{-r} = q - y_r$. Of course, there are the corresponding equations involving the parameters x_q and $x_{-q} = p - x_q$, but they will not play any role in our argument. But all four parameters x_q, x_{-q}, x_r, x_{-r} do. In the first place, μ is defined to be the minimum of these parameters (3.8). Furthermore, at this stage we want to identify the smaller

of the two for each pair $x_{\pm q}$ and $x_{\pm r}$. We let q' denote the coice of $\pm q$ corresponding to $x_{q'} < x_{-q'}$ ($\neq$ by (3.10)) and do the same with $\pm r$: $r' = \pm r$ with $x_{r'} < x_{-r'}$. Note that

$$x_{q'}, x_{r'} < p/2 \quad \text{and} \quad \mu = \min(x_{q'}, x_{r'}). \tag{3.14}$$

Next, set

$$a = (C-1)u \quad \text{and} \quad \ell = aqr. \tag{3.15}$$

Since

$$a < Cu \leq \mu < p/2, \tag{3.16}$$

note that $x_\ell = a$ and $f(\ell) = aq$. We now show that

$$\chi(\ell - i) = 1, \quad \text{for } 0 \leq i \leq C-1, \text{ and} \tag{3.17}$$
$$\chi(\ell + i) = 0, \quad \text{for } 0 < i < p. \tag{3.18}$$

By Lemma 2 and (3.7), (3.17) is equivalent to $f(\ell - i) \leq aq$. By (3.5) and (3.6), we have

$$f(\ell - i) = \langle a - ui \rangle_p q + \langle -vi \rangle_q p = \langle a - ui \rangle_p q + \langle v'i \rangle_q p,$$

where

$$v' = q - v < q/p^2, \tag{3.19}$$

by (3.9). Whence

$$f(\ell - i) = (a - ui)q + v'ip = aq - i(uq - v'p) \leq aq,$$

implying (3.17). We handle (3.18) in a similar fashion:

$$\begin{aligned} f(\ell + i) &= \langle a + ui \rangle_p q + \langle vi \rangle_q p \geq \langle vi \rangle_q p \\ &= (q - iv')p > pq - q > aq, \end{aligned}$$

and (3.18) follows by Lemma 2.

Our next step is to show that

$$\chi(\ell - r' + i) = 0, \quad \text{for } -C < i < p. \tag{3.20}$$

Since $\left\lfloor \frac{\ell - r' + i}{r} \right\rfloor \leq aq - r'/r$, this equality follows from the inequality $f(\ell - r' + i) > aq - \frac{r'}{r}$, by Lemma 2. In the range $-C < i \leq 0$, we obtain

$$\begin{aligned} f(\ell - r' + i) &\geq \langle a - r'u + ui \rangle_p q = \langle a - x_{r'} + ui \rangle_p q \\ &= (p - x_{r'} + a + ui)q \geq (p - x_{r'})q \\ &\geq (x_{r'} + 1)q > (a+1)q, \end{aligned}$$

by (3.5), (3.6), (3.14) and (3.16). In the remaining range,

$$\begin{aligned} f(\ell - r' + i) &\geq \langle -r'v + iv \rangle_q p = \langle -y_{r'} - iv' \rangle_q p \\ &> (q - y_{r'} - pv')p > pq - y_{r'}p - q, \end{aligned}$$

by (3.5), (3.6) and (3.19). Combining this with (3.13) yields

$$f(\ell - r' + i) > x_{r'}q - r'/r - q \geq aq - r'/r,$$

by (3.14) and (3.16), completing the verification of (3.20).

In addition to (3.20) we will also need

$$\chi(\ell + r' + i) = 0, \quad \text{for } -C < i < p. \tag{3.21}$$

The verification here is nearly identical and slightly simpler. Since $\left\lfloor \frac{\ell + r' + i}{r} \right\rfloor \leq aq+1$, we only need to show that $f(\ell + r' + i) > aq + 1$. In the range $-C < i \leq 0$, we get

$$\begin{aligned} f(\ell + r' + i) &\geq \langle a + x_{r'} + ui \rangle_p q = (x_{r'} + a + ui)q \\ &\geq x_{r'}q \geq (a+1)q, \end{aligned}$$

and in the remaining range,

$$\begin{aligned} f(\ell + r' + i) &\geq \langle y_{r'} + vi \rangle_q p = (y_{r'} - v'i)p \geq y_{r'}p - q + 1 \\ &= pq - x_{r'}q + r'/r - q + 1 \geq (p - x_{r'} - 1)q \geq x_{r'}q \geq (a+1)q, \end{aligned}$$

as desired.

Our final step in this calculation is an analogue of (3.20) and (3.21),

$$\chi(\ell - q' + i) = 0, \quad \text{for } -C < i < p, \tag{3.22}$$

which we prove in exactly the same manner. Since

$$\left\lfloor \frac{\ell - q' + i}{r} \right\rfloor \leq aq + \left\lfloor \frac{q+p}{r} \right\rfloor < aq + q,$$

(3.22) follows from $f(\ell - q' + i) \geq aq + q$. For $-C < i \leq 0$, we get

$$\begin{aligned} f(\ell - q' + i) &\geq \langle a - q'u + iu \rangle_p q = \langle a - x_{q'} + iu \rangle_p q \\ &= (p - x_{q'} + a + iu)q \geq (p - x_{q'})q \\ &\geq (x_{q'} + 1)q > (a+1)q, \end{aligned}$$

and for $0 \leq i < p$, we get

$$\begin{aligned} f(\ell - q' + i) &\geq \langle vi \rangle_q p = (q - v'i)p > pq - q \\ &\geq (a+1)q + (p - 1 - \mu)q > (a+1)q, \end{aligned}$$

as required.

We are now ready to exhibit large/small coefficients of Q_τ. Put $m = \ell + p - C$ and observe that (3.17) and (3.18) imply that

$$S(m) = \sum_{m-p<n\le m} \chi(n) = \sum_{-C<i\le p-C} \chi(\ell + i) = C,$$

while (3.20)-(3.22) imply that

$$S(m \pm r) = S(m - q') = 0.$$

Therefore

$$S(m) - S(m - q') - S(m \pm r) + S(m - q' \pm r) \ge C. \tag{3.23}$$

Now, if $q' = q$ then, by Lemma 1, the left side in (3.23) with the choice $-r$ equals to a_m, and with the choice $+r$ equals to $-a_{m+r}$. And if $q' = -q$, then the two choices $\mp r$ correspond to the coefficients $-a_{m+q}$ and a_{m+q+r}, respectively. This completes the proof of the proposition. □

4. Proof of Theorem 1

The following heuristic guides what one might expect from an arbitrary family of polynomials $\Phi^*_{p^a q^b r^c}$. Let h be the multiplicative order of q modulo p, so $h \mid p - 1$. There is the largest exponent a_0 such that h is the order of q modulo p^{a_0}. For all $a \ge a_0$, the order of q modulo p^a is $p^{a-a_0}h$. Therefore, for $P = p^a$ with $a \ge a_0$, there are $c \cdot P$ distinct residues q^i modulo P, where the constant c depends only on q. Similarly, there are $c' \cdot P$ distinct residues of r^j modulo P. One might expect that if P is sufficiently large, powers q^i and r^j cover the reduced residue system modulo P sufficiently well. Fixing a particular power $Q = q^b$, one also expects r^j to cover the reduced residue system modulo Q pretty well. This suggests that as exponents b and c vary, sets of coefficients of polynomials Φ^*_{PQR} resemble those of "typical" $Q_{\{P,\cdot,\cdot\}}$.

The snag in this heuristic is the question of distribution of exponential residues, such as $q^i \pmod P$. Our chief objective in Proposition 2 was to get a sufficiently flexible result on polynomials Q_τ to be able to cover our problem for polynomials $\Phi^*_{p^a q^b r^c}$, given what is known about such exponential congruences. More specifically, the key result on exponential congruences we will use to complete our argument is given in Lemma 3 below. This lemma is only a special case of a result proved by Korobov [9, Theorem 3]. The reader is also referred to Shparlinski's paper [12] for a convenient reference to this result. In particular, our formulation of Lemma 3 follows the exposition in [12].

Lemma 3. *Let a prime number p and integers a and g relatively prime to p be fixed. For an arbitrary integer b and a positive integers N and ν, let $T(b, N; \nu)$ denote the number of integers $n \in [b+1, b+N]$ such that $n \equiv a \cdot g^i \pmod{p^\nu}$ for some i. Now fix a real $\frac{1}{2} < \theta < 1$ and restrict N to be of size $p^{\theta \cdot \nu} < N < p^\nu$. Then for all b and N, we have*

$$T(b, N; \nu) \sim c(p, g) \cdot N,$$

as $\nu \to \infty$, where the constant $c(p, g)$ depends only on p and g.

Next we use Lemma 3 to gain desired control of simultaneous residues $\langle q^i \rangle_P$, $\langle r^j \rangle_P$ and $\langle q^i r^j \rangle_P$. Of course, the notation $\langle \cdot \rangle_P$ follows the meaning established in Section 3.

Lemma 4. *Let $0 < \varepsilon < 1/4$ be fixed. Then for all sufficiently large powers $P = p^a$ we can find exponents i and j such that $\langle q^i r^j \rangle_P = 1$, while*

$$\min\big(\langle q^i \rangle_P, P - \langle q^i \rangle_P, \langle r^j \rangle_P, P - \langle r^j \rangle_P\big) > (\tfrac{1}{4} - \varepsilon)P.$$

Proof. Let $P = p^a$ be an arbitrary but fixed power of p. Let us express the multiplicative orders of q and r modulo p in the form $\varphi(P)/\alpha$, $\varphi(P)/\beta$, respectively. Fix a primitive root g modulo P. Then

$$q \equiv g^{\alpha s}, \ r \equiv g^{\beta t} \pmod{P},$$

for some s and t with $(s, \varphi(P)/\alpha) = (t, \varphi(P)/\beta) = 1$. So considering the set of distinct residues $\{q^i \pmod P\}$, $\{r^j \pmod P\}$ and $\{q^i r^j \pmod P\}$ comes to the same thing as considering $\{g^{\alpha i} \pmod P\}$, $\{g^{\beta j} \pmod P\}$ and $\{g^{\alpha i} g^{\beta j} \pmod P\}$, respectively. Furthermore, one readily verifies that the first requirement in the statement of the lemma, $g^{\alpha i} \cdot g^{\beta j} \equiv 1 \pmod P$, reduces to the requirement

$$g^{[\alpha,\beta]i} \cdot g^{[\alpha,\beta]j} \equiv 1 \pmod{P}, \tag{4.1}$$

where $[\alpha, \beta] = \operatorname{lcm}(\alpha, \beta)$. But the list of all possible solutions of (4.1) corresponds to letting i run through the range $0 \le i < \varphi(P)/[\alpha, \beta]$ and taking $j = \frac{\varphi(P)}{[\alpha,\beta]} - i$. Therefore, to complete the proof of the lemma we must show that we can choose i such that all four quantities

$$\langle \pm g^{\pm[\alpha,\beta]i} \rangle_P > (\tfrac{1}{4} - \varepsilon)P.$$

(Note that we use the notation $x^{-1} \pmod P$ to denote the multiplicative inverse of x.)

In other words, we wish to show that there is i such that

$$\langle g^{\pm[\alpha,\beta]i} \rangle_P \in \mathcal{J}, \tag{4.2}$$

where $\mathcal{J} = \big((\frac{1}{4} - \varepsilon)P, (\frac{3}{4} + \varepsilon)P\big)$. By Lemma 3,

$$\#\{\langle g^{[\alpha,\beta]i}\rangle_P \in \mathcal{J}\} \sim c(p, qr) \cdot (\tfrac{1}{2} + 2\varepsilon)P, \tag{4.3}$$

as $P \to \infty$, where the constant $c(p, qr)$ depends only on p, q and r. Another application of Lemma 3 gives

$$\#\{\langle g^{-[\alpha,\beta]i}\rangle_P \notin \mathcal{J}\} \sim c(p, qr) \cdot (\tfrac{1}{2} - 2\varepsilon)P, \tag{4.4}$$

as $P \to \infty$. Combining (4.3) and (4.4) shows that if $P = p^a$ is sufficiently large, then (4.2) must hold for some i, completing the proof of the lemma. □

Proof of Theorem 1. Fix $\varepsilon \in (0, 1/4)$ and a sufficiently large power $P = p^a$, so that Lemma 4 applies. Fix a pair of exponents $i = i_1$ and $j = j_1$ satisfying the conclusions of Lemma 4. Now fix a power of q: $Q = q^{k_1\varphi(P)-i_1}$, where k_1 is an arbitrary but fixed integer and $Q > P^6$. At this stage we are not quite ready to fix R, but it will be of the form

$$R = r^{k\varphi(P)-j_1}, \tag{4.5}$$

for some k to be selected.

In preparation for application of Proposition 2 to the polynomial $\Phi^*_{PQR} = Q_{\{P,Q,R\}}$, recall the terminology introduced in Section 3. In particular, in view of

$$Q \cdot q^{i_1} \equiv 1 \equiv R \cdot r^{j_1} \pmod{P},$$

we see that

$$x_R = \langle q^{i_1}\rangle_P, \quad x_Q = \langle r^{j_1}\rangle_P \quad \text{and} \quad u = \langle q^{i_1} \cdot r^{j_1}\rangle_P = 1.$$

Therefore the quantity C defined in (3.8) satisfies

$$C = \min\big(\langle \pm q^{i_1}\rangle_P, \langle \pm r^{j_1}\rangle_P\big) > (\tfrac{1}{4} - \varepsilon)P,$$

by Lemma 4. The theorem now follows from Proposition 2 provided we make additional arrangements to fulfill the condition (3.9).

Recall that $v = \langle y_P \cdot y_R\rangle_Q$ and that, since we already fixed P and Q, y_R is already determined and satisfies the congruence $P \cdot y_R \equiv 1 \pmod{Q}$. Recall also that $Q > P^6$, whence the interval $\mathcal{J}' = (Q - Q/P^2, Q)$ is of length $> Q^{2/3}$. Now let

$$d = \gcd(\varphi(P), \varphi(Q)) = \gcd(p - 1, q - 1), \tag{4.6}$$

and consider the solubility in the variable t of the congruence

$$\langle y_R \cdot r^{j_1} \cdot r^{dt}\rangle_Q \in \mathcal{J}'. \tag{4.7}$$

Assuming that Q is sufficiently large (i.e., k_1 is large enough), another application of Lemma 3 (with $a = y_R r^{j_1}$ and $g = r^d$) shows that solutions exist. So let us fix one particular solution $t = t_2$. By (4.6), the congruence

$$k\varphi(P) + dt_2 \equiv 0 \pmod{\varphi(Q)}$$

is also soluble and we fix a particular solution $k = k_2 > 0$. With all this to hand we now fix $R = r^{k_2\varphi(P)-j_1}$. Put $j_2 = j_1 + dt_2$ and observe that $R \cdot r^{j_2} \equiv 1 \pmod{Q}$. Whence $y_p = \langle r^{j_2} \rangle_Q$ and, by (4.7), $v = \langle y_R y_P \rangle_Q$ satisfies (3.9), as required. □

References

[1] G. Bachman, On ternary inclusion-exclusion polynomials, *Integers* **10** (2010), 623–638.

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

[3] G. Bachman, Ternary cyclotomic polynomials with an optimally large set of coefficients, *Proc. Amer. Math. Soc.* **132** (2004), no. 7, 1943–1950.

[4] G. Bachman and P. Moree, On a class of ternary inclusion-exclusion polynomials, *Integers* **11** (2011), 77–91.

[5] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Springer-Verlag, New York, 1980.

[6] Y. Gallot and P. Moree, Neighboring ternary cyclotomic coefficients differ by at most one, *J. Ramanujan Math. Soc.* **24** (2009), no. 3, 235-248.

[7] G. Jones, P. Kester, L. Martirosyan, P. Moree, L. Tóth, B. White, B. Zhang, Coefficients of (inverse) unitary cyclotomic polynomials, *Kodai Math. J.* **43** (2020), 325–338.

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

[9] N. M. Korobov, On the distribution of digits in periodic fractions, *Mat. Sb.* **89** (1972), no. 4, 654–670.

[10] P. Moree and L. Tóth, Unitary cyclotomic polynomials, *Integers* **20** (2020), #A65.

[11] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., Wiley, New York, 1991.

[12] I. E. Shparlinski, Distribution of exponential functions modulo a prime power, *J. Number Theory* **143** (2014), 224–231.