A NOTE ON POLYNOMIAL SEQUENCES MODULO INTEGERS

MOHAMMAD JAVAHERI

Abstract. We study the uniform distribution of the polynomial sequence \( \lambda(P) = \{\lfloor P(k) \rfloor \mod \text{integers} \} \) mod integers, where \( P(x) \) is a polynomial with real coefficients. In the nonlinear case, we show that \( \lambda(P) \) is uniformly distributed in \( \mathbb{Z} \) if and only if \( P(x) \) has at least one irrational coefficient other than the constant term. In the case of even degree, we prove a stronger result: \( \lambda(P) \) intersects every congruence class mod every integer if and only if \( P(x) \) has at least one irrational coefficient other than the constant term.

1. Introduction

A sequence \( \{r_k\}_{k=1}^{\infty} \) of real numbers is said to be uniformly distributed (u.d.) mod 1, if for all \( 0 \leq a < b < 1 \),
\[
\lim_{N \to \infty} \frac{1}{N} \# \left\{ k \in \{1, \ldots, N\} : a \leq \{r_k\} \leq b \right\} = b - a,
\]
where \( \{r_k\} \) denotes the fractional part of \( r_k \). An integer sequence \( \{a_k\}_{k=1}^{\infty} \) is said to be u.d. mod an integer \( m \geq 2 \), if for every integer \( i \), one has
\[
\lim_{N \to \infty} \frac{1}{N} \# \left\{ k \in \{1, \ldots, N\} : a_k = i \pmod{m} \right\} = \frac{1}{m}.
\]
A sequence is called u.d. in \( \mathbb{Z} \) if it is u.d. mod \( m \) for all \( m \geq 2 \) (or equivalently for all \( m \) large enough). Given a sequence \( \{r_k\}_{k=1}^{\infty} \) of real numbers, if \( \{r_k/m\}_{k=1}^{\infty} \) is u.d. mod 1 for every \( m \geq 2 \), then \( \{\lfloor r_k \rfloor\}_{k=1}^{\infty} \) is u.d. in \( \mathbb{Z} \); see theorems 1.4 and 1.6 of [4, Ch. 5]. Therefore, one can derive the following results on u.d. sequences in \( \mathbb{Z} \) using existing results on u.d. sequences mod 1.

Example 1. If \( P(x) = \sum_{i=0}^{n} a_i x^i \) is a real polynomial with at least one irrational coefficient other than \( a_0 \), then \( \{\lfloor P(k) \rfloor \}_{k=1}^{\infty} \) is u.d. in \( \mathbb{Z} \); [4].

2010 Mathematics Subject Classification. 11K36.

Key words and phrases. Uniform distribution, Polynomial sequences.
This follows from the generalization of Weyl’s distribution theorem proved by Weyl himself via his differencing method. Weyl’s result was a generalization of Hardy and Littlewood’s result on monomials; \[2\]. We prove the converse of this statement for nonlinear polynomials in Theorem 10.

Example 2. If \(f(x) = \beta x^\alpha\), where \(\alpha \in (1, \infty) \setminus \mathbb{N}\) and \(\beta \in (0, 1]\), then \(\{\lfloor f(k) \rfloor\}_{k=1}^\infty\) is u.d. in \(\mathbb{Z}\). This follows from Weyl’s criterion together with van der Corput inequalities. Alternatively, see theorem 3.5 in \[4, \text{Ch. 1}\].

Example 3. If \(P(x) = \pm x + c\), \(c \in \mathbb{R}\), then \(\{\lfloor P(k) \rfloor\}_{k=1}^\infty\) is clearly u.d. in \(\mathbb{Z}\). Moreover, if \(P(x) = P(0) \in \mathbb{Z}[x]\) and \(\{\lfloor P(k) \rfloor\}_{k=1}^\infty\) is u.d. in \(\mathbb{Z}\), then \(P(x) = \pm x + c\) for some \(c \in \mathbb{R}\); \[8\].

Example 4. If \(f(x) = \beta \alpha x\) and \(\beta > 0\), then for almost all \(\alpha > 1\), the sequence \(\{\lfloor f(k) \rfloor\}_{k=1}^\infty\) is u.d. in \(\mathbb{Z}\). This follows from Koksma’s theorem; see also \[3\].

Niven showed in \[8\] that given a nonlinear polynomial \(P(x) \in \mathbb{Z}[x]\), there exist infinitely many primes \(p\) such that \(\{P(k)\}_{k=1}^\infty\) is not u.d. modulo \(p\). In this paper, our first goal is to extend this result to polynomials with rational coefficients in the following theorem.

**Theorem 5.** Let \(P(x)\) be a polynomial with real coefficients. If the sequence \(\{\lfloor P(k) \rfloor\}_{k=1}^\infty\) is u.d. mod all primes large enough, then either \(P(x)\) has an irrational coefficient other than the constant term or \(P(x) = x/l + P(0)\), where \(l\) is a nonzero integer.

Generalized polynomials are obtained by adding the least integer operation to the arithmetic operations involved in defining polynomials. For example, \(f(x) = \lfloor [a_1 x^2 + a_2]x \rfloor + \lfloor a_3 x + a_4 \rfloor x^2\) is a generalized polynomial. Uniform distribution of generalized polynomials were studied in \[3\], where it was shown that under some conditions relating to the independence of coefficients of \(f(x)\) over the rationals, the sequence \(\{f(k)\}_{k=1}^\infty\) is u.d. mod \(1\). The second goal of this article is to study the range of the simplest generalized polynomials mod integers, namely the range of \(\lfloor P(x) \rfloor\) mod integers, where \(P(x)\) is a real polynomial.

**Definition 6.** We say a polynomial \(P(x) \in \mathbb{R}[x]\) is complete modulo \(m\), if for every integer \(n\), the equation \(\lfloor P(x) \rfloor = n\) (mod \(m\)) has a solution \(x \in \mathbb{Z}\). We say \(P(x)\) is complete in \(\mathbb{Z}\), if it is complete modulo every integer \(m\) (or equivalently modulo all \(m\) large enough).
It follows from Example 11 that if \( P(x) \) has at least one irrational coefficient other than the constant term, then \( P(x) \) is complete in \( \mathbb{Z} \). The converse is not true in degree 1 (compare Theorems 9 and 11). However, we will show in the following theorem that, at least in the even degree case, the converse is true.

**Theorem 7.** Let \( P(x) \) be an even-degree polynomial with real coefficients. If \( P(x) \) is complete mod all primes large enough, then \( P(x) \) has an irrational coefficient other than the constant term.

2. U.D. POLYNOMIAL SEQUENCES

In this section, we determine all polynomials \( P(x) \in \mathbb{R}[x] \) for which the sequence \( \{[P(k)]\}_{k=1}^\infty \) is u.d. in \( \mathbb{Z} \). In [8, Theorem 3.1], Niven showed that the sequence \( \{[\alpha k]\}_{k=1}^\infty \) is u.d. if and only if \( \alpha \) is irrational or \( \alpha = 1/l \) for some nonzero integer \( l \). For a linear polynomial \( P(x) = \alpha x + \beta \), Niven proved that if \( \alpha \) is irrational, then the sequence \( \{[\alpha k + \beta]\}_{k=1}^\infty \) is u.d. in \( \mathbb{Z} \); this also follows form Example 11. However, the converse of this statement was not stated or proved in [8]. For the completion of the study of linear polynomials, we will prove in Theorem 9 that if the sequence \( \{[\alpha k + \beta]\}_{k=1}^\infty \) is u.d. in \( \mathbb{Z} \), then either \( \alpha \) is irrational or \( \alpha = 1/l \) for some nonzero integer \( l \). First, we need a lemma.

**Lemma 8.** Let \( a, b \) be integers such that \( \gcd(a, b) = 1 \) and \( b > 0 \). Let \( \beta \in \mathbb{R} \). Then the sequence \( \{[ak/b + \beta]\}_{k=1}^\infty \) is u.d. mod \( m \) if and only if \( \gcd(a, m) = 1 \).

**Proof.** First, suppose that the sequence \( \{[ak/b + \beta]\}_{k=1}^\infty \) is u.d. mod \( m \). Suppose that \( d = \gcd(a, m) > 1 \), and we derive a contradiction. Since we have assumed that \( \{[ak/b + \beta]\}_{k=1}^\infty \) is u.d. mod \( m \), it follows that the sequence \( \{[ak/b + \beta]\}_{k=1}^\infty \) is u.d. mod \( d \); [8, Theorem 5.1]. One notes that the sequence \( \{[ak/b + \beta]\}_{k=1}^\infty \mod d \) is periodic with period \( b \). Therefore, if the number of solutions of \( [ak/b + \beta] = 0 \mod d \) with \( 1 \leq k \leq b \) is given by \( t \), then the number of solutions of \( [ak/b + \beta] = 0 \mod d \) with \( 1 \leq k \leq sb \) is given by \( st \), and so

\[
\lim_{s \to \infty} \frac{1}{sb} \# \{k \in \{1, \ldots, sb\} : [ak/b + \beta] = 0 \mod d\} = \lim_{s \to \infty} \frac{st}{sb} = \frac{t}{b}.
\]

On the other hand, this limit must equal \( 1/d \) by the definition of u.d. mod \( d \). It follows that \( t/b = 1/d \), and so \( d \mid b \). Since \( d \mid a \) and \( \gcd(a, b) = 1 \), we have a contradiction.
For the converse, suppose that $\gcd(a, m) = 1$. One notes that the sequence $\{[ak/b + \beta]\}_{k=1}^{\infty}$ is periodic mod $m$ with period $bm$. For each $0 \leq i \leq m - 1$, let $T_i$ denote the subset of elements $k \in \{1, \ldots, bm\}$ such that $[ak/b + \beta] = i \mod m$. We show that $|T_i| = b$ for all $0 \leq i \leq m - 1$. Fix $0 \leq i \leq m - 1$, and let $T_i = \{t_1, \ldots, t_r\}$. For each $1 \leq j \leq r$, we have
\[
[a(t_j + b)/b + \beta] = a + [at_j/b + \beta] = a + i \mod m.
\]
In other words, the map $t_j \mapsto t_j + b$ is a one-to-one map from $T_i$ to $T_{i+1}$, where $t_j + b$ is computed modulo $bm$ and $a + i$ is computed modulo $m$. It follows that $|T_{i+1}| \geq |T_i|$, and so $|T_{qa+i}| \geq |T_i|$ for all $q \geq 0$, where $qa + i$ is computed modulo $bm$. Since $\gcd(a, m) = 1$, we conclude that $|T_{i'}| \geq |T_i|$ for all $i', i = 0, \ldots, m - 1$, and so $|T_i| = b$ for all $i = 0, \ldots, m - 1$. Thus, for $N = Qbm + R$, $0 \leq R < bm$, the number of solutions of $[ak/b + \beta] = i \mod m$ is between $Qb$ and $(Q + 1)b$, which is sufficient to verify the definition of u.d. mod $m$ in $[1]$.

**Theorem 9.** The sequence $\{[ak + \beta]\}_{k=1}^{\infty}$ is u.d. in $\mathbb{Z}$ if and only if $\alpha$ is irrational or $\alpha = 1/l$ for some nonzero integer $l$.

**Proof.** If $\alpha$ is irrational, then the claim follows from Example [1] (or see [2] Theorem 3.2). If $\alpha = 1/l$ for some nonzero integer $l$, then the sequence $\{[k/l + \beta]\}_{k=1}^{\infty}$ is u.d. mod $m$ for every $m$ by Lemma [3]. If $\alpha$ is rational but not of the form $1/l$ for some nonzero integer $l$, let $\alpha = a/b$ for integers $a, b$ with $\gcd(a, b) = 1$, $|a| > 1$, and $b > 0$. Then it follows from Lemma [3] that the sequence $\{[ak/b + \beta]\}_{k=1}^{\infty}$ is not u.d. mod $a$, hence it is not u.d. in $\mathbb{Z}$.

Next, we discuss nonlinear polynomials.

**Theorem 10.** Let $P(x)$ be a nonlinear polynomial with real coefficients. If the sequence $\{[P(k)]\}_{k=1}^{\infty}$ is u.d. mod all primes large enough, then $P(x)$ has at least one irrational coefficient other than the constant term.

**Proof.** Suppose on the contrary that $P(x) = \sum_{i=0}^{n} a_i x^i$ such that $a_i = r_i/s_i \in \mathbb{Q}$ with $\gcd(r_i, s_i) = 1$ for all $1 \leq i \leq n$. Let $N$ be the least common multiple of $s_i$, $1 \leq i \leq n$. Since the sequence $\{[P(k)]\}_{k=1}^{\infty}$ is assumed to be u.d. mod all primes large enough, the sequence $\{N[P(k)]\}_{k=1}^{\infty}$ is u.d. mod all primes $p$ large enough. The value $N[P(k)]$ is periodic mod $p$ with period $Np$. Therefore, it follows from the uniform distribution of $\{N[P(k)]\}_{k=1}^{\infty}$ mod $p$ that, with $\mathcal{U} = \{0, \ldots, p - 1\} \times \{0, \ldots, N - 1\}$, we have
A NOTE ON POLYNOMIAL SEQUENCES MODULO INTEGERS

#{(t, j) ∈ U : N[P(Nt + j)] = i (mod p)} = N,
for every integer i. Let $P_j(x) = N[P(Nx + j)] ∈ \mathbb{Z}[x]$ for $0 ≤ j < N$. Choose $M$ large enough so that the polynomials $f_j(x) = P_j(x) + M, 0 ≤ j < N$, are all irreducible over $\mathbb{Q}[x]$ (the existence of $M$ follows from Hilbert's irreducibility theorem [6]). Let $f(x) = f_0(x) \cdots f_{N-1}(x)$ and

$$R = \prod_{0 ≤ i < j < N} \text{Res}(f_i, f_j) ∈ \mathbb{Z},$$

where $\text{Res}(f_i, f_j)$ is the resultant of polynomials $f_i$ and $f_j$. Since $f_i$ and $f_j$ as irreducible polynomials in $\mathbb{Q}[x]$ have no common roots for all $0 ≤ i < j < N$, we must have $\text{Res}(f_i, f_j) ≠ 0$, and so $R ≠ 0$. Therefore, for any prime $p > p_0$, $\text{Res}(f_i, f_j) ≠ 0 (mod p)$, where $p_0$ is the greatest prime factor of $R$. In other words, for any prime $p > p_0$, the polynomials $f_j, 0 ≤ j < N$, have no common roots modulo $p$. By the Chebotarev density theorem, there exist infinitely many primes $p$ such that $f(x)$ splits completely into $nN$ linear factors modulo $p$. It follows that there exists arbitrarily large $p > p_0$ such that $f(x)$ has $nN$ distinct roots modulo $p$. Therefore, the number of solutions of $N[P(Nk + j)] = -M (mod p)$ is at least $nN > N$. This is in contradiction with (2), and the claim follows.

We end this section with a second proof of Theorem [10].

Second proof of Theorem [10] With $N$ as in the previous proof, let $Q(x) = N(P(x) - P(0)) ∈ \mathbb{Z}[x]$. Choose an integer $a$ such that $Q'(a)$ has an arbitrarily large prime factor $p > 6N$ (this can be done, since $Q'(x)$ is a non constant polynomial). We define $f(x) = Q(x) - Q(a)$. Then $f(a) = 0 (mod p^2)$ and $f'(a) = 0 (mod p)$. It follows from Hensel's Lemma that $f(a + mp) = f(a) = 0 (mod p^2)$ for all $m$. In particular, the equation $Q(x) = Q(a)$ has at least $p$ solutions mod $p^2$. It follows that $|T| ≥ sp^2$, where $T ⊆ \{1, \ldots, sp^2\}$ denotes the set of solutions of $Q(x) = Q(a) mod p^2$.

We show that the sequence $\{|P(k)|\}_{k=1}^∞$ is not u.d. mod $p^2$, hence it is not u.d. mod $p$, which proves the claim. On the contrary, suppose that $\{|P(k)|\}_{k=1}^∞$ is u.d. mod $p^2$. It follows from the definition that for each $0 ≤ t < p^2$,

$$\lim_{s→∞} \frac{1}{sp^2} |S_t| = \frac{1}{p^2},$$

(3)
where $S_t$ is the set of $x \in \{1, \ldots, sp^2\}$ such that $[P(x)] = t \pmod{p^2}$. In particular, for $s$ large enough, one has

$$\frac{1}{sp^2}|S_t| \leq \frac{2}{p^2}$$

for all $0 \leq t < p^2$. If $x \in T$, then $Q(x) = Q(a) + \alpha(x) \cdot p^2$ for some $\alpha(x) \in \mathbb{Z}$. It follows that

$$\lfloor P(x) - P(0) \rfloor = \left\lfloor \frac{Q(x)}{N} \right\rfloor = \left\lfloor \frac{Q(a) + \alpha(x) \cdot p^2}{N} \right\rfloor.$$

We note that the values $\left\lfloor \frac{(Q(a) + \beta p^2)/N}{N} \right\rfloor$ and $\left\lfloor \frac{(Q(a) + (\beta + N)p^2)/N}{N} \right\rfloor$ are congruent mod $p^2$, therefore, there are at most $N$ congruence classes mod $p^2$ among the values $[P(x) - P(0)]$, $\beta \in \mathbb{Z}$. Since $|T| \geq sp > 6sN$, it follows that there exists $r$ such that $[P(x) - P(0)] = r \pmod{p^2}$ has more than $6s$ solutions in the set $\{1, \ldots, sp^2\}$. Let $S$ be the set of $x \in T$ such that $[P(x) - P(0)] = r \pmod{p^2}$. In particular $|S| > 6s$.

Since, for every $x \in \mathbb{Z}$, we have $[P(x)] = [P(x) - P(0)] + [P(0)] + u$ for some $u \in \{-1, 0, 1\}$, we must have $S \subseteq S_{t-1} \cup S_0 \cup S_{t1}$, where $t_u = r + [P(0)] + u$ is computed modulo $p^2$. Therefore,

$$\frac{1}{sp^2}|S_{t-1} \cup S_0 \cup S_{t1}| \geq \frac{1}{sp^2}|S| > \frac{6s}{sp^2},$$

which contradicts (4) as $s \to \infty$. \hfill \Box

3. Complete even-degree polynomials

Let $P(x)$ be such that $P(x) - P(0) \in \mathbb{Q}[x]$. Since the sequence $\{[P(k)]\}_{k=1}^{\infty} \pmod{m}$ is periodic, it follows from Definition 5 that the polynomial $P(x)$ is complete mod $m$ if and only if for the sequence $a_k = [P(k)]$, $k \geq 1$, we have

$$\lim_{N \to \infty} \frac{1}{N} \# \{k \in \{1, \ldots, N\} : a_k = i \pmod{m} \} > 0,$$

for every integer $i$. Condition [5] is weaker than condition [1]. Therefore, if $\{[P(k)]\}_{k=1}^{\infty}$ is u.d. modulo $m$, then $P(x)$ is complete modulo $m$. The converse is not true for linear polynomials as shown by the following theorem in comparison with Theorem [9].

**Theorem 11.** The linear polynomial $P(x) = ax + \beta$ is complete in $\mathbb{Z}$ if and only if either $\alpha \in [-1, 0) \cup (0, 1]$ or $\alpha$ is irrational.
Proof. If $\alpha$ is irrational, then the claim follows from Example 1. Thus, suppose $\alpha = a/b$ where $a, b$ are coprime integers, $a \neq 0$, and $b > 0$. Suppose that $P(x)$ is complete in $\mathbb{Z}$, and so the set $\{ \lfloor \alpha k + \beta \rfloor : k \geq 1 \}$ contains the numbers $0, \ldots, |a| - 1$ modulo $|a|$. Let $k = bq + l$ where $0 \leq l < b$. Then
\[
\left\lfloor \frac{a}{b}(bq + l) + \beta \right\rfloor = aq + \left\lfloor \frac{al}{b} + \beta \right\rfloor.
\]
Therefore, the $b$ numbers $\lfloor al/b + \beta \rfloor$, $0 \leq l < b$, must contain the numbers $0, \ldots, |a| - 1$ modulo $|a|$. In particular $b \geq |a|$ and so $\alpha \in [-1, 0) \cup (0, 1]$.

For the converse, suppose $b \geq |a|$. Then the numbers $al/b + \beta$, $0 \leq l < b$ are apart by $|a/b| \leq 1$, and they stretch from $\beta$ to $a + \beta$. Therefore, the numbers $\lfloor al/b + \beta \rfloor$, $0 \leq l < b$, include $|a|$ consecutive integers, say $s, \ldots, s + |a| - 1$. Given any $i, j \in \mathbb{Z}$, we show that there exists integer $x$ such that $\lfloor ax/b + \beta \rfloor = i \pmod j$. We choose $t \in \mathbb{Z}$ such that $|tj + i - s| > |a|$ and $tj + i - s$ has the same sign as $a$. Then, write $tj + i - s = aq + u$, where $q \geq 1$ and $u \in \{0, \ldots, |a| - 1\}$. Since there exists $0 \leq l < b$ such that $al/b + \beta = s + u$, with $x = bq + l$, we have $\lfloor ax/b + \beta \rfloor = aq + \lfloor al/b + \beta \rfloor = aq + s + u = i \pmod j$. It follows that $P(x)$ is complete in $\mathbb{Z}$, and the proof is completed.

To prove Theorem 7 we need the following two lemmas.

Lemma 12. Let $R(x)$ be a polynomial with integer coefficients with no real roots. Then there exist infinitely many primes $p$ such that $R(x)$ has no roots mod $p$.

Proof. Suppose on the contrary that $R(x)$ has a root modulo all primes large enough. It follows from the Chebotarev density theorem that every element of the Galois group of the splitting field of $R(x)$ has a fixed point in the action on the roots. In particular, complex conjugation must have a fixed point on the set of the roots of $R(x)$, which contradicts our assumption that $R(x)$ has no real roots. \hfill $\Box$

Lemma 13. Let $Q(x)$ be a polynomial of even degree with integer coefficients, and let $A_0, \ldots, A_{N-1} \in \mathbb{Z}$. Then, there exist an arbitrarily large prime $p$ and an integer $m$ such that $Q(x) + A_i \neq m \pmod p$ for all $x \in \mathbb{Z}$ and $i \in \{0, \ldots, N - 1\}$.

Proof. Choose $M \in \mathbb{Z}$ so that $Q(x) + M + A_i$ has no real roots for all $0 \leq i < N$. We let
\[
R(x) = (Q(x) + M + A_0) \cdots (Q(x) + M + A_{N-1}).
\]
Then \( R(x) \) has no real roots. By Lemma 12, there exists an arbitrarily large prime \( p \) such that \( R(x) \not\equiv 0 \pmod{p} \) for all \( x \in \mathbb{Z} \). It follows that \( Q(x) + A_i \neq -M \) for all \( x \in \mathbb{Z} \) and \( i \in \{0, \ldots, N - 1\} \). \( \square \)

We are now ready to prove Theorem 7.

**Proof of Theorem 7.** Let \( P(x) = \sum_{i=0}^{n} a_i x^i \) such that \( a_i = \frac{r_i}{s_i} \in \mathbb{Q} \) with \( \gcd(r_i, s_i) = 1 \) for all \( 1 \leq i \leq n \). Let \( N \) be the least common multiple of \( s_i, 1 \leq i \leq n \). One has

\[
\lfloor P(Nk+j) \rfloor = \lfloor P(j) \rfloor + \frac{N}{s_i} \left( (Nk+j)^i - j^i \right).
\]

And so

\[
N[P(Nk+j)] = N[P(j)] + N \sum_{i=1}^{n} \frac{r_i}{s_i} ((Nk+j)^i - j^i).
\]

\[
= N[P(j)] - \sum_{i=1}^{n} \frac{N}{s_i} j^i + Q(Nk+j)
\]

(6)

where \( Q(x) = N(P(x) - P(0)) \in \mathbb{Z}[x] \) and \( A_j \in \mathbb{Z} \) depending on \( j \) and \( P(x), 0 \leq j < N \). By Lemma 13 there exist an arbitrarily large prime \( p > N \) and integer \( m \) such that \( Q(x) + A_j \neq m \pmod{p} \) for all \( x \in \mathbb{Z} \) and \( j \in \{0, \ldots, N - 1\} \). We claim that \( P(x) \) is not complete mod \( p \). On the contrary, suppose there exists an integer \( x \) such that \( \lfloor P(x) \rfloor = K \pmod{p} \), where \( K \) is such that \( NK = m \pmod{p} \). But then, writing \( x = Nk + j \) with \( 0 \leq j < N \), we have \( Q(Nk+j) + A_j = N\lfloor P(Nk+j) \rfloor = NK = m \pmod{p} \). This is a contradiction, and the proposition follows. \( \square \)

4. Complete monomials

Let \( p \) be a prime and \( n \) be a positive integer that divides \( p - 1 \). An \( n \)th power character modulo \( p \) is any homomorphism \( \chi : \mathbb{Z}_p^* \to \mathbb{C} \) that is onto the group of \( n \)th roots of unity. By a theorem of A. Brauer [1, 9], given \( n, l \geq 1 \), there exists a constant \( z(n, l) \) such that for every prime \( p > z(n, l) \) and any \( n \)th power character \( \chi \) modulo \( p \), there exists an integer \( t \) such that

\[
\chi(t) = \chi(t+1) = \cdots = \chi(t+l-1).
\]

(7)
A number $x$ is an $n$th power residue mod $p$, if there exists $y$ such that $x = y^n \pmod{p}$. If $\chi$ is an $n$th power character mod $p$ and $x$ is an $n$th power residue mod $p$, then $\chi(x) = \chi(y^n) = (\chi(y))^n = 1$. Therefore, to show that a number $z$ is not an $n$th power residue mod $p$, it is sufficient to find an $n$th power character mod $p$ such that $\chi(z) \neq 1$. We use this fact in the proof of the following lemma.

**Lemma 14.** For any positive integer $l$, there exist infinitely many primes $p$ such that all of the numbers $t, t + 1, \ldots, t + l - 1$ are all $n$th power non-residues modulo $p$ for some positive integer $t$.

**Proof.** To prove this claim, we assume without loss of generality that $n$ is prime and $l \geq 4$. By a result of Mills [7, Theorem 3], for every $m \geq 1$, there exists infinitely many primes $p$ with an $n$th power character $\chi$ modulo $p$ such that $\chi(2) \neq 1$, $\forall 2 \leq i \leq m$: $\chi(p^i) = 1$, where $p_i$ is the $i$th prime. Let $t$ be defined by (7); we can choose $t > 1$ by adding multiples of $p$ if necessary. Pick $m$ to be large enough so that $p_m > t + l - 1$. Choose $i \in \{0, \ldots, l - 1\}$ such that $t + i - 1 = 2(2d + 1)$ for some integer $d$. Then

$$\chi(2(2d + 1)) = \chi(2)\chi(2d + 1) \neq 1.$$ 

It then follows from (7) that $\chi(t) = \chi(t + 1) = \ldots = \chi(t + l - 1) \neq 1$ i.e., none of the values $t, t + 1, \ldots, t + l - 1$, are $n$th power residues modulo $p$. \[\square\]

**Theorem 15.** Let $P(x) = ax^n + c$, where $a \in \mathbb{Q}$ and $c \in \mathbb{R}$. If $n > 1$, then $P(x)$ is not complete mod infinitely many primes.

**Proof.** Let $a = M/N$ and $Q(x) = Mx^n$. Also, let $A_0, \ldots, A_{N-1}$ be given by (8). On the contrary, suppose $P(x)$ is complete mod all primes $p$ large enough. By Lemma 14 for $l = 1 + \max_i M^{n-1}A_i - \min_i M^{n-1}A_i$, there exists an arbitrarily large prime $p > MN$ and an integer $t$ such that $t + j$ is not an $n$th power residue modulo $p$ for any $0 \leq j < l$.

Let $K = t + \max_i M^{n-1}A_i$, and choose $L$ such that $M^{n-1}L = K \pmod{p}$. Since $P(x)$ is complete mod $p$, there exists an integer $x$ such that $N[P(x)] = L \pmod{p}$. Writing $x = Nk + j$ with $0 \leq j < N$, we have

$$M^{n-1}(Q(x) + A_j) = M^{n-1}N[P(x)] = M^{n-1}L = K \pmod{p}.$$
Since $t \leq K - M^{n-1}A_j < t + l$ and $K - M^{n-1}A_j = M^{n-1}Q(x) = (Mx)^n \pmod{p}$ is an $n$th power residue mod $p$, we have a contradiction, and the proposition follows. \hfill \Box

Remark 16. In light of the proofs of Theorems 7 and 15, one can prove Theorem 15 for all nonlinear polynomials if the following fact is true: Given a polynomial $P(x)$ with integer coefficients and a positive integer $l$, there exist an arbitrarily large prime $p$ and a positive integer $k$ such that $P(x) \neq l + i \pmod{p}$ for all $i = 0, \ldots, k - 1$.

References

[1] A. Brauer, Über sequenzen von Potenzresten, S.-B Deutsch Berlin, S. (1928) 9–16.
[2] G.H. Hardy and J.E. Littlewood, Some problems of Diophantine approximation. III: The fractional part of $n^k\theta$, Acta Math. 37 (1914), 155–191.
[3] I.J. Haländ, Uniform Distribution of Generalized Polynomials. J. Number Theory 45 (1993), 327–366.
[4] L. Kuipers and H. Niederreiter, Uniform distribution of sequences, Wiley, New York, 1974.
[5] W.J. LeVeque, Note on a theorem of Köksma, Porc. Amer. Math. Soc. 1 (1950), 380–383.
[6] S. Lang, Hilbert’s Irreducibility Theorem. In: Fundamentals of Diophantine Geometry. Springer, New York, NY, 1983.
[7] W.H. Mills, Characters with preassigned values, Canad. J. Math. 15 (1963), 169–171.
[8] I. Niven, Uniform distribution of sequences of integers, Trans. Amer. Math. Soc. 98 (1961) 52–61.
[9] J.R. Rabung and J.H. Jordan, Consecutive power residues or nonresidues, Math. Comput. 24 (111) (1970) 737–740.